

*‘To Protect My Health,  
or  
To Protect My Health Data?’*

Examining the Influence of Health Information  
Privacy Concerns on Citizens’ Health Technology  
Adoption.

Grace Kenny, M.Sc., B.B.S

Research Supervisor: Professor Regina Connolly

A Thesis Submitted to Dublin City University Business School in partial  
fulfilment of the requirements

for the degree of

Doctor of Philosophy

September 2016

## **DECLARATION**

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of Doctor of Philosophy is entirely my own work, and that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: \_\_\_\_\_ ID No.: \_\_\_\_\_

Date: \_\_\_\_\_

## DEDICATION

*To my love Charles, my inspiring mother, and my precious nephew Ryan.*

## ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to my supervisor Professor Regina Connolly for her continual support and guidance over the past three years. Her expertise has helped sculpt the PhD, and provided me with great clarity at crucial points of the journey. Regina's encouragement, motivation, and belief, encouraged me to persevere throughout this journey. I am also very thankful to Professor Alan Smeaton, my panel member, who encouraged me to think big. Alan's genuine interest in my progress and willingness to help, coupled with his fountain of ideas and knowledge, helped make the PhD more interesting. I am extremely grateful to all Academic and Administrative staff at Dublin City University who offered support, advice, and encouragement throughout the journey.

I was very fortunate to visit Arizona State University. I am extremely grateful to Dr. Breda Kieran and the DCU-ASU Transatlantic Partnership for facilitating this visit. A huge thanks must be given to Dr. Deb Williams, and Dr. Matt Buman for their advice in developing the survey instrument and their help in data collection. I am also grateful to all anonymous reviewers of the papers developed from this thesis and the faculty mentors at the ECIS Doctoral Consortium 2015 for their expert advice on strengthening the thesis.

This PhD was supported by the Daniel O'Hare PhD Scholarship Scheme at Dublin City University. Without this scholarship, the PhD would not have been possible and I am grateful to Dublin City University for providing me with this opportunity. I am thankful to the Graduate Studies Office for all their support and help throughout the course of the PhD. I am also very thankful to the staff at MedEx and the Intergenerational Learning Programme at DCU for their help with data collection.

My PhD journey would not have been possible without the support and of company of the PhD community at Dublin City University. I was very fortunate to share this journey

with some wonderful people. A special thanks to Roisin Lyons, my wonderful office mate for the past three years, your company and advice has helped me so much. Thanks also to Catherine Faherty for the friendship, much needed laughs and the coffee counselling sessions. Frances O'Connell, thank you for sharing your wonderful mind with me. Your wisdom and support helped me so much throughout this journey. A huge thanks to Xiaoning Liang for sharing this journey with me and helping solve every problem I encountered. Thank you for every cup of coffee, every walk, every 'shut up and write' session, and every encouraging text. I am so grateful for your friendship.

To my parents, Imelda and Frank I am so grateful for everything you have done for me throughout my life. I hope you are proud. To my sister Helena, her husband Alan, and my brothers John and Aaron, thank you for the support, love, and encouragement over the course of this journey. To my great friend, Emma thank you for the continual motivation, belief, and for ensuring life remained fun throughout this journey. I am most grateful to my love Charles. Thank you for your constant belief in me, unwavering support, endless encouragement, vested interest in each aspect of the thesis, and most of all, your love. You have shared every moment of this journey with me, and I am so lucky to be able to share my life with you.

## TABLE OF CONTENTS

DECLARATION .....	i
DEDICATION .....	ii
ACKNOWLEDGEMENTS .....	iii
TABLE OF CONTENTS.....	v
LIST OF TABLES .....	xiii
LIST OF FIGURES .....	xv
LIST OF ABBREVIATIONS .....	xvi
PUBLICATIONS DEVELOPED FROM THE THESIS .....	xvii
ABSTRACT.....	xviii

## CHAPTER ONE: INTRODUCTION

1.1	Overview of the Dissertation .....	1
1.2	Justification of the Research .....	2
1.2.1	The Importance of the Health Context.....	2
1.2.2	HIPC and Technology Adoption.....	3
1.2.3	The Need for Comprehensive Studies.....	4
1.2.4	Significance of the Research Context .....	5
1.2.5	Summary: The Importance of this Study .....	6
1.3	Research Objectives.....	6
1.4	Research Questions and Framework.....	7
1.5	Key Hypotheses .....	8
1.6	Research Methodology .....	9
1.7	Dissertation Outline .....	9

## CHAPTER TWO: LITERATURE REVIEW

2.1	Introduction.....	11
-----	-------------------	----

2.2	Information Privacy: Historical Roots & Conceptualisations .....	13
2.2.1	Historical Foundations .....	13
2.2.2	Privacy Definitions Across Disciplines .....	14
2.2.3	Health Information Privacy: Seeking Definitional Clarity .....	18
2.3	Research Questions .....	19
2.4	Information Privacy and Theory .....	20
2.4.1	The Origin of Privacy Concerns .....	20
2.4.2	Institutional Factors and Concern .....	22
2.4.3	Individual Factors and Concern .....	22
2.4.4	Privacy Concern and Behavioural Outcomes .....	24
2.4.5	Exploring the Trade-Offs .....	24
2.4.6	Developing a Theoretical Framework.....	25
2.5	Antecedents to Information Privacy Concern .....	27
2.5.1	Individual Characteristics .....	27
2.5.2	Individual Perceptions.....	31
2.5.3	Individual Experiences.....	34
2.5.4	Additional Antecedents.....	36
2.5.5	Summary of the Chosen Antecedents .....	39
2.6	Understanding Information Privacy Concerns.....	42
2.6.1	Dimensions of Information Privacy Concern .....	42
2.6.2	Measures of Information Privacy Concern .....	46
2.6.3	Choosing a Measure for this Study .....	48
2.7	Outcomes of Information Privacy Concern .....	52
2.8	Information Privacy Concerns and Technology Adoption .....	54
2.8.1	Models of Technology Adoption .....	54
2.8.2	Health Technology Adoption Among Health Professionals.....	58
2.8.3	Health Technology Adoption Among Citizens.....	59
2.9	Summary of Gaps in the Literature.....	66
2.10	Conclusion .....	67

### **CHAPTER THREE: PROPOSED FRAMEWORK & HYPOTHESES**

3.1	Introduction.....	68
3.2	Existing Literature and This Study .....	70
3.3	Proposed Research Framework.....	76
3.3.1	Theoretical Background.....	77
3.4	Hypotheses: Antecedents .....	79
3.4.1	Individual Characteristics .....	79
3.4.2	Individual Perceptions.....	82
3.4.3	Individual Experiences.....	84
3.5	Hypotheses: HIPC and Adoption.....	86
3.5.1	Technology 1: EHRs.....	86
3.5.2	Technology 2: Mobile Health Solutions .....	88
3.5.3	Additional Factors.....	90
3.6	Hypotheses: Moderation .....	91
3.6.1	Health Conditions as Moderators.....	91
3.6.2	Privacy Invasion Experiences as Moderators .....	93
3.7	Summary and Next Steps.....	94

### **CHAPTER FOUR: RESEARCH METHODOLOGY**

4.1	Introduction.....	96
4.2	Competing Philosophies & Methodologies .....	98
4.2.1	Quantitative vs. Qualitative Methodologies.....	98
4.2.2	Mixed Methods, the Third Methodological Movement .....	99
4.2.3	Pragmatism as a Research Philosophy .....	101
4.3	Context Selection .....	102
4.4	Research Design.....	103
4.5	Sampling Procedures .....	106
4.5.1	Recruitment: Exploratory Interviews.....	108
4.5.2	Survey Sample Recruitment.....	108



4.5.3	Interview Participant Recruitment .....	109
4.6	Stage One: Exploratory Interviews .....	110
4.6.1	Analysis: Exploratory Interviews.....	110
4.7	Stage Two: Survey .....	114
4.7.1	Survey Design and Pilot Testing.....	115
4.7.2	Survey Structure.....	116
4.7.3	Measurement of Variables .....	116
4.7.4	Summary .....	121
4.8	Stage Three: In-depth Interviews .....	121
4.9	Conclusion .....	122

## **CHAPTER FIVE: QUANTITATIVE DATA ANALYSIS**

5.1	Introduction.....	124
5.2	Sample Response Rates .....	126
5.2.1	Responses: Irish Sample .....	126
5.2.2	Responses: U.S. Sample.....	127
5.3	Data Screening and Preparation.....	127
5.3.1	Addressing Missing Data .....	127
5.3.2	Identifying Outliers .....	128
5.4	Sample Profile.....	129
5.4.1	Profile: Irish Sample .....	129
5.4.2	Profile: U.S. Sample.....	129
5.5	Testing Multivariate Assumptions .....	130
5.6	Model 1: HIPC and EHR Acceptance.....	131
5.6.1	Model 1: Model Fit .....	133
5.6.2	Model 1: Validity & Reliability Testing .....	134
5.6.3	Model 1: Testing for Common Method Bias .....	136
5.6.4	Model 1: Individual Variables .....	136
5.6.5	Model 1: Correlations .....	142

5.6.6	Model 1: Hypothesis Testing .....	142
5.6.7	Model 1: Testing Moderation Effects .....	145
5.6.8	Model 1: Testing Mediation Effects .....	149
5.6.9	Model 1: Additional Constructs .....	150
5.6.10	Model 1: Summary.....	151
5.7	Model 2: HIPC and mHealth Adoption .....	152
5.7.1	Model 2: Model Fit .....	153
5.7.2	Model 2: Validity & Reliability Testing .....	154
5.7.3	Model 2: Testing for Common Method Bias .....	156
5.7.4	Model 2: Individual Variables .....	156
5.7.5	Model 2: Correlations .....	163
5.7.6	Model 2: Hypothesis Testing .....	163
5.7.7	Model 2: Testing Moderation Effects .....	167
5.7.8	Model 2: Testing Mediation Effects .....	171
5.7.9	Model 2: Additional Constructs .....	171
5.7.10	Model 2: Summary.....	172
5.8	Chapter Summary .....	172

## **CHAPTER SIX: QUALITATIVE ANALYSIS**

6.1	Introduction.....	174
6.2	Qualitative Analysis Procedures .....	176
6.2.1	Sample Overview .....	178
6.2.2	Validation Procedures .....	178
6.3	Overview of the Themes .....	181
6.4	Antecedents of HIPC .....	181
6.4.1	Awareness of Privacy Media Coverage .....	181
6.4.2	Privacy Invasion Experience.....	185
6.4.3	Health Information Seeking Experience .....	190
6.4.4	Perceived Trust .....	192

6.4.5	Perceived Risk.....	198
6.4.6	Perceived Sensitivity.....	200
6.5	Examining Citizens' HIPC.....	203
6.5.1	Collection.....	204
6.5.2	Unauthorised Secondary Use .....	205
6.5.3	Improper Access .....	206
6.5.4	Errors.....	208
6.5.5	Control .....	208
6.5.6	Awareness .....	209
6.6	HIT Acceptance and Adoption .....	211
6.6.1	Perceived Benefits and Adoption.....	212
6.6.2	HIPC and Adoption.....	213
6.7	Additional Factors.....	214
6.7.1	Perceived Ownership .....	214
6.7.2	Health Locus of Control.....	216
6.7.3	Privacy Protective Behaviours .....	216
6.8	Integrated Findings .....	217
6.8.1	Development of Meta-Inferences.....	222
6.9	Conclusion .....	223

## **CHAPTER SEVEN: DISCUSSION**

7.1	Introduction.....	224
7.2	Research Objectives.....	226
7.2.1	Examining the Antecedents .....	226
7.2.2	Measuring HIPC .....	228
7.2.3	Investigating the HIPC-Intention Relationship.....	229
7.2.4	Exploring Moderating Influences .....	230
7.3	Reviewing the Findings .....	231
7.3.1	Antecedents to HIPC.....	231

7.3.2	Towards a comprehensive measure of HIPC .....	234
7.3.3	Understanding the HIPC-Intention Relationship .....	236
7.3.4	Examining Moderating Influences.....	237
7.4	Research Contributions .....	239
7.5	Towards a Revised HIPC Framework .....	243
7.6	Implications for Practice .....	247
7.7	Conclusion and Summary of the Contributions .....	252

## **CHAPTER EIGHT: CONCLUSION**

8.1	Introduction.....	254
8.2	Contributions to Theory .....	254
8.2.1	Addressing Gaps in the Literature.....	255
8.2.2	Additional Contributions.....	258
8.3	Overview of the HIPC Framework .....	259
8.4	Limitations and Directions for Future Research .....	260
8.5	Summary .....	263

<b>REFERENCES.....</b>	<b>264</b>
------------------------	------------

APPENDIX A: HEALTH TECHNOLOGY ADOPTION STUDIES .....	283
--	-----

APPENDIX B: SYSTEMATIC LITERATURE REVIEW SEARCH TERMS .....	286
---	-----

APPENDIX C: SYSTEMATIC LITERATURE REVIEW: JOURNALS .....	287
--	-----

APPENDIX D: ETHICAL APPROVAL LETTER.....	288
--	-----

APPENDIX E: SURVEY INVITATION EXAMPLE .....	289
---	-----

APPENDIX F: SURVEY INSTRUMENT.....	290
------------------------------------	-----

APPENDIX G: SURVEY ITEMS AND SUPPORT.....	307
---	-----

APPENDIX H: INTERVIEW CONSENT FORM.....	311
---	-----

APPENDIX I: INTERVIEW GUIDE.....	312
----------------------------------	-----

APPENDIX J: CODING PROTOCOL.....	318
APPENDIX K: INTERVIEW ANALYSIS: MEDIA COVERAGE .....	320
APPENDIX L: INTERVIEW ANALYSIS: PRIVACY INVASION EXPERIENCE .....	332
APPENDIX M: INTERVIEW ANALYSIS: HEALTH INFORMATION SEEKING .....	343
APPENDIX N: INTERVIEW ANALYSIS: TRUST .....	360
APPENDIX O: INTERVIEW ANALYSIS: RISK.....	376
APPENDIX P: INTERVIEW ANALYSIS: SENSITIVITY .....	382
APPENDIX Q: INTERVIEW ANALYSIS: HIPC.....	389
APPENDIX R: INTERVIEW ANALYSIS PERCEIVED BENEFITS.....	423
APPENDIX S: INTERVIEW ANALYSIS: ADOPTION INTENTIONS .....	435

## LIST OF TABLES

2.1 Privacy definitions across disciplines .....	17
2.2 Gender and Privacy .....	28
2.3 Studies Exploring Age as an Antecedent .....	29
2.4 Additional Demographic Variables .....	30
2.5 Antecedents in the Study .....	40
2.6 Existing Measures of Information Privacy Concern .....	49
2.7 Dimensions of HIPC .....	52
2.8 Technology Adoption Models .....	58
2.9 Systematic Review Comparison .....	60
2.10 Inclusion Criteria for Systematic Review .....	61
2.11 Systematic Review Findings .....	62
3.1 Comparing this Study with Previous Work .....	71
4.1 Comparison of Paradigms .....	102
4.2 Antecedents: Findings .....	112
4.3 Additional Antecedents .....	113
4.4 Dimensions of HIPC .....	113
5.1 Model fit statistics: Model 1 .....	134
5.2 Validity and Reliability: Model 1 .....	135
5.3 Model 1: Construct Descriptives .....	139
5.4 Model 1: Correlations .....	142
5.5 Model 1: Findings .....	145
5.6 Model 1: Moderating Effects of Chronic Illness .....	146
5.7 Model 1: Moderating Effects of Sensitive Illness .....	147
5.8 Model 1: Moderating Effects of Personal Privacy Invasion .....	147
5.9 Model 1: Moderating Effects of Health Privacy Invasion .....	148
5.10 The Mediating Role of HIPC .....	149

5.11 Model 2: Model fit statistics .....	154
5.12 Validity and Reliability: Model 2 .....	155
5.13 Model 2: Construct Descriptives.....	159
5.14 Model 2: Correlations .....	163
5.15 Model 2: Findings .....	166
5.16 Model 2: Moderating Effects of Chronic Illness.....	167
5.17 Model 2: Moderating Effects of Sensitive Illness .....	168
5.18 Model 2: Moderating Effects of Personal Privacy Invasion .....	169
5.19 Model 2: Moderating Effects of Health Privacy Invasion .....	170
5.20 Quantitative Findings .....	173
6.1 Coding Example.....	178
6.2 Integrated Findings .....	219
6.3 Summary of Meta-Inferences.....	223
7.1 Summary of Study Contributions .....	253

## LIST OF FIGURES

1.1 Proposed Research Framework.....	7
1.2 Research Design.....	9
1.3 Conceptual map of the Dissertation .....	10
2.1 Chapter Structure .....	12
2.2 Theories included in this Study.....	26
2.3 Cultural Comparison Between Ireland and the U.S. ....	38
3.1 Chapter Structure .....	69
3.2 Proposed Research Framework.....	76
4.1 Chapter Structure .....	97
4.2 Stages of the Research .....	105
5.1 Chapter Structure .....	125
5.2 Proposed Model 1 .....	132
5.3 Model 1: Results .....	144
5.4 Proposed Model 2 .....	153
5.5 Model 2: Results .....	165
6.1 Chapter Structure .....	175
6.2 Privacy Media Coverage and HIPC.....	185
6.3 Privacy Invasion Experience and HIPC.....	190
6.4 Perceived Trust and HIPC.....	196
6.5 Perceived Risk and HIPC.....	199
6.6 Perceived Sensitivity and HIPC .....	203
7.1 Chapter Structure .....	225
7.2 Proposed Antecedents .....	227
7.3 HIPC Dimensions .....	228
7.4 Proposed HIPC-Intention Relationship.....	230
7.5 Final HIPC Framework.....	243



## **LIST OF ABBREVIATIONS**

ASU = Arizona State University

CFA = Confirmatory Factor Analysis

DCU = Dublin City University

EFA = Exploratory Factor Analysis

EHR = Electronic Health Record

HIPAA = Health Insurance Portability and Accountability Act

HIPC = Health Information Privacy Concerns

HIT = Health Information Technology

HSE = Health Service Executive

IBT = Information Boundary Theory

ILP = Intergenerational Learning Programme

mHealth = Mobile Health

MIS = Management Information Systems

PC = Privacy Concern

PMT = Protection Motivation Theory

SEM = Structural Equation Modelling

SPSS = Statistical Package for the Social Sciences

TPB = Theory of Planned Behaviour

TRA = Theory of Reasoned Action

UTAUT = Unified Theory of Acceptance and Usage of Technology

## PUBLICATIONS DEVELOPED FROM THE THESIS

### Book Chapters

Kenny, G. and Connolly, R. 2016. Citizens' Health Information Privacy Concerns: Developing a Framework. *IN: Fabrizio D'Ascenzo et al. (eds.) Blurring the Boundaries through Digital Innovation*, Lecture Notes in Information Systems. Switzerland: Springer Series, Vol. 19, PP.131-143.

### Conference Proceedings

Kenny, G. 2016. Mobile Health Technologies and Information Privacy: A Citizen Perspective. *76<sup>th</sup> Academy of Management Conference*, 5-9<sup>th</sup> Aug 2016, Anaheim.

Kenny, G., and Connolly R. (2016). Drivers of Health Information Privacy Concerns: A Comparison Study. *22nd Americas Conference on Information Systems (AMCIS)*, 11-13th Aug 2016, San Diego.

Kenny, G., Connolly, R., and McConalogue, E. (2016). 'For my Doctor told me so'. Examining the Influence of Trust on Citizens' Information Privacy Concerns and Health Technology Acceptance. *19th Irish Academy of Management Conference (IAM)*, 1<sup>st</sup>-2<sup>nd</sup> Sep 2016, University College Dublin, Ireland.

Kenny, G. (2015). Technology Enabled Health Ageing: Exploring the Inhibiting Role of Information Privacy Concerns. *Inaugural Age Friendly Universities Conference*, 2nd-3rd Nov 2015, Dublin, Ireland.

Kenny, G. and Connolly, R. (2015). Developing an Approach to Measure Citizens' Health Information Privacy Concerns (HIPC). *The Amsterdam Privacy Conference (APC2015)*, 23rd-26th Oct 2015, Amsterdam, The Netherlands.

Kenny, G. and Connolly, R. (2015). Unlocking the Potential of ICT in Healthcare, one Barrier at a Time: A Citizen Health Information Privacy Concern Perspective. *The 18th Irish Academy of Management Annual Conference 2015 (IAM)*, 2nd- 4th Sep 2015, National University of Galway, Galway, Ireland.

Kenny, G. and Connolly, R. (2015). Citizens' Health Information Privacy Concerns: A Multifaceted Approach. *23rd European Conference on Information Systems (ECIS)*, 26th – 29th May 2015, Muenster, Germany.

Kenny, G. and Connolly, R. (2014). Why do Information Privacy Concerns Warrant Consideration when implementing Electronic Health Record Systems? *The 17th Irish Academy of Management Annual Conference 2014 (IAM)*, 3rd-5th Sep 2014, University of Limerick, Limerick, Ireland.

Kenny, G. and Connolly, R. (2014). Electronic Health Record Systems: The Need to Consider Patient Privacy Concerns. *The 8th Annual Irish Human Computer Interaction Conference 2014 (iHCI)*, 1<sup>st</sup>-2<sup>nd</sup> Sep 2014, Dublin City University, Dublin Ireland.

# ABSTRACT

**Grace Kenny**

*‘To Protect My Health,  
or  
To Protect My Health Data?’*

## Examining the Influence of Health Information Privacy Concerns on Citizens’ Health Technology Adoption

This study conducts a holistic investigation of citizens’ health information privacy concerns (HIPC). Specifically, it develops a framework for examining the drivers, dimensions, and outcomes of HIPC. It is proposed that HIPC are formed from individuals’ characteristics, perceptions, and experiences. HIPC are expected to reduce individuals’ intentions (1) to accept Electronic Health Records (EHRs) and (2) to adopt mobile health (mHealth) solutions.

To explore these assumptions, the study utilises a three-stage sequential mixed methods approach. In the first stage, exploratory interviews were conducted to refine the proposed framework. In the second stage, the hypothesised relationships in the framework were empirically tested, using a survey of 445 citizens in Ireland and the United States. In the third stage, in-depth interviews were conducted with 50 citizens in both countries to further explore these relationships. The quantitative and qualitative findings were then integrated to elucidate the underpinnings of HIPC.

The integrated findings show that citizens’ HIPC are shaped by characteristics such as age and healthcare need, perceptions of trust, risk, and sensitivity, and experience of privacy media coverage. HIPC reduces adoption intentions, and influences the type of mHealth solution citizens are willing to adopt, as well as the type and volume of data disclosed. Perceived hedonic and utilitarian benefits positively influence adoption intentions, but in order to sustain this influence, these benefits must remain relevant to the individual.

The study provides detailed insights into how citizens’ HIPC are developed, and how along with perceived benefits, they can influence adoption intentions and subsequent use behaviours. It also extends the Information Boundary theory (Petronio, 1991), Protection Motivation theory (Rogers, 1975), and Privacy Calculus theory (Culnan 1993) to the health information privacy context. The study’s findings provide actionable insights which can assist health organisations and technology companies in addressing citizens’ HIPC more successfully.

# **CHAPTER ONE: INTRODUCTION**

## **1.1 Overview of the Dissertation**

This dissertation examines the influence of citizens' health information privacy concerns (HIPC) on their acceptance and adoption of Health Information & Communication Technologies (ICTs). The research objectives include examining the antecedents to HIPC, developing a comprehensive measure of HIPC, exploring the relationship between these concerns and citizens' adoption of health ICTs, and investigating the indirect moderating influences on this relationship. To achieve these objectives, the study develops the HIPC framework which aims to unravel the labyrinthine information privacy construct in the health context.

The HIPC framework is developed based on the extant information privacy and technology adoption literature in the Management Information Systems (MIS) and Health Informatics disciplines. The framework explores several antecedents to HIPC across three categories (individual characteristics, perceptions, and experiences), measures HIPC across six dimensions, and investigates the relationships between HIPC, perceived benefits, and adoption response. The framework is based on the foundations of the Theory of Reasoned Action (TRA) (Fishbein and Azjen, 1975), and is supported by the Information Boundary Theory (IBT) (Petronio, 1991), Protection Motivation theory (PMT) (Rogers, 1975), and the Privacy Calculus theory (PCT) (Culnan, 1993; Culnan and Armstrong, 1999). A three-stage sequential mixed methods research design was developed to test the proposed framework. The study's integrated quantitative and qualitative findings are discussed in conjunction with the insights provided by existing literature to enhance understanding of citizens' HIPC.

This chapter begins by justifying the need for this research. The objectives of the research are then outlined along with the proposed research framework and key hypotheses. The chapter concludes with an overview of the dissertation structure.

## 1.2 Justification of the Research

The need for this study is discussed across four areas: the special nature of health data, HIPC and technology adoption, the need to comprehensively examine HIPC, and the study sample.

### 1.2.1 *The Importance of the Health Context*

Information privacy began attracting attention in terms of public conversation, policy changes, and empirical research in the 1960s (Regan *et al.*, 2013). However, only in recent years has the interest of information privacy researchers shifted to the health context. To date, a small number of studies in the MIS and Health Informatics literature have examined health information privacy, a fraction of which have focused on citizens as opposed to health professionals. The under-examination of privacy in the health context is surprising as health is an issue of fundamental importance to society and individuals, and privacy represents a contentious issue in health (Payton *et al.*, 2011). Furthermore, privacy has been a vital component of healthcare delivery for centuries, with doctors around the world pledging to protect patients' privacy under the Hippocratic Oath (Lasagna, 1964). It is argued that the health context represents a fruitful avenue for information privacy research for four reasons. Firstly, due to its personal nature, health information is more sensitive than other information types. For instance, 93% of Irish citizens describe their health information as very sensitive (Eurobarometer, 2011). Secondly, individuals have been found to express high privacy concerns regarding their health data (e.g. Clarke *et al.*, 2009; Lafky and Horan, 2011). Thirdly, if health data privacy is not protected, individuals' lives can be negatively impacted (Anderson and Agarwal, 2011). Fourthly, HIPC can reduce individuals' willingness to adopt health technologies (Angst and Agarwal, 2009), and cause individuals to withhold health data (Campos-Castillo and Anthony, 2014). While similar outcomes are associated with information privacy concerns in other contexts, these behaviours are particularly important in the health context as withholding health data can lead to dangerous misdiagnoses, and refusal to accept an EHR can reduce the quality of care received.

Recent studies which have focused on health information privacy (e.g. Angst and Agarwal, 2009; Hwang *et al.*, 2012; Dinev *et al.*, 2016) illustrate the relevance of this research stream. However, many gaps persist in our understanding of the information privacy construct in the health context, thus supporting the need for further exploration (Agarwal *et al.*, 2010).

### ***1.2.2 HIPC and Technology Adoption***

The adoption of health ICTs, both in the context of healthcare delivery and personal health management has grown exponentially in recent years. In terms of the former, Electronic Health Record systems (EHRs) enable health professionals to create, maintain, and share comprehensive patient records (Angst and Agarwal, 2009). EHRs promise many benefits including: facilitating the monitoring of patient health over time (Department of Health, 2013), enabling access to test results in real time (E-Estonia, 2014), and facilitating monetary savings (Evans, Nichol, and Perlin, 2006; Robey, 2014). These benefits are wide reaching, affecting healthcare professionals, healthcare organisations, citizens, and patients (European Commission, 2012).

In terms of the latter, mobile health (mHealth) solutions offer individuals the ability to monitor their health conditions and health indicators (Eng and Lee, 2013). They have the potential to transform healthcare by empowering citizens to take control of their illnesses and overall health (Whittaker, 2012; Eng and Lee, 2013; Gay and Leijdekkers, 2015). This study focuses on three specific mHealth technologies, the first being mHealth applications, which are applications on mobile devices that enable individuals to track anything from pregnancy symptoms, to chronic illness factors such as glucose levels (Fox and Duggan, 2012). Use of mHealth applications has grown massively, with 19% of U.S. adults utilising an mHealth application in 2012 (Fox and Duggan, 2012). It was also forecast that 500 million people worldwide would use an mHealth application in 2015 (Privacy Rights ClearingHouse, 2013). The second mHealth technology which this study focuses on is wearable health devices, such as smartwatches and fitness bands that facilitate the tracking of steps taken, sleep quality, and heart rate. Despite their recent emergence, 13 million wearables were sold by 2013, a number which is expected to rocket to 187

million by 2020 (Mottl, 2015). The third mHealth technology which this study focuses on is Personal Health Records (PHRs), such as Microsoft Healthvault, which enable individuals to maintain an electronic record of their health (Li *et al.*, 2014). PHR adoption has been slower, with 7% of U.S. adults utilising PHRs in 2010 (Ackerman, 2010).

Both EHRs and mHealth solutions have enormous potential to benefit individuals and organisations, while also reducing the financial burden on health services (PWC, 2013). However, these benefits are predicated on citizen acceptance and adoption (Or *et al.*, 2011). Consequently, it is important to explore the factors that drive or inhibit the adoption of these technologies (Dinev *et al.*, 2016) such as HIPC, which is widely viewed as the greatest barrier facing the success of health ICTs (Chhanabhai and Holt, 2007). Research shows that citizens' HIPC negatively impact (1) their intentions to opt-in to EHRs (Angst and Agarwal, 2009; Li and Slee, 2014), (2) their intentions to adopt PHRs (Li *et al.*, 2014), and (3) their intentions to adopt mHealth applications (Hwang *et al.*, 2012). Therefore, there is a need to further explore the relationship between HIPC and adoption intentions to explain the reasons for the negative influence, and to identify the factors driving citizens' HIPC. This is fundamental to developing approaches to address citizens' HIPC, and increase acceptance and adoption of health ICTs.

### ***1.2.3 The Need for Comprehensive Studies***

This study is a response to the multiple calls by researchers (Korzaan and Boswell, 2008; Smith *et al.*, 2011) for a comprehensive study which explores the antecedents and consequences of HIPC. It does so by developing a framework, which leverages several theories to conduct a comprehensive investigation of information privacy in the health context. The framework includes antecedents that have been employed in previous studies, such as gender (Vodicka *et al.*, 2013), age (Hwang *et al.*, 2012), perceived sensitivity (Bansal *et al.*, 2010), and perceived trust (Dinev *et al.*, 2016), whilst also investigating the influence of additional antecedents such as privacy media coverage awareness, which is examined for the first time in this context. The study also goes beyond the one dimensional measures of concern that are employed in many studies

(e.g. Hwang *et al.*, 2012), and the four dimensional measure that has been frequently used in recent work on this issue (Angst and Agarwal, 2009; Li *et al.*, 2014; Dinev *et al.*, 2016). As a result, six dimensions of HIPC are employed in this study, which provides more granular insight into the factors influencing health information privacy concern. Similar to earlier work on this issue (e.g. Dinev *et al.*, 2016), the study leverages the Privacy Calculus theory in order to examine the relationships between HIPC, perceived benefits, and adoption intentions. In addition, this study focuses both on EHRs and mHealth solutions, whereas prior studies have focused only on one technology using limited measures to capture HIPC. Moreover, this study employs a mixed methods approach, which provides a more comprehensive understanding of the information privacy construct in the health context.

#### ***1.2.4 Significance of the Research Context***

The proposed framework is tested among citizens in the Republic of Ireland and the United States. These countries make for an interesting comparison due to differences in their health systems. The Irish health system is predominately publicly funded, while the U.S. system is largely privatised. Government spending accounted for 48.0% of healthcare spending in the U.S. in 2012, compared to 68.5% of spending in Ireland for the same year (OECD, 2015). Additionally, both countries differ in terms of the prevalence of health ICTs. While 78.4% of physicians in the U.S. used EHRs by 2013 (Hsiao and Hing, 2014), Ireland is yet to introduce a national EHR, despite announcing plans to do so (Department of Health, 2013). Thus U.S. citizens have greater exposure to the use of ICTs in the health setting. In terms of citizens' use of mHealth, in 2012, 19% of adults utilised an mHealth application in the U.S. (Fox and Duggan, 2012), where patient acceptance of health ICTs is a national priority (Or *et al.*, 2011). In contrast, there are no statistics indicative of mHealth usage among Irish citizens.

The selection of data samples drawn from these countries simultaneously answers calls for privacy research in European countries (Bélanger and Crossler, 2011), calls for the exploration of HIPC among different cultures (Dinesen *et al.*, 2016) and calls for health privacy studies which



compare U.S. and European countries (Li *et al.*, 2016). Both data samples include individuals of varying ages (18-82 years old), health status, education levels, technical competence, and job status. Consequently, the study also answers calls for studies which compare student and non-student populations (Bélanger and Crossler, 2011), and studies with older populations (Li *et al.*, 2014).

### ***1.2.5 Summary: The Importance of this Study***

This research is justified on three grounds. Firstly, as noted in the preceding sections, there are many gaps in our understanding of information privacy in the health context. This study addresses these gaps and conducts a comprehensive investigation of citizens' HIPC to enhance understanding of the drivers of HIPC, the important facets of HIPC, and the relationship between HIPC and adoption intentions. Secondly, the integrated quantitative and qualitative findings enable the presentation of practical recommendations which can be employed by health and technology organisations to appease citizens' HIPC and increase their adoption of health ICTs. Thirdly, the study findings identify additional avenues which have potential for researchers in this area. The HIPC framework can be tested and built upon by researchers in other countries, which will further enhance our understanding of information privacy in the health context.

## **1.3 Research Objectives**

The overarching aim of this study is develop a more comprehensive understanding of information privacy in the health context. This aim is represented by four research objectives.

The first objective is to explore the antecedents to citizens' HIPC. Based on the existing literature, and the theoretical arguments presented by the Information Boundary theory and Protection Motivation theory, a number of individual characteristics, perceptions, and experiences are identified as possible antecedents. The second objective is to develop a comprehensive measure for examining citizens' HIPC. To do so, this study adapts the Internet privacy concerns (IPC) measure (Hong and Thong, 2013) to the health context. The third objective aims to develop an

in-depth understanding of the relationship between HIPC and citizens' adoption intentions, as citizens' HIPC represent a barrier to the success of both EHRs (Dinev *et al.*, 2016) and mHealth solutions (Guo *et al.*, 2013; Li *et al.*, 2014; Li *et al.*, 2016). The study uses a mixed methods approach to gain a deeper understanding of adoption intentions and explain the trade-offs between HIPC and perceived benefits. The fourth objective seeks to explore the moderating influences of health conditions and privacy invasion experiences on the relationships between HIPC, perceived benefits, and adoption intentions.

## 1.4 Research Questions and Framework

The research objectives outlined above are addressed in the following three research questions:

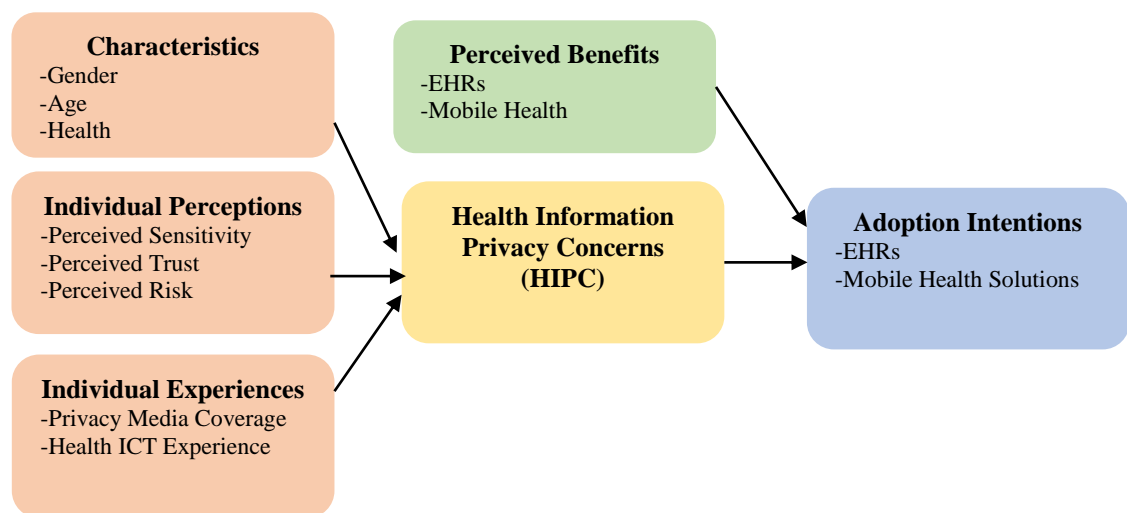
RQ1: What are the factors that influence HIPC?

RQ2: What dimensions of information privacy concern are most influential in the health context?

RQ3: Does HIPC influence citizens' acceptance and adoption of health ICTs?

The research framework outlined in Figure 1.1 below, explores these questions by investigating the predictors of HIPC, examining six dimensions of privacy concern, and exploring the relationship between HIPC and adoption intentions.

**Figure 1.1 Proposed Research Framework**



The research framework argues that individuals' HIPC are shaped by their personal characteristics, perceptions, and experiences. In line with the Information Boundary theory (IBT), it is proposed that higher perceptions of sensitivity will increase HIPC (Bansal *et al.*, 2010). In accordance with Protection Motivation theory (PMT) (Rogers, 1975), it is posited that threat appraisal factors including perceived risks associated with health data disclosure and privacy media coverage awareness, will increase HIPC, and coping appraisal factors including perceived trust in health professionals and technology vendors, and experience of using technology for health purposes, will reduce HIPC. Lastly, following the Privacy Calculus theory, it is proposed that individuals' adoption intentions will be negatively influenced by HIPC, and positively influenced by perceived benefits.

## 1.5 Key Hypotheses

The key hypotheses in the study are outlined in Table 1.1 below. These hypotheses are developed in Chapter 3 based on the Literature Review conducted in Chapter 2.

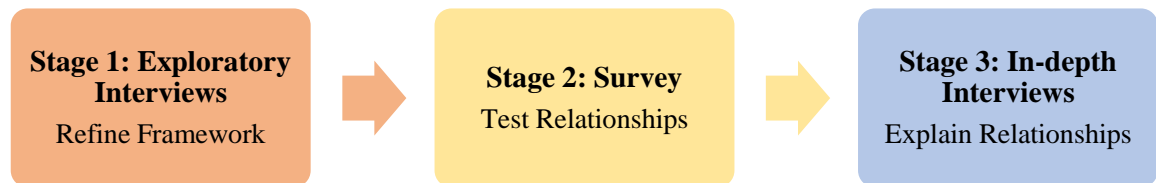
**Table 1.1 Key Hypotheses in the Study**

Hypotheses	
H1	Females express higher HIPC
H2	Age positively influences HIPC
H3	Health Status positively impacts HIPC
H4	Healthcare Need positively impacts HIPC
H5	Perceived Sensitivity increases HIPC
H6	Perceived Trust reduces HIPC
H7	Perceived Risk increases HIPC
H8	Privacy Media Coverage Awareness increases HIPC
H9	Health Information Seeking Experience reduces HIPC
H10	Mobile Health Experience reduces HIPC
H11	HIPC reduce intentions to adopt Health ICTs
H12	Perceived Benefits increase intentions to adopt Health ICTs

## 1.6 Research Methodology

To test the proposed research framework, this study follows a three-stage sequential mixed methods research design, as outlined below in Figure 1.2.

**Figure 1.2 Research Design**



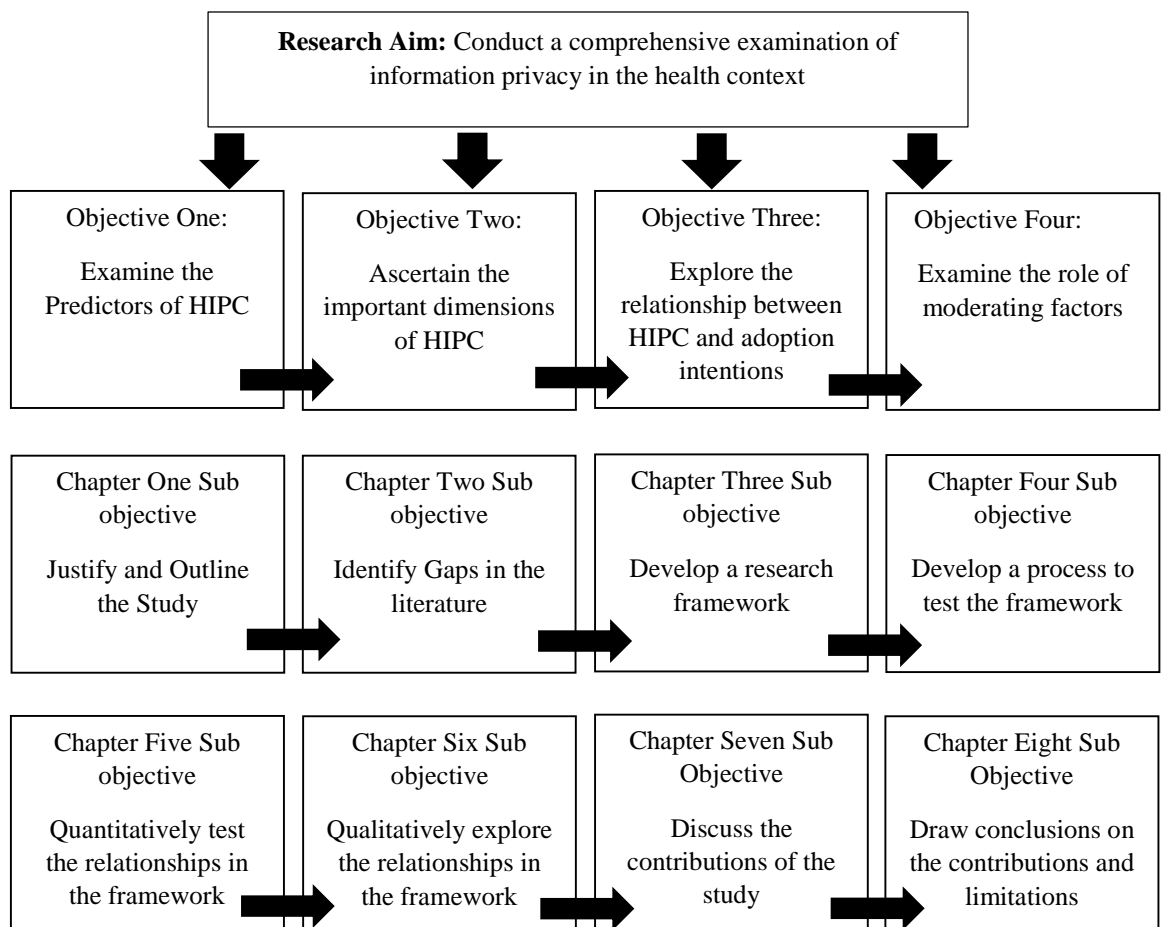
In the first stage, a preliminary study consisting of six exploratory interviews is conducted to test and refine the framework. The second stage of the study is explanatory and involves testing the relationships in the framework using a survey of 445 citizens in Ireland and the United States. In the final stage, these relationships are explored on a deeper level via in-depth interviews with 50 Irish and U.S. citizens. Following separate analysis, the quantitative and qualitative findings are integrated to deepen the understanding of information privacy in the health context. The findings provide strong empirical support for the influence of individual characteristics, perceptions, and experiences in shaping HIPC, and the use of a six dimensional measure of privacy concern. In addition, the integrated findings provide in-depth explanations of the complex relationships between HIPC, perceived benefits, and adoption intentions.

## 1.7 Dissertation Outline

The dissertation consists of eight chapters. Chapter One justifies the need for the research and details the study's objectives, research questions, and main hypotheses. The existing literature is reviewed in Chapter Two to identify gaps in our understanding of information privacy in the health context, and identify theories and constructs pertinent to addressing these gaps and holistically examining citizens' HIPC. Chapter Three builds upon the Literature Review chapter to present the proposed research framework and the hypotheses to be tested in the study. Chapter

Four discusses the philosophical assumptions underpinning this study and provides a detailed overview of the three-stage sequential mixed methods research design and the sampling procedures followed in each stage. Chapter Five presents the results from quantitative data analysis. The two models in the study are discussed individually with attention paid to reliability, validity, common method bias, and hypothesis testing using structural equation modelling (SEM). Chapter Six discusses the qualitative data analysis procedures and findings. The quantitative and qualitative findings are then integrated, and a number of meta-inferences are presented. Chapter Seven discusses the contributions of the study and presents the revised research framework along with several theoretical assumptions. The chapter also discusses the implications for practice. Chapter Eight draws conclusions on the contributions of the study and outlines the limitations inherent in the study and directions for future research. The structure of the dissertation in terms of the research aim, objectives, and the aim of each chapter is outlined below in Figure 1.3.

**Figure 1.3 Conceptual map of the Dissertation**



## CHAPTER TWO: LITERATURE REVIEW

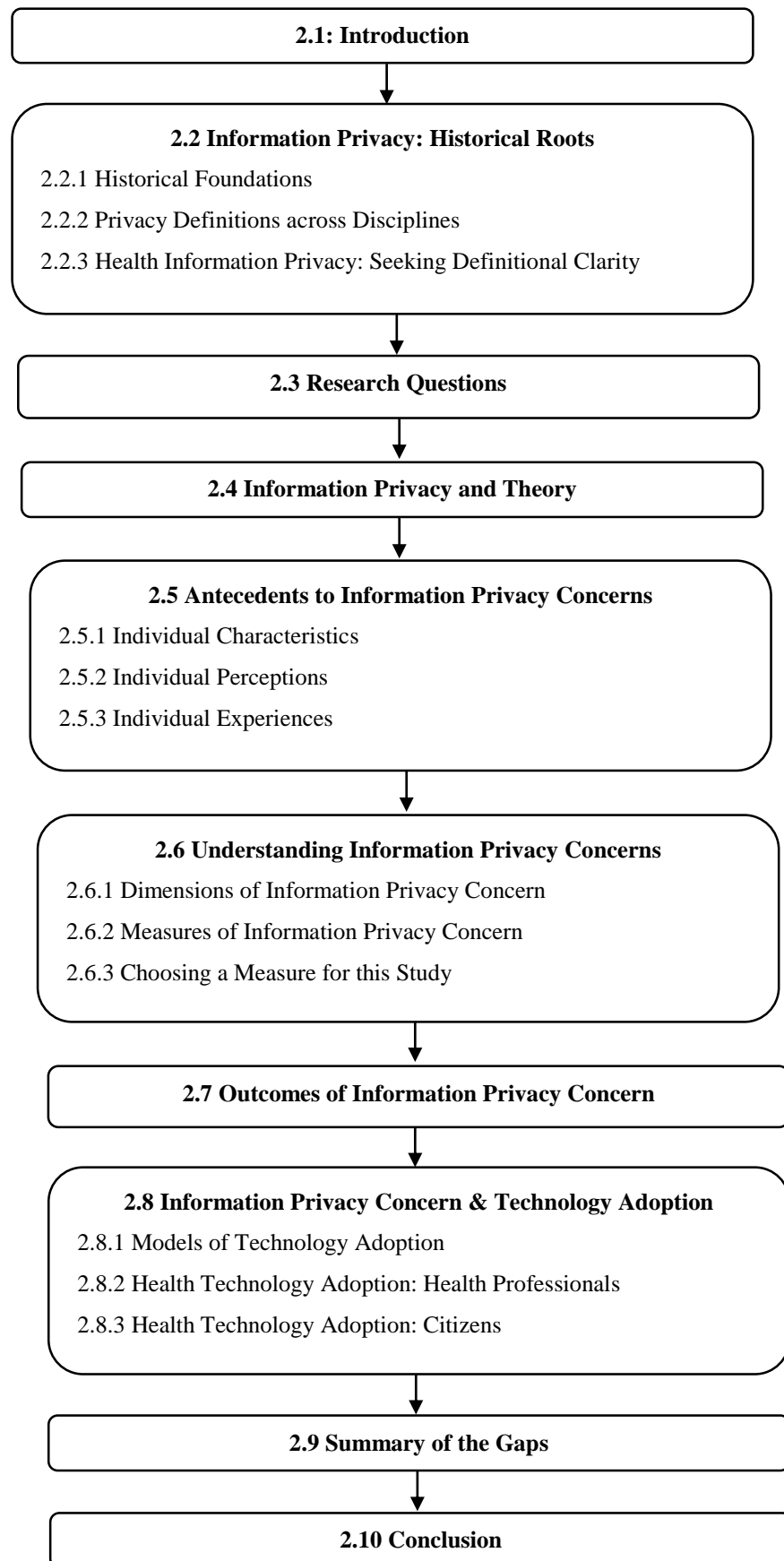
*Privacy: ‘a state in which one is not observed or disturbed by other people’*

*- Oxford English Dictionary*

### 2.1 Introduction

This chapter provides a review of the existing information privacy literature. The extant literature was reviewed with two aims. The first aim was to establish the current knowledge level and identify gaps in our understanding. The second aim was to determine what theories and constructs could be leveraged to address these gaps and answer the study’s research questions. The structure of this chapter is depicted below in Figure 2.1 (pg.12). The chapter begins by briefly reviewing the history of the information privacy construct. In order to identify an appropriate definition of information privacy for this study, the conceptualisations of privacy evidenced in various academic disciplines are discussed. The study’s research questions are then briefly restated. The relevant theories in the information privacy literature are reviewed to determine their relevance to the health context. The remainder of the chapter explores the existing literature under three broad sections related to the research questions: (1) the factors influencing information privacy concerns, (2) methods of measuring concerns, and (3) examining the relationship between information privacy concerns and technology adoption. The chapter concludes with a brief recap of the gaps in the literature.

**Figure 2.1 Chapter Structure**



## **2.2 Information Privacy: Historical Roots & Conceptualisations**

Privacy has been an issue of enduring concern across a wide variety of academic disciplines, and throughout history. Despite sustained interest, there are differing and conflicting perspectives on how to best define privacy. This section begins by tracing the historical roots of the privacy construct. The prevailing definitions of privacy across numerous academic disciplines interested in the phenomenon are then outlined. The section concludes by presenting and justifying the definition chosen for this study.

### **2.2.1 Historical Foundations**

The term ‘privacy’ stems from the Latin word *Privare*, meaning to separate (Zheng *et al.*, 2010). The history of privacy is difficult to pinpoint, due to the various contradictory accounts regarding the roots of the concept. Some believe the history of the issue is rooted in the writings of Greek philosophers throughout the 4<sup>th</sup> century B.C. (Newell, 1995, 1998). For instance, Aristotle described two spheres of activity that humans engage in: the public sphere, which pertains to political activities, and the private sphere of activities, which individuals engage in alone or in the presence of family (DeCew, 2002). Another view asserts that privacy dates back to Chinese philosophers in the 3<sup>rd</sup> century, who also developed a clear separation between one’s public and private self (Moore, 1984; Newell, 1995).

These early views of privacy relate to the individual’s physical environment. Information privacy, which is a subset of the overall privacy construct, forms the focus of this study (Bélanger and Crossler, 2011). While the concept of privacy in the physical world has been discussed for centuries; conversations among members of the public, increased presence in government policy, and research around information privacy can be traced back to the 1960s (Regan *et al.*, 2013). The period spanning 1961-1979 is described as the first era of contemporary privacy development (Westin, 2003). In recent decades, discussions and research around information privacy have sustained continuous growth. This is in part due to the increasing prevalence of the Internet and Information & Communication Technologies (ICTs). These technologies facilitate the collection



and sharing of copious volumes of information, which results in increased privacy concern, and greater organisational accountability with regards to managing personal information (Regan *et al.*, 2013). As a result, information privacy is often viewed as one of the key ethical issues facing the information age (Mason, 1986). Information privacy is still a relatively new research area, with all research conducted prior to the late 1990s categorised as early information privacy research (Conger, Pratt, and Loch, 2013). We are currently in the third era of contemporary privacy development (Westin, 2003), where individuals' information privacy concerns have reached all-time highs (Smith *et al.*, 2011).

### ***2.2.2 Privacy Definitions Across Disciplines***

Despite the large volume of privacy research, differing definitions persist across and within academic disciplines. In spite of efforts to reach a comprehensive definition of privacy, such a definition remains lacking (Hsu, 2006). The absence of a universally accepted definition is often attributed to the multidisciplinary nature of the privacy phenomenon and the differing lenses used to explore it (Pavlou, 2011). This study examines information privacy from the perspective of the Management Information Systems (MIS) discipline. As views within MIS have been influenced by other disciplines, the dominant views of these disciplines are outlined, prior to discussing MIS, and the definition chosen for this study.

#### ***2.2.2.1 Law: Privacy Definitions***

Privacy has attracted a great deal of attention within the Legal discipline over the past two centuries. There has been much debate surrounding how to best define privacy in terms of the appropriate level of legal protection afforded to citizens, organisations, and governments. The start of the privacy conversation within academia is often attributed to Warren and Brandeis' Harvard Law Review essay in 1890. They stated that despite individuals' entitlement to be left alone by the press, an element of public interest must also be considered. Warren and Brandeis are widely quoted across disciplines as defining privacy as individual's right '*to be let alone*' (Edney and Buda, 1976; Phelps *et al.*, 2000; Sheehan, 2002; Liu *et al.*, 2005). However, Warren

and Brandeis stated that while privacy protection fell under this broad right to be let alone, privacy was not an absolute right (Austin, 2003). Not all legal scholars agree on the right to privacy. For example, strong opposition against this view was presented by Prosser (1960), who claimed that all aspects of privacy law were protected under four separate, pre-existing torts. In arguing against Prosser, Moore (2003) stated that these torts are related, as they are each concerned with the control of personal information. He defines privacy as an individual's right to limit access to their physical being and personal information. Due to the complexities surrounding privacy in the legal sense, the Younger Committee Report (1972) concluded that privacy could not be defined in legal terms. Thus the search for one definition in this discipline has ceased. While questions remain regarding the ideal amount of privacy to be legally afforded to citizens, the consensus agrees that there is a need to balance the privacy rights of the individual, with the greater need of society (Hughes, 2012), and the information needs of organisations and governments.

#### 2.2.2.2 *Psychology: Privacy Definitions*

Privacy has also garnered a great deal of attention in the Psychology discipline. Two of the most notable contributions in this area and across the realm of privacy research were made by Alan Westin and Irwin Altman. Westin (1967) defined privacy as the claim of individuals to decide what information about themselves is known by others. This definition has been used in other disciplines such as Marketing (e.g. Bellman *et al.*, 2004). Altman (1975) defined privacy as the selective control of access to the self. Both definitions assume individuals have the ability to control or regulate their privacy. In addition, both Altman and Westin stressed the importance of this control, asserting that the ability to limit or open access to oneself in different situations is imperative to an individual's self-definition (Altman, 1975,1977). This represents the majority view in the Psychology discipline, that privacy is a vital element of a human's development (Jourard, 1964; Edney and Buda, 1976).

#### 2.2.2.3 *Privacy Economics: Definitions*

In recent decades, Privacy Economics has emerged as a stream of literature, which aims to understand the benefits and costs of information disclosure to individuals and institutions

(Acquisti, 2009). Within this discipline, privacy has been described as ‘the concealment of information’ (Posner, 1981, p. 405), and the restriction of the use and collection of information pertaining to an individual (Stigler, 1980). In Privacy Economics, privacy is viewed as a commodity, which individuals are willing to trade or sell in return for benefits. It has also been argued that information asymmetry exists and individuals are privately aware of their preferences for privacy and the price they require to disclose information (Chellappa and Sin, 2005). Furthermore, Posner (1981) argued that the concealment of information only benefits individuals with something to hide. The commodity-based view of privacy, and the negative connotation inherent in this discipline conflicts with other disciplines such as Law and Psychology, where scholars stress the importance of preserving individuals’ privacy.

#### *2.2.2.4 Marketing: Privacy Definitions*

Privacy research has also grown in importance within the Marketing discipline in recent decades. This can be partly attributed to the copious volume of information about customers collected by marketers for purposes such as personalising services and understanding customers’ preferences. This data collection often increases customers’ concerns for their privacy (White, 2004). Privacy in Marketing has been defined as a consumer’s ability to control the physical presence of others and the dissemination of their information during commercial transactions (Goodwin, 1991). Control is at the centre of many definitions in this discipline, with the majority believing that consumers should have some degree of control over their personal information. For example, Culnan and Armstrong (1999) asserted that individuals have the right to control how information about them is used in a marketing context. This perspective is also echoed by Brown and Muichra (2004), who argued that individuals have the moral right not to be monitored by organisations. Within the Marketing discipline, it is agreed that some degree of information collection occurs in commercial transactions. However, questions remain regarding how much control consumers should have over their personal information.

#### 2.2.2.5 Privacy: The Need for Definitional Clarity

Defining the privacy construct has presented difficulties across all disciplines. However, within each discipline, there tends to be a majority view in favour of one perspective, albeit not a precise definition. These views are categorised as value-based and cognate-based definitions, in line with Smith *et al.*, (2011). Table 2.1 provides an overview of the prevailing definition in each discipline. These views are briefly reviewed, prior to discussing the definitions dominating the MIS discipline, and choosing a definition for this study.

**Table 2.1 Privacy definitions across disciplines**

View	Discipline	Perspective	Description	Limitation of this view
<b>Value Based views</b>	<i>Law</i>	Privacy as a right	Individuals have a right to privacy, which must be balanced with the public interest.	Difficulty in defining the right to privacy in legal terms has led to inconsistencies in court rulings on privacy cases (Gerety, 1977).
	<i>Economics</i>	Privacy as a commodity	Privacy is a commodity which can be bought, traded, and sold.	Assumes individuals always act rationally when deciding what information to disclose.
<b>Cognate Based views</b>	<i>Psychology</i>	Privacy as a state	Privacy is achieved when an individual selectively controls access to themselves.	Assumes individuals can control physical access to themselves and others will respect their desire for privacy.
	<i>Marketing</i>	Privacy as a right to control	Privacy is an individual's right to control physical access to themselves and access to their personal information during commercial transactions	Assumes individuals can exercise control over their information disclosure.

Value-based definitions include the *privacy as a right* and *privacy as a commodity* views predominately discussed in the Law and Privacy Economics disciplines. In the legal discipline, the majority believe that individuals have a right to privacy free from intrusion. While this view was originally focused on a right to physical privacy, it has been applied to information contexts, such as the Internet context (e.g. Liu *et al.*, 2005). However, this view has also received criticism. The commodity view of privacy, which stems from Privacy Economics research, argues that privacy is traded and sold by individuals upon completion of a cost-benefit analysis. It is argued

that viewing privacy merely as a commodity, is severely limiting as it assumes individuals can exercise complete control over the disclosure of their personal information, that individuals are always aware of how much information they wish to disclose, and that individuals will always be influenced by the benefits on offer when making disclosure decisions.

Cognate-based definitions include *privacy as a state* and *privacy as control* definitions. Within the Psychology discipline, privacy is widely viewed as a state which is pivotal to self-development and growth (Jourard, 1964; Westin, 1967; Altman, 1975). For instance, Westin (1967) discussed four states of privacy: anonymity, solitude, intimacy, and reserve. A myriad of privacy definitions across disciplines encompass the *privacy as a state* view, although many of these definitions are combine other elements such as control (Dinev *et al.*, 2012). One primary limitation associated with defining *privacy as a state*, relates to descriptions of privacy as a dichotomous event, assuming that individuals either have privacy or do not. The privacy as a control view is also largely influenced by Westin and Altman, and is the dominant view within the Marketing discipline, where control relates to information collected about an individual and used in marketing communications. The control-based view has also received critique, as it assumes individuals can control their privacy in a physical and informational sense.

### ***2.2.3 Health Information Privacy: Seeking Definitional Clarity***

As evidenced in the preceding sections, there is great variety in how privacy is defined. Many of these definitions initially pertained to privacy in a physical sense, but maintain relevance in the information context. Each prevailing view can also be critiqued. A comprehensive definition of privacy may be unobtainable, due to the many different lenses privacy is examined under (Pavlou, 2011). It is thus argued that researchers should chose the definition of privacy most relevant to their research question, and the context of their study. The MIS and Health Informatics literature were reviewed to determine how privacy is defined in these disciplines. The majority of privacy studies in the Health Informatics literature do not offer new definitions of privacy, nor do they adapt existing definitions. Indeed, many of these studies fail to clearly define privacy. In their

systematic literature review, Shaw *et al.*, (2011) noted that none of the 21 existing health privacy studies provided an unambiguous definition of privacy, with many failing to distinguish between privacy and similar but distinct concepts, such as security and confidentiality. These definitions are troublesome, as security relates to technical measures in place to protect data (King *et al.*, 2012), whereas privacy relates to individuals' perceptions, rights, and desire to control data collection and usage. Thus it was necessary to adapt a definition from the MIS literature.

Definitions in the MIS discipline draw heavily from the *privacy as a right* and *privacy as control* views. Scholars within this discipline do not assume individuals have an absolute right to privacy, or the ability to control. In contrast, scholars argue that individuals *should* be able to exercise some control over organisations' use of their information (Clarke, 1999). Based on Clarke's assertions, Bélanger & Crossler (2011) define information privacy as an individual's desire to have more control over the collection and dissemination of their personal information. This definition overcomes the weaknesses of control based views as it does not imply that individuals currently have control over the information they disclose, nor that they desire complete control, but argues that they desire greater control. This definition is adapted to the health context, with information privacy defined as: *the desire of citizens' to be afforded a **degree of control** over the **collection and dissemination** of their **personal health** information by **health organisations** and **technology vendors***. This definition is used throughout the remainder of this chapter and thesis when referring to privacy or information privacy.

## 2.3 Research Questions

Prior to discussing the existing literature, it is important to restate the study's research questions. This study aims to develop a comprehensive understanding of citizens' health information privacy concerns (HIPC). The study addresses this broad aim under three research questions:

RQ1: What are the factors that influence HIPC?

RQ2: What dimensions of information privacy concern are most influential in the health context?

RQ3: Does HIPC influence citizens' acceptance and adoption of Health ICTs?

In order to develop an approach to answer these questions, the privacy literature in the MIS and Health Informatics disciplines was reviewed to identify relevant theories and explore gaps in current understanding.

## **2.4 Information Privacy and Theory**

To date, a number of theories have been leveraged to examine information privacy in the MIS discipline. Indeed, several studies have leveraged more than one theory, as some theories explain the factors predicting concern, while others seek to understand the outcomes of concern (Li, 2012). In contrast, many studies in the Health Informatics discipline lack guiding theoretical foundations (Or and Karsh, 2009). It is acknowledged that the sensitive nature of health data may necessitate unique theorising or the adaption of existing information privacy theories (Agarwal *et al.*, 2010). Thus, this section reviews existing theories to determine which theories can be leveraged to explain the role of citizens' information privacy concerns in the health context. Based on the work of Li (2012), who reviewed all theories in the information privacy literature, existing theories are discussed across five categories:

1. Theories related to the origin of privacy concerns
2. Theories related to institutional factors
3. Theories related to individual factors
4. Theories related to the behavioural outcomes of privacy concerns
5. Theories related to the trade-offs between privacy concerns and behaviour

Theories in each category are briefly outlined, prior to a discussion on the relevance of these theories to health information privacy and this study.

### **2.4.1 The Origin of Privacy Concerns**

Agency theory and Social Contract theory have been utilised in the existing literature to explain the origins of privacy concern (Li, 2012). Agency theory has been applied in several disciplines,

and relates to the issues arising within the transactional relationships between principles (customers) and agents (e.g. organisations), such as the agent pursuing their own interests as opposed to principles' interests (Eisenhardt, 1989). In the information privacy context, organisations collect customers' data during transactions and may use this data for their own purposes, leading to privacy risks. Thus, customers must decide whether or not to engage in these transactions and how to limit these privacy risks (Li, 2012). To date, Agency theory has been applied in a small number of information privacy studies. For example, Pavlou *et al.*, (2007) found that information privacy concerns increased individuals' uncertainty perceptions, and as a result reduced purchases of both books and prescription medication.

Social Contract theory posits that when organisations engage in transactions with customers, they also enter into a social contract. This contract implies that organisations can only use the individual's data in accordance with social norms, and that individuals have some level of control (Bélanger and Crossler, 2011). This theory assumes that individuals will enter into a social contract with an organisation once they perceive that the benefits of this relationship outweigh the risks (Donaldson and Dunfee, 1994). Social Contract theory has been harnessed in a number of information privacy studies including Malhotra, Kim and Agarwal (2004), Okazaki, Li, and Hirose (2009), Li Sarathy, and Xu (2010). In addition, Bansal, Zahedi, and Gefen (2010) empirically tested the assumptions of Social Contract theory in the health context. They provided support for the positive influence of privacy invasion experience on concern, but the proposed negative influence of privacy concern on trust in health websites was not supported.

These theories have been leveraged when developing privacy concern scales (Malhotra *et al.*, 2004), and to explain the relationship between privacy invasion and privacy concern (Bansal *et al.*, 2010). However, it is argued that these theories are not relevant to the current study for three reasons. Firstly, these theories are best used to explore relationships with a given organisation. This study focuses on citizens' adoption of health technologies and their views towards health professionals and technology vendors in a general sense. Secondly, Social Contract theory relates to social norms of how data *should* be treated and not how the data *is* actually treated. This study



focuses on the latter, and explores citizens' perceptions and concerns regarding the collection and use of their health data. Lastly, despite the interesting insights these theories provide into the origins of concern, neither theory provides an adaptable framework for studying the role of privacy in a given context (Li, 2012).

#### **2.4.2 *Institutional Factors and Concern***

Institutional factor theories include Procedural Fairness, Social Presence, and Social Response theory. Procedural Fairness theory posits that individuals will disclose personal information if they believe there are fair procedures in place to protect their information (Culnan and Armstrong, 1999). Fair procedures are often represented by privacy policies or privacy legislation (Li, 2012). Social Presence theory proposes that Internet privacy concerns can be reduced by increasing the social presence or 'real life feel' of websites (Li, 2012). These assumptions have received mixed support in the existing literature. Social response theory promotes reciprocity, and hypothesises that individuals will share data in response to disclosure from another individual or the organisation (Li, 2012). Institutional theories are deemed irrelevant to this study for three reasons. Firstly, they have a tendency to focus on online communications between an individual and a website, which is not the focus of this study. Secondly, these theories focus on interventions such as privacy policies to reduce privacy concerns. This again is not pertinent to the focus of this study on understanding the relationship between HIPC and adoption. Thirdly, these theories have received mixed results to date, and have not been explored in the health context.

#### **2.4.3 *Individual Factors and Concern***

Theories which focus on the influence of individual factors on privacy concerns include Protection Motivation theory, Information Boundary theory, and Personality theories. Protection Motivation Theory (PMT) was developed by Rogers (1975) to examine how fear appeals influence individuals' health behaviours. The theory is comprised of two broad elements; threat and coping appraisals. PMT posits that individuals' behavioural reactions are influenced by their threat appraisal, formed from their perception of the breadth and severity of risks, and the

perceived likelihood these risks will occur. Individuals' coping appraisal relates to their perceived ability to take action to minimise these threats (Rogers, 1975). Several components of PMT have been applied in information privacy studies. For example, Xu *et al.*, (2011) found that individuals' perceived privacy risk and control influenced their privacy concerns, thus providing support for the role of threat appraisal and coping appraisal.

The second theory, Information Boundary theory (IBT) is often referred to as Communications Boundary Management theory (CPM). This theory states that individuals develop personal boundaries to determine what information they are willing to share, and the circumstances under which they are willing to disclose (Li, 2012). When information one is not willing to share is requested, this may lead to privacy concerns (Petronio, 1991; Metzger, 2007). This theory has been applied in a number of information privacy studies. For instance, Rohm and Milne (2004) found that individuals expressed higher concerns for health information, due to its sensitivity. This provides empirical support for the role of personal boundaries, and the link between sensitive information and privacy concerns.

Personality theories propose that personality traits influence individuals' privacy concerns and related behaviours. Numerous researchers have explored the influence of personality on privacy concern including Smith, Milberg, and Burke (1996), Korzaan and Boswell (2008), and Junglas *et al.*, (2008). In the context of information privacy concerns, both Korzaan and Boswell, and Junglas *et al.*, (2008) explored the influence of the big five personality traits, yielding conflicting findings. While Korzaan and Boswell found that agreeableness positively influenced concerns, Junglas *et al.* found that agreeableness reduced concern. In addition, conscientiousness had a positive influence in the study conducted by Junglas and colleagues, but was insignificant in Korzaan and Boswell's study. In the health context, Bansal *et al.*, (2010) found that emotional instability increased perceived sensitivity, agreeableness had a slightly positive influence on sensitivity, and intellect had a negative influence on sensitivity.

Theories focusing on the role of individual factors are popular in the existing literature as they provide interesting insights into the factors influencing concerns. In terms of PMT, Li (2012)

argues that threat and coping appraisals represent the foundations of individuals' privacy concerns. Threat and coping appraisals can be represented using various variables. Information Boundary theory provides insights into the influence of perceived sensitivity on individuals' information privacy concern. Due to the flexibility of PMT and the importance of sensitivity in the health context, PMT and IBT are deemed relevant to this study. Based on the mixed findings, personality traits are ruled out from this study.

#### ***2.4.4 Privacy Concern and Behavioural Outcomes***

Various theories have been utilised in the information privacy literature to explore the behavioural outcomes of concerns (Bélanger and Crossler, 2011). These theories are predominately adopted from the technology adoption literature and include the theory of Reasoned Action (TRA), the theory of Planned Behaviour (TPB), and the Unified theory of Acceptance and Use of Technology (UTAUT). Technology adoption theories such as TRA posit that individuals' behaviours are influenced by their intentions, which are formed from their salient beliefs and attitude toward the behaviour (Fishbein and Azjen, 1975; Azjen and Fishbein 1977). Information privacy studies have supported the negative influence of privacy concerns on individuals' attitudes towards social networking sites (Shin, 2010), online purchasing frequency (Phelps, D'Souza, and Nowak, 2001), and willingness to interact with an online organisation (Malhotra *et al.*, 2004). In the health context, privacy concerns have been found to negatively impact individuals' intentions to opt-in to an Electronic Health record (EHR) (Angst and Agarwal, 2009), and attitudes towards an EHR (Dinev *et al.*, 2016). These studies offer strong support for the relationship between concern and technology adoption in many contexts (Li, 2012). Technology adoption theories are pertinent to addressing the study's third research question, and explaining the relationship between citizens' HIPC and their adoption of health technologies.

#### ***2.4.5 Exploring the Trade-Offs***

A number of theories have been leveraged to explain the trade-offs facing individuals. These include the Privacy Calculus theory (PCT), which posits that individuals are willing to provide

an organisation with their personal information for as long as the perceived benefits outweigh the perceived risks or consequences (Culnan, 1993). This theory states that in order to make information disclosure decisions, individuals conduct a cognitive cost-benefit analysis, considering the benefits of disclosure and the potential negative outcomes or repercussions the individual might experience (Culnan and Armstrong, 1999; Li, Sarathy, and Xu, 2010). Information privacy studies leveraging PCT have examined a number of factors, illustrating the multiple interpretations of PCT (Li, 2012). These studies support the underlying foundations of PCT, showing that factors such as privacy concerns and risks can reduce intentions, and benefits can increase intentions. For instance, in a recent study, privacy risk reduced intentions towards wearable health devices, while perceived benefits increased intentions (Guo et al., 2013).

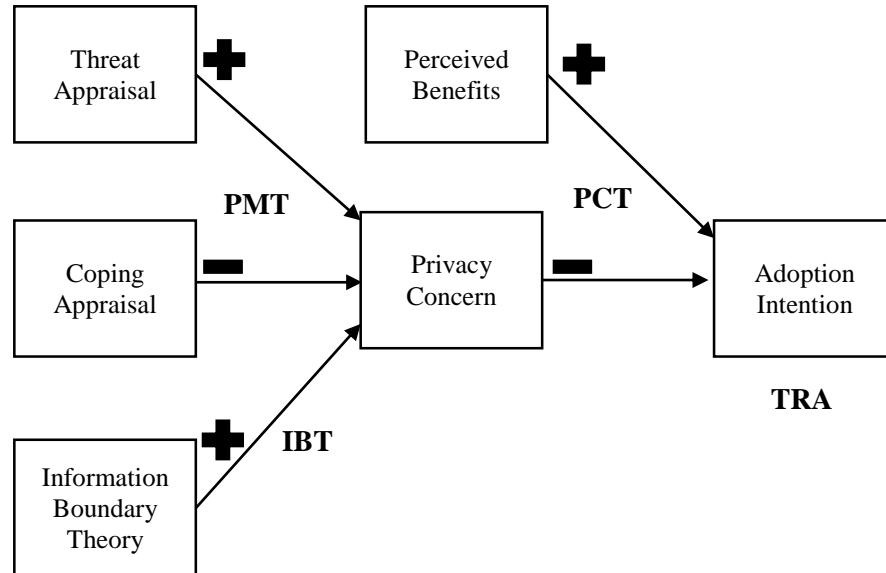
Expectancy Value theory is often harnessed in information privacy studies to examine the trade-offs between individuals' salient beliefs and privacy-related behaviours. Expectancy Value theory provides the foundation for technology adoption theories such as TRA, as it assumes that individuals' behaviours are influenced by their salient beliefs. Thus Expectancy Value theory is often utilised in conjunction with the Privacy Calculus theory. The combination of these two theories provides a flexible foundation for examining the influence of individuals' perceptions on their technology adoption decisions (Li, 2012). These theories are deemed relevant to this study.

#### ***2.4.6 Developing a Theoretical Framework***

Following his review of the existing theories, Li (2012) presented an integrative theoretical framework to guide future privacy research. He asserted that technology adoption theories such as TRA, and the underlying Expectancy Value theory, combined with the Privacy Calculus theory, provide a strong theoretical foundation for examining the negative influence of privacy concerns on technology adoption, and a flexible means for investigating the influence of competing beliefs such as perceived benefits and privacy concerns on adoption intentions. Theories such as Protection Motivation theory (PMT) and Information Boundary theory (IBT) are useful for explaining the drivers of privacy concerns. Based on the assertions of Li (2012),

empirical support, and relevance to the health context, several theories are leveraged in this study. These theories are depicted in Figure 2.2 below, and briefly reviewed.

**Figure 2.2 Theories included in this Study**



Information Boundary theory and Protection Motivation theory are harnessed to explore the antecedents to HIPC in this study. IBT posits that individuals develop boundaries to determine what data they are willing to disclose, and often express higher concerns regarding data they are not willing to disclose (Petronio, 1991). Using this theory, the boundaries individuals create around their health data can be explored, as well as the interplay between these boundaries and HIPC. PMT argues that individuals consider the breadth and severity of threats to their data to determine their own vulnerability, as well as reflecting on their abilities to cope with these threats. PMT enables the investigation of individuals' threat perceptions with regards to their health data, and factors which reduce these threats. Lastly, Privacy Calculus theory is leveraged to explore the influence of individuals' HIPC and perceived benefits on their health technology adoption. Together these theories are underpinned by the assumptions of TRA and Expectancy Value theory, and posit that individuals' perceptions (IBT and PMT) influence their attitudes (HIPC). Both HIPC and perceived benefits influence individuals' intentions. These underlying foundations bare resemblance to the overarching APCO (Antecedents → Privacy Concerns → Outcomes) framework presented by Smith *et al.*, (2011) for comprehensively examining privacy

in a given context. In order to develop an approach to investigate privacy in this study, the empirical findings of previous studies are examined. These findings are discussed under the headings of APCO, focusing first on the antecedents to privacy concerns, followed by the methods used to measure privacy concerns, and the outcomes of concern.

## **2.5 Antecedents to Information Privacy Concern**

In line with the first research question, antecedents are described as the factors influencing individuals' HIPC. Understanding the antecedents is fundamental to developing methods to address privacy concerns (Phelps *et al.*, 2001). Antecedents to information privacy concerns in general, and in the health context are included in this discussion. Each antecedent is reviewed to determine its relevance to this study. To date, a myriad of antecedents have been examined in the MIS literature, and a smaller number have been explored in the Health Informatics literature. Based on recent categorisations, the antecedents are reviewed across three broad categories: (1) individuals' characteristics, (2) perceptions, and (3) experiences (Li, 2011; Smith *et al.*, 2011).

### **2.5.1 Individual Characteristics**

The role of individual characteristics has been examined in a host of studies across various contexts. This section reviews the findings regarding the influence of several individual characteristics including; gender, age, income, and education.

#### **2.5.1.1 Gender as an Antecedent**

Gender has been explored in a number of studies in the MIS and Health Informatics literature. These studies use varying conceptualisations of privacy and differing measures of privacy concern, but share one commonality; they all hypothesise that females will express higher privacy concerns. The findings of these studies are outlined in Table 2.2. below.

**Table 2.2 Gender and Privacy**

Study	Context	Findings		
		Women have statistically higher privacy concerns	Men have statistically higher privacy concerns	No statistical differences
Sheehan (1999)	Internet	X		
Phelps <i>et al.</i> , (2000)	Internet			X
Janda & Fair (2004)	Internet	X		
Bellman <i>et al.</i> , (2004)	Internet	X		
Yao <i>et al.</i> , (2007)	Internet			X
Youn (2009)	Internet	X		
Nehmad & Fogel (2009)	Internet	X		
Laric <i>et al.</i> , (2009)	Health	X		
Hoy & Milne (2010)	Internet	X		
Joinson <i>et al.</i> , (2010)	Internet	X		
Hwang <i>et al.</i> , (2012)	Health			X
Vodicka <i>et al.</i> , (2013)	Health	X		

As shown above, the findings on the role of gender are mixed. The majority of studies found that gender had a significant influence on privacy concern. Females expressed higher concerns for the privacy of their information in many contexts, including on social networking sites (Fogel and Nehmad, 2009; Hoy and Milne, 2010) and on the Internet (Sheehan, 1999; Joinson *et al.*, 2010). A small number of studies found that gender did not significantly influence privacy concern (Yao *et al.*, 2007). Findings in the health context are also mixed. For instance, Laric *et al.*, (2009) found that females in the United States and Canada expressed higher privacy concerns regarding a number of health data types, but Hwang *et al.*, (2012) found that gender did not have a significant influence on the information privacy concerns of Taiwanese citizens. The information privacy literature offers potential explanations for conflicting findings. For example, males have been found to be more likely to engage in behaviours to protect their privacy such as falsifying data disclosed online (Chen and Rea, 2004), and using privacy-preserving technology solutions (Joinson *et al.*, 2010). Thus, men may express lower privacy concerns because they believe these behaviours protect their privacy. It is argued that due to the support offered by the majority of studies, gender is an important factor to consider when examining HIPC. There is a need for further research to explore the influence of gender in the health context among other samples, and to clarify the reasons behind mixed findings.

### 2.5.1.2 Age as an Antecedent

Age has also been examined in numerous information privacy studies across various contexts including health. These studies utilised differing measures of privacy concern, but all proposed that age would have a positive influence, with older individuals expressing higher privacy concerns. The findings of these studies are illustrated in Table 2.3 below.

**Table 2.3 Studies Exploring Age as an Antecedent**

Study	Context	Findings	
		Age significantly influences concern	No statistical differences
Phelps <i>et al.</i> (2000)	Internet		X
Chen <i>et al.</i> (2001)	Internet	X	
Sheehan (2002)	Internet	X	
Bellman <i>et al.</i> (2004)	Internet	X	
Janda and Fair (2004)	Internet	X	
Laric <i>et al.</i> (2009)	Health	X	
Zhang <i>et al.</i> (2002)	Internet	X	
Joinson <i>et al.</i> (2010)	Internet	X	
Ji & Lieber (2010)	Internet	X	
Tsai <i>et al.</i> (2011)	Internet		X
Hwang <i>et al.</i> (2012)	Health		X
King <i>et al.</i> (2012)	Health	X	
Kordzadeh <i>et al.</i> (2016)	Health	X	

As evidenced above, several studies support the hypothesised positive influence of age on concern in the Internet context (e.g. Janda and Fair, 2004; Joinson *et al.*, 2010). However, some of these studies only provide partial support. For instance, in Chen *et al.*, (2001) age only significantly influenced concerns regarding credit card misuse among individuals with no online purchasing experience. In addition, Zhang *et al.*, (2002) found that age positively influenced concern among U.S. respondents, but was negative among Chinese respondents, thus suggesting the influence of age may vary across nationalities. Furthermore, in a small number of studies, age did not have a significant influence (Tsai *et al.*, 2011). This adds to the murkiness surrounding the role of age.

In the health context, the findings are also mixed. One Taiwanese study found that age did not have a significant influence on privacy concerns (Hwang *et al.*, 2012). In contrast, in Laric *et al.*, (2009), older respondents expressed higher concerns regarding the privacy of several health data types. Partial support was offered by Kordzadeh *et al.*, (2016), who found that age positively



influenced concern among individuals who were not members of virtual health communities, but was insignificant among members. In addition, an Australian study offered some support, revealing that age positively influenced privacy concerns up to a certain age, but individuals aged 60 and above expressed lower concerns (King *et al.*, 2012). This echoes the findings of Sheehan (2002), who found that older individuals either expressed very high or very low concerns. Despite the mixed findings, it is widely argued that age influences individuals' information privacy concerns (Li, 2011). Further empirical investigation is required to clarify the influence of age in the health context, and to explain the reasons underlying this influence.

#### 2.5.1.3 Additional Demographic Variables as Antecedents

The education level and income level achieved by the individual have been examined to a lesser degree in the literature. The table below outlines the findings of these studies.

**Table 2.4 Additional Demographic Variables**

Study	Context	Findings			
		Education: Significant differences	Education: No statistical differences	Income: Significant differences	Income: No statistical differences
Phelps <i>et al.</i> (2000)	Internet	X			X
Chen <i>et al.</i> (2001)	Internet		X		X
Zhang <i>et al.</i> (2002)	Internet		X	X	
Hwang <i>et al.</i> (2012)	Health		X	-	-
Rogith <i>et al.</i> (2014)	Health		X	-	-

In terms of education, Phelps *et al.*, (2000) provided support for a negative correlation with college graduates expressing the lowest level of privacy concern. The influence of education was not supported in other studies, including those in the health context. With regards to income level, Zhang *et al.*, (2002) found it had a positive, significant influence on information privacy concerns among Chinese respondents, but had an insignificant influence among U.S. respondents. In addition, income level was not significant in the other studies, and has not been explored in the

health context. Based on these findings, it is argued that education and income are unlikely to have a strong influence on individuals' HIPC.

#### **2.5.1.4 Health Status as an Antecedent**

Many researchers have asserted that individuals' health status will influence their health information privacy concerns. However, the nature and direction of this influence is the subject of much debate. Some researchers argue that individuals of poorer health status will be less concerned for privacy, due to the benefits offered by health technologies (e.g. Angst and Agarwal, 2009). In support of this assertion, Lafky and Horan (2011) found that individuals with chronic illnesses were more willing to disclose health data. In addition, the findings of Koradezah *et al.*, (2016) offer partial support, as poor health status reduced HIPC among non-members of virtual health communities, but not among existing members. On the other hand, some researchers assert that poor health status will increase HIPC, as these individuals may have more detailed, sensitive health records (Flynn *et al.*, 2003). In line with this view, Bansal *et al.*, (2010) found that poor health status increased sensitivity perceptions and indirectly impacted HIPC as a result. In addition, studies have shown that individuals with sensitive illnesses such as mental health conditions and HIV express extremely high privacy concerns (Flynn *et al.*, 2003; van Heerden *et al.*, 2013). There is an apparent need to further explore the influence of individuals' health status on their HIPC, and a need to ascertain if different conditions have differing influences.

### **2.5.2 Individual Perceptions**

A myriad of factors representing individuals' perceptions have been examined in conjunction with Protection Motivation theory, Privacy Calculus theory, and Information Boundary theory. This section discusses these perception-based factors and their relevance to this study.

#### **2.5.2.1 Perceived Sensitivity as an Antecedent**

Perceived sensitivity relates to individuals' views of how sensitive certain data types are. In line with Information Boundary theory, it is assumed that individuals will express higher privacy concerns regarding information they view as sensitive (Petronio, 1991). In the MIS literature,

several studies show that individuals express higher privacy concerns regarding personally identifiable information (Ward *et al.*, 2005), and information they view as sensitive (Andrade *et al.*, 2002). Financial and health data are widely described as sensitive (Malhotra *et al.*, 2004). However, individuals may also view certain health data types as more sensitive than others. For instance, Caine and Hanania (2013) examined individuals' willingness to share different types of information stored in their EHRs, and found that individuals were less willing to share sensitive information such as information pertaining to genetics, mental health, reproductive health, and substance abuse. While this study didn't relate directly to privacy concerns, it illustrates the relevance of sensitivity perceptions.

The relationship between perceived sensitivity and HIPC has been explored in one U.S. study, which provides empirical evidence for the positive relationship between perceived sensitivity of health data and HIPC (Bansal *et al.*, 2010). In a similar vein, perceived sensitivity has been shown to increase individuals' perceptions of the risks associated with wearable health devices (Li *et al.*, 2016). Due to the undisputed sensitivity of health data, and the assertions that this sensitivity increases privacy concerns (Dinev *et al.*, 2016), it is argued that perceived sensitivity is of the utmost relevance in this context. There is a need to directly examine the influence of perceived sensitivity on HIPC among a non-U.S. sample to confirm this relationship.

#### 2.5.2.2 *Perceived Trust as an Antecedent*

Trust has attracted a great deal of attention in the information privacy literature. Trust is often explored across three dimensions: competence (belief that the trustee is capable of providing a service), benevolence (belief that the trustee acts in the individuals' best interest), and integrity (belief that the trustee is honest) (McKnight *et al.*, 2002). High perceived trust in the trustee's benevolence and integrity is likely to manifest in low privacy concerns (McKnight *et al.*, 2002). The existing literature supports the negative influence of trust on concern. For instance, Pavlou *et al.*, (2007) found that trust reduced individuals' privacy concerns associated with online purchasing of books and prescription medication. In addition, in an Australian study, trust reduced individuals' privacy concerns when interacting with financial organisations (Tsarenko

and Tobjib, 2009). A number of studies in the MIS literature have examined trust as an outcome of privacy concern as opposed to an antecedent. These studies also support the negative association between trust perceptions and concern. For example, high privacy concerns regarding one's information online reduced trust in online organisations (e.g. Malhotra *et al.*, 2004; Hong and Thong, 2013). Trust has also been positioned as a potential mediator of the concern-intention relationship (Korzaan and Boswell, 2008; Guo *et al.*, 2013). The measurement of trust as an antecedent, outcome, and mediator has led to confusion regarding its relationship with privacy concern across all contexts including health. There is a need for further investigation to clarify the role of trust (Li, 2011).

It is argued that trust represents an antecedent to HIPC in this study for three reasons. Firstly, this study is interested in understanding how individuals' perceptions shape their privacy concerns. The potential predictive influence of trust on citizens' HIPC is thus of great interest. Secondly, trust is viewed as paramount in the health context, where it is positioned and examined as an antecedent. For instance, researchers have posited that trust in health professionals could reduce HIPC (Rahim *et al.*, 2013). In addition, trust in EHR vendors has been empirically shown to reduce HIPC (Dinev *et al.*, 2016). Moreover, one study which examined trust as an outcome of concern in the health context, found that this relationship was not supported (Bansal *et al.*, 2010). Thirdly, while the study conducted by Dinev *et al.*, (2016) supports the relevance of trust in this context, there is a need for further examination (1) to clarify the influence of trust in technology vendors in a broad sense, and (2) to determine the role of trust in health professionals.

#### 2.5.2.3 *Perceived Risk as an Antecedent*

Perceived risk encompasses many dimensions including performance risk, financial risk, time risk, psychological risk, and social risk (Cunningham, 1967), along with the new privacy risk dimension (Featherman and Pavlou, 2003). In this study, perceived risk is described as an individual's expectation that disclosing health information to a particular organisation will result in a negative outcome (Featherman and Pavlou, 2003; Dinev *et al.*, 2012). Numerous information privacy studies have examined the influence of perceived risk, often in conjunction with trust.

These studies all propose that perceived risk will have a positive influence on individuals' information privacy concerns (Hong and Thong, 2013). In the MIS literature, studies have explored slightly different risk variables. For instance, Youn (2009) examined the influence of perceived risk of disclosure, while others (Okazaki *et al.*, 2009; Xu *et al.*, 2011) explored perceived risk of loss in a broad sense, and perceived risk of loss on the Internet (Dinev and Hart, 2006). Despite the differences in naming conventions and focus, all of these studies found that perceived risk increased individuals' information privacy concerns. Perceived risk has also been investigated as an outcome of privacy concern in a small number of studies. These studies focused on risks associated with disclosing data to online organisations, and support the positive association between perceived risks and concerns (Malhotra *et al.*, 2004; Hong and Thong, 2013).

The use of different variables to measure risk perceptions coupled with the uncertainty surrounding whether perceived risk is an antecedent or outcome of privacy concern, obfuscates our understanding of the influence of risk perceptions. It is argued that perceived risk represents a pertinent antecedent to HIPC for three reasons. Firstly, while the influence of perceived risk on HIPC has not been directly examined, existing literature suggests this relationship will be salient. For instance, Xu *et al.*, (2011) found that perceived risk had a positive impact on information privacy concerns towards health websites. In addition, research has shown when individuals believe there is a risk of a privacy breach, they express high concerns for their information in EHRs (Simon *et al.*, 2009). Secondly, many researchers have highlighted the relevance of risk perceptions. For instance, Fichman *et al.*, (2011) argue that health ICTs present many privacy risks, and individuals' perception of risk is likely to influence their privacy concerns. Thirdly, further empirical work is required to understand the role of perceived risk in the health context.

### **2.5.3 Individual Experiences**

In order to develop an understanding of citizens' information privacy concerns, it is important to understand the influence of individuals' experiences (Li, 2011). The role of experience-related factors is discussed in this section to ascertain their relevance to the current study.

#### 2.5.3.1 *Privacy Media Coverage Awareness as an Antecedent*

Privacy media coverage awareness relates to individuals' level of exposure to privacy-related news coverage. The assumption is that greater awareness of privacy media coverage will increase concerns for the privacy of one's own information. The relationship between media coverage awareness and information privacy concerns has been examined in two studies to date. These studies revealed that greater media coverage awareness increased individuals' privacy concerns pertaining to information collected by organisations (Smith, Milberg, and Burke, 1996) and online websites (Malhotra *et al.*, 2004). Privacy media coverage has not been examined in the context of health information privacy concerns. However, it is proposed that awareness of privacy-related media coverage could be an important antecedent in the health context for two reasons. Firstly, privacy media coverage has had a negative influence on EHR implementation in the past. When the media heavily criticised an EHR system introduced in England, the subsequent implementation of a comprehensive EHR in Wales failed due to outcry regarding privacy, leading to the introduction of a summary record system (Greenhalgh *et al.*, 2013). Secondly, there is an abundance of news stories related to health information technology and associated privacy issues. A Google search in May 2016, using the term 'Health information technology privacy' returned approximately 5.59 million news stories. With the prevalence of these news stories, and the supporting empirical evidence in the Internet context, it is argued that privacy media coverage represents an important antecedent which warrants investigation in the health context.

#### 2.5.3.2 *Technology Experience as an Antecedent*

Many studies have explored the influence of Internet experience on concern, yielding mixed results. A number of studies found that greater Internet experience was associated with lower information privacy concerns (Bellman *et al.*, 2004; Dinev and Hart, 2006; Yao and Zhang, 2008). Similarly, Perera *et al.*, (2011) found that lower Internet experience led to higher privacy concerns regarding data stored in health technologies. However, some studies have found that Internet experience had a positive impact on privacy concerns. For example, Yao *et al.*, (2007) found that years of Internet experience had no impact on privacy concerns, but fluency of Internet use had a

positive impact, and the diversity of Internet use had a negative impact. In addition, several studies have found that Internet experience does not have a significant impact on concern (Ward *et al.*, 2005; Youn, 2009). It is argued that Internet experience in the general sense is unlikely to strongly influence citizens' HIPC. Experience of using the Internet as a source of health data, or using health ICTs may have an influence on the other hand. Experience of using the Internet and mHealth solutions to retrieve health data has been shown to increase individuals' intentions to adopt mHealth technologies (Lim *et al.*, 2011; Bidmon *et al.*, 2014). This experience suggests a comfort in using technology for health purposes, and thus these individuals may express lower concerns regarding the use of their health data.

#### **2.5.3.3 Privacy Invasion Experience as an Antecedent**

It is often argued that individuals who have previously experienced a privacy invasion will express higher concerns for the privacy of their personal information, across all areas including health. A number of studies in the MIS literature offer support for the positive influence of privacy invasion experience on concern (e.g. Smith *et al.*, 1996; Okazaki *et al.*, 2009). In addition, one study in the health context provides support for this relationship. Bansal *et al.*, (2010) found that individuals with health information invasion experience expressed higher concerns regarding the privacy of their health data disclosed to health websites. Due to the unrivalled support offered by existing studies, it is argued that privacy invasion experience is an important factor to consider when investigating citizens' HIPC.

#### **2.5.4 Additional Antecedents**

In addition to individual characteristics, perceptions, and experiences, a variety of other factors have been examined as antecedents in the existing information privacy literature. These factors, derived largely from the literature review conducted by Li (2011), are briefly outlined in this section.

#### 2.5.4.1 *Psychological Factors as Antecedents*

A number of psychological factors have been examined as possible antecedents to privacy concern including personality type, disposition to value privacy, computer anxiety, and self-efficacy. Many researchers have proposed that personality type may shape individuals' information privacy concerns. The findings in existing studies however are mixed and conflicting. For instance, one study found that agreeableness increased privacy concerns (Korzaan and Boswell, 2008), whereas another study found it had a negative influence (Junglas *et al.*, 2008). One health study showed that certain personality types could influence perceived sensitivity, but the direct relationship between personality and privacy concern was not explored (Bansal *et al.*, 2010). Due to the mixed findings, it is argued that personality type is unlikely to have a strong influence on HIPC. Personality is thus deemed irrelevant to the current study.

Self-efficacy is described as an individual's beliefs in their ability to carry out an action (Bandura, 1977). With regards to information privacy, it is argued that self-efficacy in terms of one's ability to competently use technology can reduce their information privacy concerns. However, two studies found that self-efficacy did not significantly impact concern (Yao *et al.*, 2007; Youn, 2009). A recent study found that mobile self-efficacy reduced individuals' risk perceptions (Keith *et al.*, 2015) suggesting that self-efficacy may influence privacy concerns indirectly, via its influence on other factors. Furthermore, research suggests that self-efficacy may influence health ICT adoption intentions (Kim and Park, 2012). As this study is focused on understanding the factors directly shaping HIPC, self-efficacy is deemed irrelevant.

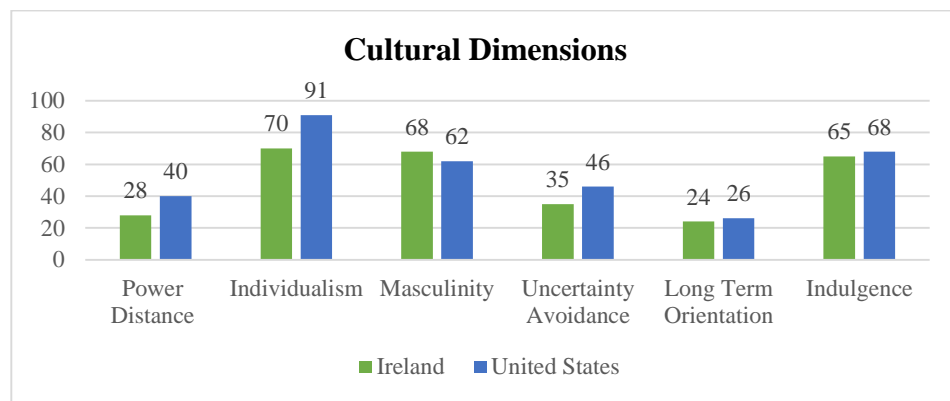
#### 2.5.4.2 *Environmental Factors as Antecedents*

Two macro-environmental factors have been studied as antecedents to information privacy concerns (Li, 2011). Firstly, the influence of regulation on concern has been examined. Government protection was found to have a negative impact on information privacy concerns (Wirtz *et al.*, 2007; Xu, Teo, and Tan, 2005). Secondly, the influence of culture has attracted attention in the existing literature. Two studies have explored the relationship between culture and privacy concern. In both studies, the cultural dimensions of power distance and individualism



positively impacted information privacy concerns, while uncertainty avoidance had a negative impact (Millberg *et al.*, 2000; Bellman *et al.*, 2004). In one of these studies, the influence of culture on concern was fully mediated by regulation (Bellman *et al.*, 2004), thus indicating that culture may not have a strong influence on concern. The influence of regulation and culture on concern has not been examined in the health context. However, Li (2011) argued that both regulation and culture are likely to influence general privacy concerns, as opposed to specific concerns. Based on this assertion, and the cultural similarities between the two countries in this study (see Figure 2.3 below), regulation and culture are ruled out as possible antecedents.

**Figure 2.3 Cultural Comparison Between Ireland and the U.S.**



Source: Hofstede (2016)

#### 2.5.4.3 Organisational Factors as Antecedents

The final category of antecedents outlined by Li (2011) relates to organisational factors, many of which pertain to an organisation's website. Both the perceived convenience (Nam *et al.*, 2006), and the comprehensiveness of a website (Pavlou *et al.*, 2007), have been shown to reduce information privacy concerns. The reputation of an organisation or website has also been explored yielding conflicting results. While Andrade *et al.*, (2002) and Eastlick *et al.*, (2006) found that the website's reputation reduced information privacy concerns, reputation did not have a significant influence in Nam *et al.*, (2006). The completeness of a privacy policy has also been found to reduce concerns (Andrade *et al.*, 2002). These factors represent an interesting avenue for future privacy research across all contexts including health. However, due to this study's

focus on the relationship between citizens' HIPC and health ICT adoption in a general sense and not on a specific website, these factors are ruled out as possible antecedents.

### ***2.5.5 Summary of the Chosen Antecedents***

The chosen antecedents are justified in Table 2.5 below and discussed further in the following hypotheses development chapter. At this point, each factor is merely viewed as pertinent to examining citizens' HIPC. Previous sections discussed these antecedents across various contexts in the information privacy literature, whereas this section focuses exclusively on their role in the health context.

**Table 2.5 Antecedents in the Study**

	Antecedent	Studies	Study Details	Findings	Gaps in Knowledge	Reasons for Inclusion
<b>Individual Characteristics</b>	<b>Gender</b>	Laric <i>et al.</i> , (2009)	Examine U.S. and Canadian citizens' privacy concerns regarding different types of health data.	Females expressed higher privacy concerns regarding a number of health data types.	The influence of gender among European citizens remains unexplored.	Gender is widely supported in other contexts. There is a need to clarify the role of gender in the health context.
		Hwang <i>et al.</i> , (2012)	Examine the privacy concerns of Taiwanese citizens regarding EHRs.	Gender did not have a significant influence on privacy concern.		
	<b>Age</b>	Laric <i>et al.</i> , (2009)	See above.	Older individuals expressed higher privacy concerns regarding several health data types.	The impact of age on privacy concerns among European citizens has not been investigated.	Further exploration is needed to determine the influence of age, and to explain the reasons behind these differences. The world's population is ageing; it is thus imperative to discern differences in privacy concern across age groups in order to address these concerns.
		Hwang <i>et al.</i> , (2012)	See above.	Age did not significantly impact privacy concern.		
		King <i>et al.</i> , (2012)	Examine the privacy concerns of Australian adults regarding national health databases.	Age had a positive influence on privacy concern up to the age of 60.		
		Kordzadeh <i>et al.</i> , (2016)	Explore the antecedents to concerns regarding virtual health communities (U.S.).	Older non-users of VHCs expressed higher privacy concerns.		
	<b>Health Status</b>	Kordzadeh <i>et al.</i> , (2016)	See above.	Poor health status was associated with lower privacy concerns among non-users of VHCs.	The influence of health status on privacy concerns among Europeans remains unknown.	Empirical investigation is required to resolve the debate surrounding the influence of health status.
<b>Individual Perceptions</b>	<b>Perceived Sensitivity</b>	Bansal <i>et al.</i> (2010)	Investigate the influence of U.S. citizens' concerns on their use of health information websites.	Perceived sensitivity of health data results in higher privacy concerns.	The role of sensitivity in the European context requires confirmation.	It is argued that sensitivity increases health privacy concerns (Dinev <i>et al.</i> , 2016).
	<b>Perceived Trust</b>	Dinev <i>et al.</i> , (2016)	Explore the relationship between U.S. & Italian adults' privacy concerns and attitudes towards EHRs.	Trust in EHR vendors reduced health information privacy concerns.	The influence of trust in technology vendors, and trust in health professionals on concern remains unclear.	The importance of trust in the health context has been repeatedly asserted (Rahim <i>et al.</i> , 2013, Dinev <i>et al.</i> , 2016).

	Antecedent	Studies	Study Details	Findings	Gaps in Knowledge	Reasons for Inclusion
	<b>Perceived Risk</b>	Xu <i>et al.</i> , (2011)	Examine the influence of privacy concerns on citizens' views towards different types of websites.	Risk perceptions increase privacy concerns regarding health websites.	The impact of risk in technology vendors & health professionals on HIPC is unknown.	The potential of perceived risk to increase concern in the health context has been noted (Simon <i>et al.</i> , 2009, Fichman <i>et al.</i> , 2011).
<b>Individual Experiences and Knowledge</b>	<b>Media Coverage</b>	No studies to date	N/A	N/A	The role of privacy media coverage on privacy concern has not been explored in the health context.	Privacy media coverage has negatively influenced EHR implementation previously, thus illustrating its relevance.
	<b>Technology Experience</b>	No studies to date	N/A	N/A	The relationship between relevant technology experience and health privacy concerns has not been examined.	Experience searching online for health data has been linked to higher intentions to adopt mHealth (Lim <i>et al.</i> , 2011; Bidmon <i>et al.</i> , 2014). The link between this experience and concern should be explored.
	<b>Privacy Invasion</b>	Bansal <i>et al.</i> , (2010)	See above	Privacy invasion experience increased health information privacy concern.	There is a need to examine privacy invasion experience in the European context.	Due to the sensitivity of health data, privacy invasion experience is likely to be important.

## **2.6 Understanding Information Privacy Concerns**

This section focuses on information privacy concerns, the second element of the APCO model (Smith *et al.*, 2011), and the second research question in this study. It is widely argued that the success of new information technologies is, to a degree, contingent on understanding and addressing citizens' privacy concerns (Hong and Thong, 2013). Furthermore, due to the sensitive nature of health data, citizens' privacy concerns are widely cited as the greatest barrier facing the success of health technologies (Chhanabhai and Holt, 2007; Whittaker, 2012; Dinev *et al.*, 2016). It is thus imperative to develop a comprehensive understanding of citizens' HIPC, in order to develop approaches to address and appease these concerns. Prior to discussing the various measures of privacy concern, it is imperative to define information privacy concerns in this study. Similar to the information privacy construct, the literature offers an array of definitions to describe privacy concerns, many of which centre on individuals as online customers and pertain to fears regarding possible loss of privacy (Xu *et al.*, 2011), or possible uses of data disclosed online (Son and Kim, 2008). Based on these views, and this study's definition of privacy, health information privacy concerns (HIPC) are described as individuals' concerns regarding the collection, use, and dissemination of large quantities of their health information by different health entities. This section continues with a review of the existing measures of privacy concern in the MIS and Health Informatics literature, prior to deciding on the appropriate measure for this study.

### **2.6.1 Dimensions of Information Privacy Concern**

As the information privacy construct is so complex, it cannot be quantified and thus, cannot be measured. Therefore, researchers must utilise proxies to examine privacy. In the existing literature, the majority of studies harness privacy concerns as a means of examining privacy (Bélanger and Crossler, 2011). The popularity of privacy concerns is partly attributable to the availability of validated scales for measuring concerns which have emerged from the innumerable information privacy studies (Dinev *et al.*, 2012). Among the existing measures of concern, there is no agreed upon set of dimensions or factor structure. However, despite differences in the

number of dimensions and naming conventions, the majority of measures share similarities. Among the existing measures, the most popular dimensions are: Collection, Unauthorised Secondary Use, Improper Access, Errors, Control, and Awareness (Hong and Thong, 2013). Each of these six dimensions is reviewed to determine its relevance to examining HIPC.

#### *2.6.1.1 Collection*

Collection relates to individuals' concerns regarding an organisation's collection and storage of a great deal of their personal information (Smith, Milberg, and Burke, 1996). The collection dimension is included in the two most popular privacy concern measures, the Concern for Information Privacy (CFIP) measure and the Internet Users' Information Privacy Concerns (IUIPC) measure (Smith *et al.*, 1996; Malhotra, Kim and Agarwal, 2004). In the context of health information, collection is described as individuals' concerns regarding the collection and electronic storage of vast quantities of health data by health entities (Angst and Agarwal, 2009). While individuals are accustomed to disclosing data to healthcare professionals when receiving treatment, health ICTs such as EHRs facilitate the electronic storage of this information. The emergence of health ICTs also leads to the collection of health data outside of the healthcare setting, by other parties such as health technology vendors. This can cause concern, as health data is widely viewed as sensitive. For example, 93% of Irish citizens describe their personal health information as sensitive (Eurobarometer, 2011). Furthermore, studies have shown that individuals express high concerns regarding the collection and storage of health information they view as sensitive such as mental health data (Flynn *et al.*, 2003). Due to the ease at which health and technology organisations can collect and store vast quantities of sensitive health data, it is argued that the Collection dimension is relevant to examining citizens' HIPC.

#### *2.6.1.2 Unauthorised Secondary Use*

Unauthorised Secondary Use involves individuals' concerns that information collected for one purpose is subsequently used for a secondary purpose without obtaining the individual's permission (Smith *et al.*, 1996). This dimension is included in the CFIP measure. In the context of health information, it is often posited that individuals are less concerned when initially

disclosing information for the purpose of receiving treatment. However, aside from use in treatment, there are a myriad of uses for health data including reporting public health, conducting research, marketing, and media usage (Järvinen, 2009). Individuals are often unaware of how many individuals and organisations view their health information (Angst, 2006). For instance, data in mHealth applications may be accessed by wireless phone carriers, phone manufacturers, and application developers (Eng and Lee, 2013). Furthermore, existing research found that 69% of individuals were concerned that their health data was shared without their permission (Westin, 2005). Due to the plethora of uses for health data and the number of parties accessing this data, it is asserted that Unauthorised Secondary Use is important when studying citizens' HIPC.

#### *2.6.1.3 Improper Access*

Improper Access is described as individuals' concerns that an organisation does not have the measures in place to prevent unauthorised individuals from accessing their information (Smith, Milberg, and Burke, 1996). This includes non-malicious and malicious access by individuals within or external to the organisation. This dimension is included in the CFIP measure and has been included in several studies (e.g. Earp *et al.*, 2005; Liu *et al.*, 2005). As noted, health ICTs enable the collection, storage, and transfer of individuals' health data. Studies show that individuals are concerned about improper access to their health data by (1) malicious employees (Powell *et al.*, 2006), (2) hackers (Chhanabhai and Holt, 2007), (3) legal professionals, and (4) insurance companies (Pyper *et al.*, 2004). Furthermore, individuals express high concerns regarding the repercussions of this access such as possible stigmatisation (Flynn *et al.*, 2003). Based on existing findings and the growth of health ICTs, it is argued that Improper Access represents a dominant concern and warrants inclusion when investigating HIPC.

#### *2.6.1.4 Errors*

The Errors dimension relates to individuals' concerns that the organisation storing their personal information does not have the measures in place to prevent and correct errors in the data (Smith *et al.*, 1996). Errors is the final dimension in the CFIP measure and has been included in additional studies (e.g. Earp *et al.*, 2005; Liu *et al.*, 2005). It is argued that this dimension is

extremely relevant in the health context, as errors in medical data could have drastic impacts on an individual's health. In addition, research shows that individuals are concerned about potential errors in their health data. For example, 65% of respondents in a U.S. study believed that the digitisation of health information may lead to more errors (Westin, 2005). In addition, in a study exploring the concerns of elderly Australian citizens, over a third of respondents expressed concerns regarding possible errors in EHRs (Kerai, Wood, and Martin, 2014). Research suggests that these fears may not be unfounded. In a study which provided patients with access to their EHRs, 32% of respondents found errors in their health information (Powell *et al.*, 2006). It is thus concluded that Errors represents an important dimension in the health context.

#### 2.6.1.5 Control

Control pertains to individuals' concerns regarding the lack of control they have over their personal information (Malhotra *et al.*, 2004). Control is included in the IUIPC measure. In addition, the issue of control features in many information privacy definitions, including the definition chosen in this study. Prior studies in the health context offer support for the importance of control. For instance, Caine and Hanania (2013) found that individuals want to control access to their health records on a granular level, and desire the ability to determine what healthcare professionals can access their data and to decide on their level of access. The link between perceived lack of control and privacy concern has also been supported by Li and Slee (2014), who found that when individuals weren't offered some level of control over their EHR, they expressed higher privacy concerns. Similarly, Dinev *et al.*, (2016) found that high control could reduce privacy concerns. It is argued that Control is important when examining citizens' HIPC.

#### 2.6.1.6 Awareness

Awareness pertains to individuals' concerns regarding their lack of awareness of how an organisation uses and protects their personal information (Malhotra *et al.*, 2004). This dimension is included in the IUIPC measure. In the health context, individuals' lack of awareness of how their health information is used by health organisations has been repeatedly highlighted (e.g. Angst, 2006; Goodwin *et al.*, 2002). This lack of awareness can increase HIPC. For example, a



study in New Zealand found that a large number of respondents were unaware that their health data was stored in an EHR. Upon informing these respondents of the electronic storage of their health data, their privacy concerns increased (Chhanabhai and Holt, 2007). Therefore, it can be argued that Awareness is an important dimension when examining HIPC.

Based on this discussion, it is argued that all six dimensions are relevant to the examination of citizens' health information privacy concerns.

## ***2.6.2 Measures of Information Privacy Concern***

This section reviews the measures of privacy concern in the MIS and Health Informatics literature.

### ***2.6.2.1 Typologies of Privacy Concern***

Typologies have proved a popular means of categorising individuals according to their level of privacy concern. The Westin segmentation has been utilised in national polls in the U.S. since 1995. This typology segments individuals into three groups: privacy fundamentalists who place utmost value on their privacy, privacy pragmatists who place a strong emphasis on privacy but also consider the benefits of information disclosure, and privacy unconcerned individuals who place little value on privacy (Taylor, 2003). In 2002, a mere 8% of individuals were unconcerned, 58% were privacy pragmatists, and 34% were privacy fundamentalists (Harris Interactive and Westin, 2001). A small number of studies have utilised typologies (e.g. Jensen, Potts, and Jensen, 2005; Rust, Kannan, and Peng, 2002). However, while typologies are useful for grouping individuals, they do not provide an in-depth understanding of concerns. Thus these typologies do not represent a viable means for measuring concerns in this study.

### ***2.6.2.2 Popular Measures in the MIS Literature***

There are a number of measures of privacy concern in the MIS literature. These measures are briefly outlined in ascending order. The first measure, CFIP, was developed by Smith, Milberg, and Burke (1996) to examine individuals' concerns regarding organisations' privacy practices. CFIP consists of four of the most popular dimensions in the existing literature: Collection,

Unauthorised Secondary Use, Improper Access, and Errors (Smith *et al.*, 1996). While the CFIP dimensions were originally treated as four first-order factors, upon retesting the measure, Stewart and Segars (2002) added a second-order general factor of privacy concern, upon which the original four first-order factors load on. Another measure was developed by Metzger and Docter (2003). This measure does not include the popular dimensions of concern, but is comprised of four dimensions; anonymity, intrusion online, surveillance, and autonomy. This measure has been used in one subsequent study (Yao *et al.*, 2007).

IUIPC is another popular measure, which focuses on individuals' concerns on the Internet, and is comprised of a second-order general factor and three first-order dimensions regularly discussed in the literature: Collection, Control, and Awareness (Malhotra *et al.*, 2004). The IUIPC measure and factor structure was retested and supported in a recent study (Sipior *et al.*, 2013). Also, in 2004, Dinev and Hart developed a two dimensional scale. The first dimension, Abuse, is similar to the Unauthorised Secondary Use and Improper Access dimensions, whereas the Finding dimension focuses on a number of specific privacy issues. Based on the Finding dimension, Buchanan *et al.*, (2007), developed a 16 item unidimensional measure, which focuses on specific issues such as identity theft. In addition, Xu *et al.*, (2011) reduced Dinev and Hart's measure to four items. More recently, Hong and Thong (2013) combined CFIP and IUIPC to develop the Internet Privacy Concerns (IPC) measure, which aims to comprehensively measure privacy concerns in the Internet context. The six dimensional measure includes: Collection, Unauthorised Secondary Use, Improper Access, Errors, Control, and Awareness. Due to the nascence of the measure, it has not yet been retested. However, the authors conducted rigorous testing across four studies and provided support for several factor structures including a second-order general factor, with the six dimensions serving as first-order factors.

#### 2.6.2.3 *Measuring Privacy Concerns in the Health Context*

The large majority of Health Informatics studies measure privacy concern using one dimension (Shaw, Kulkarni, and Mador, 2011), with some studies using one item measures. For instance, Chhanabhai and Holt (2007) asked respondents '*Are you concerned for the confidentiality and*

*privacy of your health records?* The inclusion of confidentiality within this question obfuscates our understanding, as concern for confidentiality cannot be separated from concern for privacy. This is problematic as privacy concern relates to individuals' perceptions of how their health data is used, while confidentiality relates to the sharing of information with necessary parties (Shaw *et al.*, 2011). More recently, Guo *et al.*, (2013) utilised three items to measure concerns regarding mHealth, and Kordzadeh *et al.*, (2016) examined concerns related to virtual health communities with four items based on Xu *et al.*, (2011). Some health privacy studies have adopted CFIP to measure concerns regarding EHRs (Angst and Agarwal, 2009; Hwang *et al.*, 2012; Dinev *et al.*, 2016). These studies support the adaptation of measures from the MIS literature.

### **2.6.3 *Choosing a Measure for this Study***

The table below provides an overview of the dominant measures of information privacy concern.

**Table 2.6 Existing Measures of Information Privacy Concern**

Author	Dimensions Included							IS Studies	Health Studies
	COLL	SU	ACC	ERR	CON	AWA	Other		
Smith <i>et al.</i> , (1996) CFIP	✓	✓	✓	✓	×	×	×	Stewart and Segars (2002) Bellman <i>et al.</i> , (2004) Paulov <i>et al.</i> , (2007) Son and Kim (2008) Junglas <i>et al.</i> , (2008) Korzaan and Boswell (2008)	Angst and Agarwal (2009) Hwang <i>et al.</i> , (2012) Li and Slee (2014) Dinev <i>et al.</i> , (2016)
Metzger and Docter (2003)	×	×	×	×	×	×	Anonymity Intrusion Surveillance Autonomy	Yao <i>et al.</i> , (2007)	×
Dinev and Hart (2004, 2006)	×	×	×	×	×	×	Abuse Finding	Xu <i>et al.</i> , (2011)	Kordzadeh <i>et al.</i> (2016)
Malhotra <i>et al.</i> , (2004) IUIPC	✓	×	×	×	✓	✓	×	Yang and Miao (2008) Ho and Chau (2013) Sipior <i>et al.</i> , (2013)	×
Buchanan <i>et al.</i> , (2007)	×	×	×	×	×	×	16 items unidimensional	Joinson <i>et al.</i> , (2010)	×
Hong and Thong (2013) IPC	✓	✓	✓	✓	✓	✓	×	×	×

Note: COLL: Collection, SU: Unauthorised Secondary Use, ACC: Access, ERR: Errors, CON: Control, AWA: Awareness

As this study aims to comprehensively examine citizens' HIPC, choosing the appropriate measure is imperative. As illustrated in the table above, some measures do not include any of the popular dimensions in the information privacy literature. The measure developed by Metzger and Docter (2003) focuses on surveillance and anonymity, which is pertinent to studies focused on individuals' online privacy concerns, whereas this study explores citizens' HIPC. As individuals explicitly disclose data to health professionals and mHealth technologies, these dimensions and this measure are deemed irrelevant to this study. The measure developed by Buchanan *et al.*, (2007) consists of 16 items across one dimension. As empirical support has been provided for the multidimensionality of the information privacy concern construct (Hong and Thong, 2013), unidimensional measures pose a problem. In addition, the large majority of items in the measure are irrelevant to the current study, with the exception of 'concerns regarding access to medical records'. This one item would not provide the deep insights into concerns sought in this study, and thus the measure is deemed insufficient. As noted above, a number of health privacy studies utilised one dimensional scales. This approach, while useful for studies where privacy concern is not the focus, is not sufficient when seeking to comprehensively measure HIPC. The measure developed by Dinev and Hart (2004) captures two dimensions under the term 'Abuse'. However, items in the Finding dimension focuses on Internet specific concerns, which are not transferable to the health context. The inclusion of two of the dominant dimensions is also deemed inadequate.

The two most popular measures in the MIS literature are CFIP and IUIPC. In 2013, IPC was developed based on these two measures. As these three measures include some of the popular dimensions from the literature, they are compared to determine the most appropriate measure for this study. The acceptance of these measures can be noted. Both CFIP and IUIPC have been applied to a number of studies across various contexts (Bélanger & Crossler, 2011). However, owing to its nascence, IPC is yet to be utilised in additional studies. Due to the focus of this study on comprehensively investigating the role of privacy in the health context from antecedents to concerns and outcomes, it is important that the chosen measure can fit within a comprehensive framework. Both CFIP and IUIPC, have been utilised in studies which have included antecedents

and outcomes. However, IPC was developed with the specific aim of inclusion in a nomological model to examine privacy comprehensively in a specific context (Hong and Thong, 2013). Relevance to the health context must also be determined. To date, only CFIP has been adapted and used in health information privacy studies. While this supports the relevance of the CFIP dimensions, it is argued here that the four dimensions included in the CFIP measure are not sufficient. The authors of the CFIP acknowledged the importance of routine re-examination of the measure, to ascertain its continued relevance in light of advances in research and technology (Smith *et al.*, 1996). Furthermore, IUIPC has been proven to be more effective in terms of variance explained (Bélanger and Crossler, 2011) and researchers have called for the examination of the IUIPC dimensions such as Control in the health context (Kordzadeh *et al.*, 2016). It is argued that while both CFIP and IUIPC are acceptable measures of concern in the health context, neither measure is sufficient to comprehensively examine HIPC. Based on the discussion in Section 2.5.1, it is asserted that the six popular dimensions of concern are pertinent to the health context. It is therefore concluded that the IPC measure is the most comprehensive, and thus the most appropriate measure for this study. The authors of this instrument have also advised that it may be applied to different contexts such as health, which adds support to its use in this instance. Utilising this measure addresses the gap in the health information privacy literature for a comprehensive measure of concern. To ensure its applicability with the current study, the IPC measure is termed HIPC or the Health Information Privacy Concerns measure. Each dimension is also reworded to reflect the health context, as shown in table 2.7 below.

**Table 2.7 Dimensions of HIPC**

<b>Dimension</b>	<b>Original Definition</b>	<b>HIPC Definition</b>
Collection (CFIP& IUIPC)	Individuals' concern that an organisation is collecting and storing a great deal of their personal information (Smith <i>et al.</i> , 1996).	Individuals' concern regarding the collection and storage of large quantities of health data by health entities and technology vendors.
Unauthorised Secondary Use (CFIP)	Concern that data is collected for one purpose and used for a secondary purpose without permission ( Smith <i>et al.</i> , 1996).	Concern that health information collected for one purpose, is used for another without the individual's permission.
Improper Access (CFIP)	Concern that an organisation does not have the measures in place to protect against unauthorised individuals accessing personal information (Smith <i>et al.</i> , 1996).	Individuals' concern that unauthorised individuals might access their personal health data.
Errors (CFIP)	Concern that the organisation does not have the measures in place to prevent errors in personal data (Smith <i>et al.</i> , 1996).	Concern that health and technology organisations do not have the measures in place to prevent and correct errors in health data.
Control (IUIPC)	Individuals' concerns regarding their lack of control over their data (Malhotra <i>et al.</i> , 2004).	Individuals' concern that they cannot exercise control over their personal health data.
Awareness (IUIPC)	Individuals' concerns regarding their lack of awareness of how an organisation uses and protects the privacy of their personal information (Malhotra <i>et al.</i> , 2004).	Individuals' concern that they lack awareness of how their health data is used and protected.

## 2.7 Outcomes of Information Privacy Concern

This section reviews the outcomes of information privacy concerns discussed in the existing literature, and relates to the final component of the APCO framework. Understanding the outcomes is imperative for illustrating the importance of addressing privacy concerns (Phelps *et al.*, 2001). Various outcomes have been examined in the literature including: privacy-protective behaviours, changes in attitude, reduced willingness to disclose information, and reduced technology adoption intentions. Privacy-protective behaviours have been explored in the MIS literature. Son and Kim (2008) developed a taxonomy of information privacy-protective

behaviours across three categories: information provisions, private actions, and public actions. In terms of information provisions, a number of studies have found that information privacy concerns lead to refusal to disclose personal data (e.g. Culnan and Armstrong, 1999; Solove, 2006), and the falsification of data disclosed (e.g. Sheehan and Hoy, 1998; Chen and Rea, 2004). Private actions such as requesting the removal of one's information (Phelps *et al.*, 2000; Sheehan and Hoy, 1998) and spreading negative word of mouth (Culnan and Armstrong, 1999) have been evidenced in the literature. Public actions such as joining others online to confront an organisation about their privacy practices (Sheehan and Hoy, 1998) have also been identified. The relationship between privacy concerns and individuals' adoption of technologies has received a great deal of attention in the existing literature (Bélanger and Crossler, 2011). Studies have shown that privacy concerns can reduce (1) individuals' willingness to continue their relationship with an online organisation (Malhotra *et al.*, 2004), (2) their online purchasing frequency (Phelps, D'Souza, and Nowak, 2001), and (3) their adoption intentions (Liu *et al.*, 2005).

In the health context, less research exists surrounding the relationship between HIPC and the various outcomes. Researchers have argued that privacy concerns will lead to mental health patients abstaining from seeking medical attention or withholding important information (Fetter, 2009). In support of this assertion, a U.S. study found that 13% of respondents had previously falsified data disclosed to health professionals due to privacy concerns related to EHRs (Campos-Castillo and Anthony, 2014). As patients are diagnosed and administered treatment based on the information available to physicians, withholding or falsifying information can lead to drastic impacts for patients such as misdiagnoses. In terms of technology adoption, HIPC have been found to negatively influence individuals' attitudes towards EHRs (Dinev *et al.*, 2016), reduce their intentions to opt-in to EHRs (Angst and Agarwal, 2009; Li and Slee, 2014), and reduce their intentions to adopt personal health records (Li, Sarathy, and Xu, 2014). While, privacy-protective behaviours such as withholding and falsifying data disclosed pose interesting problems, this study focuses on the relationship between HIPC and adoption intentions, as privacy concerns are viewed as a barrier facing the success of health ICTs (Whittaker, 2012; Dinev *et al.*, 2016).



## 2.8 Information Privacy Concerns and Technology Adoption

The third research question focuses on exploring the influence of citizens' HIPC on their (1) acceptance of EHRs, and (2) adoption of mHealth solutions. Developing an understanding of the factors influencing individuals' technology adoption decisions and continued usage is paramount to the success of new technologies (Morris and Venkatesh, 2000; Venkatesh *et al.*, 2003). Health ICTs can foster privacy concerns among citizens (Li *et al.*, 2014). It is therefore imperative to explore the relationship between HIPC and health technology adoption. This section reviews the technology adoption literature to develop an approach for examining this relationship.

### 2.8.1 Models of Technology Adoption

The various models for examining the predictors of technology adoption are briefly outlined.

#### 2.8.1.1 Theory of Reasoned Action (TRA)

The theory of Reasoned Action (TRA) is viewed as one of the most influential theories of human behaviour. Rooted in the Psychology literature, TRA has been applied to predict a range of behaviours across various contexts, and was first applied in the technology adoption context by Davis (1989). TRA posits that individuals' attitude toward adoption is influenced by their salient beliefs (Fishbein and Azjen, 1975). This attitude coupled with subjective norm or the individual's perception of how referent others will view this behaviour, influence their behavioural intention (Fishbein and Azjen, 1975). Behavioural intention is defined as the individual's internal subjective judgement of the probability that they will perform the behaviour in question. TRA postulates that behavioural intention will lead to the performance of the behaviour. TRA has been applied in many contexts including privacy, and has influenced the development of later models.

#### 2.8.1.2 Technology Acceptance Model (TAM)

The Technology Adoption model (TAM) developed by Davis *et al.*, (1989) is arguably the most widely applied technology adoption model. TAM uses TRA as a guiding framework, and also proposes that attitude is formed from individuals' beliefs. However, in TAM these beliefs are

predetermined and include perceived ease of use (PEOU), the individual's belief that use of this technology will be free from effort (Davis, 1989), and perceived usefulness (PU), the individual's perception that the technology can improve their job performance (Davis *et al.*, 1989). PU is a stronger predictor of attitude than PEOU, although PEOU also influences PU (Davis, 1993).

#### 2.8.1.3 TAM2

TAM2 was developed by Venkatesh and Davis (2000), and includes all original relationships in TAM, but adds several antecedents to PU such as job relevance, output quality, and result demonstrability. Several moderators were also added including subjective norm, voluntariness (the individual's perception of whether or not they have a choice to adopt the technology), and image (the individual's desire to behave in ways that result in favourable status). They found that PU had a strong influence on intention, while PEOU played a significant indirect role and subjective norm moderated the influence of PU and PEOU on intention in mandatory settings (Venkatesh and Davis, 2000).

#### 2.8.1.4 Theory of Planned Behaviour (TPB)

Another model developed using TRA as a guiding framework is the theory of Planned Behaviour (TPB) (Ajzen, 1991). TPB posits that intention is influenced by attitude, subjective norm, and perceived behavioural control (PBC), described as the individual's perceptions of how easy or difficult it would be to perform the behaviour (Ajzen, 1991). Intention then influences behaviour.

#### 2.8.1.5 Motivation Model (MM)

The Motivation Model (MM) was also originally developed within the Psychology discipline, and was adapted to the technology adoption context by Davis, Bagozzi, and Warshaw (1992). It is comprised of two core dimensions: extrinsic motivation or individuals' motivation to perform an activity based on their perception the activity will lead to outcomes such as improved job performance, and intrinsic motivation which is individuals' motivation to perform an activity based on no other benefit than performing the activity itself (Davis, Bagozzi and Warshaw, 1992).

When combined, intrinsic and extrinsic motivation influence behavioural intention and actual behaviour (Venkatesh and Speier, 1999).

#### *2.8.1.6 C-TAM-TPB*

TAM and TPB were combined to create the combined TAM & TPB model or C-TAM-TPB (Taylor and Todd, 1995). This model is comprised of TPB predictors and perceived usefulness from TAM. Within C-TAM-TPB, PEOU is as an antecedent to PU, and influences attitude and intention indirectly through PU, which influences both attitude and intention. Attitude, subjective norm, and perceived behavioural control influence behavioural intention as in TPB.

#### *2.8.1.7 Model of Personal Computer Utilisation (MPCU)*

The model of Personal Computer Utilisation (MPCU) was developed by Thompson, Higgins, and Howell (1991) to examine the adoption of personal computers. MPCU adopts Triandis' 1980 theory, which argues that behavioural intentions are developed based on individuals' feelings toward a behaviour, social factors, the perceived consequences of the behaviour, complexity, job fit, and long term consequence or benefit. Actual behaviour is then influenced by past behaviour, intentions, and facilitating conditions or factors in the environment that facilitate undertaking the behaviour (Thompson, Higgins, & Howell, 1991).

#### *2.8.1.8 Innovation Diffusion Theory (IDT)*

The Innovation Diffusion theory (IDT) was originally developed to study the acceptance of agricultural innovations in the 1960s (Rogers, 1995). IDT proposes that individuals' adoption of a new technology is influenced by their perceptions of the characteristics of the technology. These innovation characteristics were adapted to study technology adoption by Moore and Benbasat (1991), and include image or how use of the innovation may enhance an individual's status, visibility of the innovation in the organisation, the degree to which the results of using the innovation are demonstrable to others, compatibility, trialability and complexity (Karahanna, Straub, and Chervany, 1999).

#### 2.8.1.9 *Social Contract Theory (SCT)*

Social Contract theory (SCT) is considered to be one of the most influential theories of human behaviour. SCT was developed by Bandura (1986) and adopted to study the usage of computers by Compeau and Higgins (1995). Under SCT, behaviour is the outcome of a set of beliefs about the technology and affective responses to the behaviour (Compeau, Higgins, and Huff, 1999). SCT proposes a reciprocal interaction between an individual's environment, their cognitive perceptions (self-efficacy and outcome expectations), and their actual behaviour (Compeau *et al.*, 1999). Outcome expectations relate to an individual's perceptions regarding the consequences of using a technology and includes performance outcomes related to one's job and personal outcome expectations related to image and status (Compeau and Higgins, 1995). Under SCT, performance outcome expectations influence affect and usage, while personal outcome expectations were found to have little impact (Compeau *et al.*, 1999).

#### 2.8.1.10 *Unified Theory of Acceptance and Use of technology (UTAUT)*

The Unified Theory of Acceptance and Use of Technology (UTAUT) was developed following a re-examination of the existing technology adoption models. UTAUT predicts the likelihood individuals will accept a new technology (Venkatesh *et al.*, 2003), and is comprised of four core dimensions: performance expectancy, effort expectancy, social influence, and facilitating conditions. Performance expectancy draws comparisons to PU and is described as the individual's belief that using the technology will improve their job performance (Venkatesh *et al.*, 2003). Effort expectancy is similar to perceived ease of use, and social influence is based on subjective norm (Venkatesh *et al.*, 2003). According to UTAUT, intention is directly influenced by performance expectancy, effort expectancy, and social influence, and actual use is predicted by behavioural intention and facilitating conditions.

The technology adoption models are summarised in Table 2.8 below. Each of the technology adoption models has inherent advantages and limitations. These models can be simplified, concatenated with other models, and modified to add new dimensions to suit a specific context. The utilisation of technology adoption models in the health context is now discussed.

**Table 2.8 Technology Adoption Models**

<b>Model</b>	<b>Author</b>	<b>Constructs</b>
<b>Theory of Reasoned action (TRA)</b>	Fishbein and Azjen (1975)	Attitude toward behaviour (ATT) Subjective norm (SN)
<b>Technology acceptance model (TAM)</b>	Davis (1989)	Perceived usefulness (PU) Perceived ease of use (PEOU)
<b>TAM2</b>	Venkatesh and Davis (2000)	Perceived usefulness (PU) Perceived ease of use (PEOU) Subjective Norm (SN)
<b>Theory of Planned behaviour (TPB)</b>	Ajzen (1991)	Attitude toward behaviour adapted from TRA Subjective norm adapted from TRA (SN) Perceived behavioural control (PBC)
<b>Motivational Model (MM)</b>	Davis <i>et al.</i> , (1992)	Extrinsic motivation Intrinsic motivation
<b>Combined TAM and TPB (C-TAM-TPB)</b>	Taylor and Todd (1995)	Attitude (ATT) Subjective Norm (SN) Perceived behavioural control (PBC) Perceived Usefulness (PU)
<b>Model of PC Utilisation (MPCU)</b>	Thompson <i>et al.</i> , (1991)	Job fit (similar to PU) Complexity (similar to PEOU) Long term consequences Attitude towards use Social Factors Facilitating conditions
<b>Innovation Diffusion Theory (IDT)</b>	Rogers (1995)	Relative advantage Ease of use Image Visibility Compatibility Results demonstrability Voluntariness of Use
<b>Social cognitive theory (SCT)</b>	Compeau and Higgins (1995)	Performance Outcome expectations Personal Outcome expectations Self-efficacy Affect Anxiety
<b>UTAUT</b>	Venkatesh <i>et al.</i> , (2003)	Performance Expectancy (PE) Effort Expectancy (EE) Social Influence (SI) Facilitating Conditions (FC) Moderators: Gender, Age, Experience and Voluntariness

### 2.8.2 Health Technology Adoption Among Health Professionals

Prior to discussing health information technology adoption among citizens, the literature on adoption by health professionals is briefly noted. A number of recent systematic literature views have been conducted to identify studies utilising technology adoption models to study health professionals' technology adoption (Yarborough and Smith, 2007; Holden and Karsh, 2010; Li *et al.*, 2013). The findings of these studies are illustrated in Appendix A, pg. 283. A number of

observations can be made based on these findings. Firstly, the body of studies offers mixed support for the various technology adoption constructs. For example, Perceived Usefulness influenced intentions to adopt an E-prescriptions system in Spain (Escobar-Rodriguez *et al.*, 2012), health ICTs in Taiwan (Chen and Hsiao, 2012), and mHealth systems in China (Wu *et al.*, 2011), but did not significantly influence intentions to adopt Telemedicine in a South American study (Saigí-Rubió *et al.*, 2014). Similar evidence was provided for the majority of constructs, with support offered by some studies but not others. Secondly, in terms of the relationship between intention and actual behaviour, empirical support was offered by Kijasanayotin, Pannarunothai, and Speedie (2009), and Chang *et al.*, (2007). They found that adoption intentions influenced actual use of HIT in Thailand, and Clinical Decision Support Systems in Taiwan. Thirdly, the authors of these systematic reviews offer different recommendations. While Holden and Karsh (2010) advocate the use of TAM in health ICT adoption studies, and Li *et al.*, (2013) argue that UTAUT is a promising model for future studies in this context, Yarbrough and Smith (2007), suggest that the explanatory power of these models can be improved by adding external variables such as barriers to technology adoption.

### **2.8.3 Health Technology Adoption Among Citizens**

Despite many researchers highlighting the importance of citizens' adoption of health technologies (Or and Karsh, 2009; Kim and Park, 2012), citizens' acceptance of EHRs and adoption of mHealth solutions remain under-examined in the MIS literature, and the majority Health Informatics studies are descriptive in nature (Rai *et al.*, 2013; Li *et al.*, 2014; Hennington and Janz, 2007). It is argued that technology adoption models provide validated models for understanding the factors motivating health ICT adoption (Angst and Agarwal, 2009; Cho, 2016). The importance of choosing the most appropriate technology adoption model has been highlighted by Venkatesh, Sykes, and Zhang (2011). In order to decide upon a suitable technology adoption model, a systematic literature review was conducted. This systematic review builds upon an earlier review conducted by Or and Karsh (2009), who examined the literature on patients' acceptance of consumer health ICTs. A total of 52 articles met their inclusion criteria.

A number of observations can be made from their review. Firstly, the majority of studies examined patients' acceptance of health information websites, as opposed to mHealth technologies. This is unsurprising due to the recent emergence of mHealth, and adds support for the need to investigate citizens' acceptance of new health ICTs. Secondly, 94 different factors were examined. This is partly applicable to studies' failure to adopt existing theoretical models for guidance in variable choice, and is problematic as it leads to a sporadic body of knowledge, which can obfuscate efforts to draw conclusions and lead to murkiness around what is known and what requires further investigation. Thirdly, many studies examined the role of demographic variables. Age was measured in 39 studies, 26 of which were significant. Gender was insignificant in the majority of studies it was examined in (84%). Experience with health technology was positively related to acceptance in 15 of 20 studies. Fourthly, 7 studies examined the role of the TAM variables, 5 of which found PEOU and PU significantly influenced acceptance. Two studies also examined and empirically supported the influence of self-efficacy. Failure to apply a technology adoption model in the majority of studies is an inherent weakness in the existing literature in the area. Studies utilising and adopting existing models can greatly add to the area. In line with this assertion, Or and Karsh (2009) called for the inclusion of technology adoption models and social factors. The two systematic reviews are compared in Table 2.9 below. In this study, the focus is on all citizens as opposed to just patients, and the technologies of interest are EHRs and mHealth solutions. Theoretically speaking, this review includes technology adoption models and the Privacy Calculus theory, due to the privacy focus of the study.

**Table 2.9 Systematic Review Comparison**

	<b>Or and Karsh (2009)</b>	<b>Review in this study</b>
<i>Sample focus</i>	Patients only	All citizens: patients and healthy individuals
<i>Technology focus</i>	Consumer health IT only	EHRs and mHealth solutions
<i>Theoretical focus</i>	All factors influencing acceptance	Technology Adoption models Privacy Calculus
<i>Methodological focus</i>	All empirical	Empirical
<i>Literature sources</i>	Databases	Top journals in MIS and Health Informatics
<i>Search terms</i>	Two terms	36 total terms including Boolean searches

The systematic review followed the steps outlined by Kitchenham (2004). The first planning step involved defining a research question, deciding on search terms and literature sources. The review aimed to develop an approach to explore the relationship between citizens' HIPC and their adoption of health ICTs. A total of 36 search terms (outlined in Appendix B, pg. 286) were developed to ensure studies utilising any of the technology adoption models among a citizen population were included. Literature sources are detailed in Appendix C (pg. 287), and included the IS Senior Scholars' Basket of 8 top MIS Journals (AIS, 2011), and the 13 Q1 Health Informatics Journals based on Scopus rankings (SCImago, 2011). Each Journal was searched with all search terms. The search yielded a total of 3,224 results. Upon reviewing the titles and abstracts of the results, the search was narrowed to 141 papers. An additional 24 papers were removed due to duplication, and 26 papers with healthcare providers as a sample group were removed. A total of 91 papers focused on health technology adoption among patients or citizens. These papers were subjected to the inclusion criteria outlined in Table 2.10 below.

**Table 2.10 Inclusion Criteria for Systematic Review**

<b>Inclusion criteria</b>	<b>Rationale if appropriate</b>
Written in English language	N/A
Published between 2002- 2016	Studies examining health ICT acceptance prior to 2002 failed to utilise guiding theoretical frameworks (Chau and Hu, 2002)
Must be Empirical	Conceptual studies meeting the rest of criteria are not included
Utilise a technology adoption model or Privacy Calculus theory	Aim of the review is to ascertain the appropriate model of technology adoption for use in the current study
Focus on patients/citizens	In line with aim of current study

Upon reading 88 papers, the review was narrowed down to 13 studies. This is significantly less than the 52 studies included in Or and Karsh (2009), as this review is more narrow in focus. Furthermore, within their study, Or and Karsh (2009) noted that 7 studies explored TAM variables namely PU and PEOU. However, upon reviewing these studies it became apparent that only 3 utilised a validated technology adoption model. These 3 studies are included in this review. The table below outlines the findings of these studies.



**Table 2.11 Systematic Review Findings**

<b>Author</b>	<b>Focus</b>	<b>Model</b>	<b>Dependent variable</b>	<b>Findings</b>
Wilson and Lankton (2004)	Patients' eHealth acceptance	TAM + MM	70%: Intention	PU and extrinsic motivation influenced intention Satisfaction with healthcare predicted intrinsic motivation Information seeking preference predicted PEOU Healthcare need was not significant
Kim and Chang (2006)	Providers and users' intentions regarding health information websites	TAM + potential antecedents to TAM variables	User satisfaction	Usage support and customisation features significantly influenced both PU & PEOU PU influenced user satisfaction
Klein (2007)	Internet patient-physician portals	TAM, individual innovativeness, healthcare need	38%: Intention 47%: Use	PU, Healthcare need, and individual innovativeness significantly influenced intention
Lanseng and Andreassen (2007)	Patients and self-diagnosis technologies	TAM, technology readiness, trust	83%: Intention	PU influenced attitude but not intention PEOU influenced PU Trust influenced PU and PEOU Attitude influenced intention
Lim <i>et al.</i> , (2011)	Singaporean womens' acceptance of a mobile health information application	TAM, self-efficacy, anxiety	44%: Intention	PU & PEOU influenced intention Self-efficacy influenced intention, PU, and PEOU Anxiety did not significantly influence intention Past experience influenced PU, PEOU, self-efficacy & intention Link between intention and use was not significant
Or <i>et al.</i> , (2011)	Home care patients' acceptance of CHIT (consumer HIT)	UTAUT	54%: Intention. 68.5%: Use	SN & PEOU significantly influenced PU but not intention PU influenced intention PBC was not significant on intention Use was influenced by intention, PU & healthcare knowledge
Kim and Park (2012)	MHealth adoption in South Korea	TAM for the health context HITAM	83%: Intention 73%: Attitude	Health zone influential factors: health status, health belief & concern. Information zone: intention influenced by subjective norms which significantly influenced PU Technology zone: HIT self-efficacy and HIT reliability were influential

Author	Focus	Model	Dependent variable	Findings
Hsu, Lee, and Su (2013)	Health ICT Adoption in China	UTAUT and Security	65%: Intention	PE, SI, facilitating conditions, and Perceived Security influenced Intention EE was not significant
Sun <i>et al.</i> , (2013)	Adoption of Mobile Health Services Among Elderly Patients in China	UTAUT and PMT	44%: Intention	PE, EE, SI, Response cost, Self-efficacy, and Perceived vulnerability significantly influenced Intention
Guo <i>et al.</i> , (2013)	Adoption of Mobile Health Services Among Elderly Patients in China	UTAUT, and Resistance to change	33.5%: Intention	PE and EE significantly influenced Intention Resistance to change was not significant.
Bidmon <i>et al.</i> , (2014)	Physician rating website acceptance by German citizens	TAM, demographic variables, digital literacy, information seeking behaviours	40%: Intention 28% variance in willingness to pay for the app	Attitude= greatest predictor of adoption & willingness to play PEOU positively influenced adoption but negatively impacted willingness to pay Age negatively influenced adoption and willingness to pay
Li <i>et al.</i> , (2014)	Personal Health Record Adoption among U.S. Students	Privacy Calculus and Trust	44% Intention	Perceived Benefits, Trust, and Perceived Privacy Risk Influenced Intention Perceived severity was not significant.
Tavares and Oliveria (2016)	EHR Portal adoption by Portuguese healthcare consumers	UTAUT	50%: Intention 27%: Use	PE, EE, Health, and Habit influenced Intention Hedonic Motivation and SI did not significantly influence Intention Intention influenced Use
Li <i>et al.</i> , (2016)	Adoption of Wearable devices among Chinese consumers	Privacy Calculus theory	15%: Intention 8%: Use	Perceived Privacy Risk, and Perceived Benefits influenced Intentions Intention influenced Use.

As shown in the table above, the most popular models were TAM (applied in 7 studies), UTAUT (utilised in 5 studies), and the Privacy Calculus (applied in 2 studies). The majority of studies combined these models with additional models such as the Motivation model (Wilson and Lankton, 2004), or additional variables such as self-efficacy, perceived security, and trust (Lim *et al.*, 2011; Hsu *et al.*, 2013; Li *et al.*, 2014).

The findings for the main constructs are briefly highlighted. Perceived Usefulness (PU) in TAM, Performance Expectancy (PE) in UTAUT, and Perceived Benefits in PCT all represent a similar construct, which was examined in 12 of 13 studies, and empirically supported in 11 of these studies. For instance, PU influenced intention to adopt eHealth solutions (Wilson and Lankton, 2004), intention to use patient portals (Klein, 2007) and satisfaction with health websites (Kim and Chang, 2006), PE influenced elderly citizens' intentions to adopt mHealth services (Sun *et al.*, 2013; Guo *et al.*, 2013) and intentions to adopt an EHR (Tavares and Oliveria, 2016), and Perceived Benefits positively impacted intentions to adopt Personal Health Records (Li *et al.*, 2014), and wearable devices (Li *et al.*, 2016). The influence of Perceived Ease of Use (PEOU) in TAM, and Performance Expectancy (PE) in UTAUT was supported in 5 of 11 studies which examined its role. For example, PEOU influenced intentions to adopt an mHealth application (Lim *et al.*, 2011), and EE influenced intentions to adopt mHealth services (Sun *et al.*, 2013; Guo *et al.*, 2013), but not adoption of consumer health IT (Or *et al.*, 2011). Subjective Norm (SN) or Social Influence (SI) was supported in 2 of the 4 studies it was examined in. Perceived Behavioural Control (PBC) from TPB and self-efficacy influenced intentions in 2 of 3 studies. In both Privacy Calculus studies, the negative influence of perceived privacy risk on intention was supported (Tavares and Oliveria, 2016; Li *et al.*, 2016). Based on these findings, it is argued that PU/PE/Perceived Benefits, Social Influence, and Self-Efficacy or Perceived Behavioural control should be utilised in future studies. PEOU is excluded due to mixed findings and facilitating conditions are deemed irrelevant as this study is conducted outside of an organisational setting.

An additional 15 constructs were examined in the review, many of which were supported. For instance, experience with similar technology positively influenced intentions to adopt mHealth

applications (Lim *et al.*, 2011; Bidmon *et al.*, 2014). Trust in healthcare providers influenced PU and PEOU (Lanseng and Andreassen, 2007), whereas trust in the technology influenced intention to adopt PHRs (Li *et al.*, 2014). Individual innovativeness (Klein, 2007), perceived vulnerability (Sun *et al.*, 2013) and habit (Tavares and Oliveria, 2016) also influenced intentions. Some additional variables were not supported. For example, anxiety (Lim *et al.*, 2011), resistance to change (Guo *et al.*, 2013), perceived severity (Li *et al.*, 2014), and health information seeking preference did not influence intentions (Lim *et al.*, 2011). Based on these findings, it is argued that trust and previous technology experience are pertinent to future studies.

The role of demographic and health variables can also be noted. A small number of studies explored the influence of demographic factors. Age negatively influenced intentions to adopt a physician rating application and willingness to pay for the application (Bidmon *et al.*, 2014). In contrast, Tavares and Oliveria (2016) found that age had a positive influence, with older individuals expressing higher intentions to access an EHR portal. In terms of gender, men expressed higher intentions to adopt a physician rating application (Bidmon *et al.*, 2014). This review echoes calls for the additional examination of demographic variables to clarify their influence across different health technologies and samples (Or *et al.*, 2011; Rai *et al.*, 2013). In addition, a number of health variables were examined. Need for healthcare services was insignificant in Wilson and Lankton (2004), but significantly influenced use in Klein (2007). It is noted that Wilson and Lankton (2004) utilised a sample of middle-aged female patients, which may have impacted findings. Health status influenced intentions to adopt mHealth (Kim and Park, 2012), and health belief influenced intentions to adopt EHRs (Tavares and Oliveria, 2016). It is evident that health-related variables are important. However, the use of similar, but distinct variables can hinder efforts to consolidate findings and make any solid claims in terms of the role of health status on citizens' adoption of health ICTs. Further research is required to clarify these conflicting findings.

The studies in the review support the use of technology adoption models and the Privacy Calculus in the health context. Studies in the review explained 15-83% of variance in intention to adopt

various health technologies including websites, EHRs, and mHealth applications. In addition, intention influenced behaviour in 4 of 5 studies that explored this link. This supports the examination of behavioural intentions in the current study. Furthermore, it has been argued that in the case of emerging health ICTs, intentions represent an ideal dependent variable, as these technologies have not achieved widespread adoption yet (Bidmon *et al.*, 2014; Hsieh, 2015).

## **2.9 Summary of Gaps in the Literature**

This section reiterates the dominant gaps in the health information privacy literature across four sections: antecedents, measuring HIPC, the HIPC-intention relationship, and additional gaps.

***Antecedents to HIPC:*** Antecedents are categorised as individual characteristics, perceptions, and experiences. Individual characteristics have received limited attention in this context, which has led to mixed findings. There is a need for research to clarify if gender influences HIPC, to determine how age influences concern, and to investigate the influence of different health-related variables. Furthermore, these variables have not yet been examined in a European context, using a multi-dimensional measure of HIPC. In terms of individuals' perceptions, calls have been made for research to explore the influence of trust and risk perceptions regarding both health professionals, and technology vendors (e.g. Rahim *et al.*, 2013; Fichman *et al.*, 2011). There is also a need to examine the influence of perceived sensitivity among a European sample. With regards to experience, the influence of privacy media coverage and health ICT experience on HIPC has not been examined to date, but is extremely relevant and warrants empirical exploration.

***Measuring Health Information Privacy Concerns:*** Many existing health information privacy studies do not utilise validated measures of concern (Shaw *et al.*, 2011). This limits our understanding of citizens' privacy concerns in this context. A number of recent studies have adopted CFIP which provides insights into four relevant dimensions of HIPC. However, it is argued that the six dimensions in the IPC measure are pertinent to the health context. This measure is thus adapted and tested in this study, in an effort to comprehensively examine citizens' HIPC.

**HIPC and Technology Adoption:** The success of health ICTs has been limited due to the low level of acceptance received among patients (Or and Karsh, 2009; Or *et al.*, 2011). It is therefore imperative to understand the predictors of adoption, and the inhibitors such as privacy concerns (Dinev *et al.*, 2016). Few studies have explored the relationship between HIPC and health technology adoption. To build upon these studies, there is a need to adopt and add to existing technology adoption models (Angst and Agarwal, 2009). This study utilises a mixed methods approach to develop deep insights into the relationship between HIPC and adoption intentions.

**Additional Gaps:** There is a dearth of comprehensive information privacy studies across all contexts including health (Smith *et al.*, 2011). Thus there is a need for studies which comprehensively study privacy, including the antecedents, dimensions of concern, and the concern-adoption relationship. There is also a need for studies which harness multiple theories to explain privacy in this context. There is a gap in the literature for studies which examine technologies introduced by health providers such as EHRs, and technologies utilised by citizens such as mHealth applications. Lastly, no prior studies have examined HIPC among an Irish sample.

## **2.10 Conclusion**

This chapter reviewed the existing information privacy and technology adoption literature relevant to the examination of citizens' HIPC. As evidenced in this chapter and the preceding discussion, there are many gaps in our understanding of the role that privacy plays in the health context. These gaps include: the lack of understanding surrounding the predictors of HIPC, definitional confusion, the proliferation of unidimensional measures of HIPC, and a paucity of studies which examine HIPC in a holistic manner. This study aims to address these gaps by conducting a comprehensive mixed methods investigation of HIPC among citizens in two countries. The approach for addressing these gaps and improving our understanding of HIPC is illustrated in the following chapter, along with the hypothesised relationships.

## CHAPTER THREE: PROPOSED FRAMEWORK & HYPOTHESES

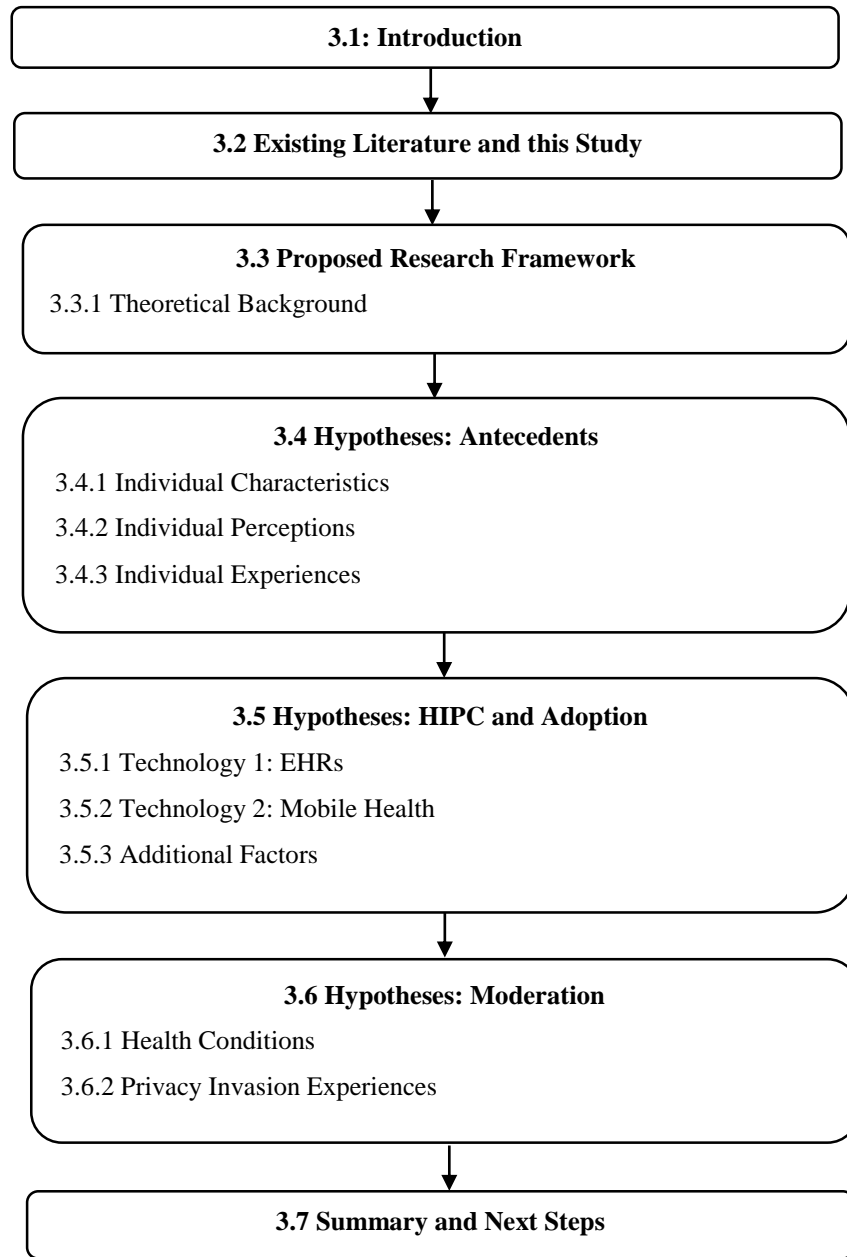
*“I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know”*

*The Hippocratic Oath, Modern version (Lasagna, 1964)*

### 3.1 Introduction

The purpose of this chapter is to present the proposed research framework, and outline the primary hypotheses which are tested in this study. The chapter structure is visually depicted in Figure 3.1 below (pg. 69). This chapter builds upon the previous Literature Review chapter and develops a framework to answer the study’s research questions, and address the gaps in our knowledge regarding health information privacy. The chapter begins by comparing this study to the existing health information privacy studies in terms of the chosen sample, the antecedents included, and the measure used to examine Health Information Privacy Concerns (HIPC). The proposed research framework is presented. The hypothesised relationships within this framework are then outlined and justified. The chapter concludes with a brief outline of the next steps in the study.

Figure 3.1 Chapter Structure





### **3.2 Existing Literature and This Study**

As noted in the previous Literature Review chapter, this study aims to conduct a comprehensive examination of citizens' information privacy concerns in the health context. This involves examining the predictors of HIPC, comprehensively measuring concerns in this context, and exploring the relationship between HIPC and health technology adoption. To illustrate the comprehensiveness of the current study, Table 3.1 below compares this study with relevant studies discussed in the previous chapter. For each study, the table details the technology of interest, guiding theory, the antecedents examined, the means used to measure HIPC, the outcomes of concern, and the technology adoption constructs included.

The technologies examined in these studies include Electronic Health Records (EHRs), mobile health (mHealth) solutions such as mHealth applications, Personal Health Records (PHRs), and wearable health devices, and other technologies such as health websites. The theories harnessed include the Information Boundary theory (IBT), Protection Motivation theory (PMT), Privacy Calculus theory (PCT), and Technology Adoption theories such as the theory of Reasoned Action (TRA), and the Unified theory of Acceptance and Use of Technology (UTAUT). Additional theories such as the Elaboration Likelihood Model (ELM) are categorised as 'Other'. The antecedents examined include individual characteristics such as gender, age, and health, individual perceptions such as perceived sensitivity, perceived trust, and perceived risks, and individual experiences such as privacy media coverage awareness, experience with health ICTs, and privacy invasion experience. In terms of examining HIPC, the six popular dimensions of HIPC discussed in the previous chapter are included (Collection, Unauthorised Secondary Use, Improper Access, Errors, Control, and Awareness). An additional option is included to illustrate the studies that examined concern using a unidimensional measure. The outcomes of interest include adoption intentions, actual use, and other outcomes such as attitudes towards adoption. Technology adoption constructs encompass perceived benefits or perceived usefulness, self-efficacy, and social influence.

**Table 3.1 Comparing this Study with Previous Work**

Category	Detail	This Study	Angst & Agarwal (2009)	Laric et al., (2009)	Bansal et al., (2010)	Lafky & Horan (2011)	Hwang et al., (2012)	Vodicka et al., (2013)	Fischer et al., (2014)	Li & Slee (2014)	Li et al., (2014)	Guo et al., (2015)	Dinev et al., (2016)	Li et al., (2016)	Kordzadeh et al., (2016)
Sample	Students	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
	Employees	✓	✓	×	×	✓	✓	✓	×	✓	×	✓	✓	✓	✓
	Older Citizens	✓	×	×	×	✓	×	✓	✓	✓	×	✓	×	×	×
Technology	EHRs	✓	✓	×	×	×	✓	✓	×	✓	×	×	✓	×	×
	mHealth	✓	×	×	×	✓	×	×	✓	×	✓	✓	×	✓	×
	Other	×	×	×	✓	×	×	×	×	×	×	×	×	×	✓
Theory	IBT	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
	PMT	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
	PCT	✓	×	×	×	×	×	×	×	×	✓	×	✓	✓	✓
	Tech adoption	✓	×	×	×	×	×	×	×	✓	×	×	✓	×	×
	Other	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×
Antecedents	Gender	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×	×
	Age	✓	×	✓	×	×	✓	×	✓	×	×	×	×	×	✓
	Health	✓	×	×	✓	✓	×	×	×	×	×	✓	×	×	✓
	Sensitivity	✓	×	✓	✓	×	×	×	×	×	×	×	×	✓	×
	Trust: Health	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×
	Trust: Tech.	✓	×	×	✓	×	×	×	×	×	✓	✓	✓	×	×
	Risk: Health	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
	Risk: Tech	✓	×	×	✓	×	×	×	×	×	✓	×	×	✓	×
	Media Coverage	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
	ICT Experience	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
	Invasion	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×
	1 dimension	×	×	✓	✓	✓	×	✓	×	×	×	✓	×	×	✓

Category	Detail	This Study	Angst & Agarwal (2009)	Laric et al., (2009)	Bansal et al., (2010)	Lafky & Horan (2011)	Hwang et al., (2012)	Vodicka et al., (2013)	Fischer et al., (2014)	Li & Slee (2014)	Li et al., (2014)	Guo et al., (2015)	Dinev et al., (2016)	Li et al., (2016)	Kordzadeh et al., (2016)
Measure of Privacy Concern	Collection	✓	✓	×	×	×	✓	×	×	✓	×	×	✓	×	×
	Secondary Use	✓	✓	×	×	×	✓	×	×	✓	×	×	✓	×	×
	Access	✓	✓	×	×	×	✓	×	×	✓	×	×	✓	×	×
	Errors	✓	✓	×	×	×	✓	×	×	✓	×	×	✓	×	×
	Control	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
	Awareness	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
Adoption Constructs	Benefits	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
	Self-Efficacy	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
	Social Influence	✓	×	×	×	×	×	×	×	✓	×	×	×	×	×
Outcomes Examined	Intention	✓	✓	×	×	×	×	×	✓	✓	✓	✓	×	✓	×
	Use	×	×	×	×	×	×	×	×	×	×	×	×	✓	×
	Other	×	×	✓	✓	✓	×	✓	×	×	×	×	✓	×	×

A number of observations are made based on the comparison of this study with prior health information privacy studies. Firstly, the samples utilised in prior studies can be noted. Several existing studies focused exclusively on student (e.g. Bansal *et al.*, 2010; Li *et al.*, 2014) or elderly samples (Fischer *et al.*, 2014). Both of these groups present interesting avenues for health information privacy research. Students are described as the group most likely to adopt mHealth solutions (Li *et al.*, 2014), whereas elderly individuals are viewed as the group who stand to benefit most from the implementation of EHRs and personal adoption of mHealth, due to the higher incidence of chronic illness and greater healthcare needs among this group (Guo *et al.*, 2015; Nolan and Kenny, 2014). However, it has been asserted that older individuals will abstain from adopting mHealth solutions due to issues surrounding privacy and trust (Or *et al.*, 2011). It is imperative to understand the factors driving and inhibiting EHR acceptance and mHealth adoption among both groups. However, as students are likely to express different levels of HIPC than elderly individuals (Bélanger and Crossler, 2011; Li *et al.*, 2014), the findings of studies focusing on one group cannot be generalised to the wider population. It is thus argued that focusing on one group is not sufficient in studies seeking to understand the predictors of HIPC, and the influence of concern on health technology adoption. In order to fully understand the role of different antecedents and the concern-adoption relationship, and to explore the influence of age, a sample with a broad age range is sought in this study. This study adds to the small number of existing health information privacy studies that have utilised a diverse age sample and answers calls for studies which compare student and non-student populations (Bélanger and Crossler, 2011), as well as calls for studies with older populations (Li *et al.*, 2014; Kordzadeh *et al.*, 2016).

Secondly, existing studies have examined a variety of different health ICTs including health technologies introduced by health organisations such as EHRs, and mHealth solutions used by individuals themselves. In addition, health information privacy concerns regarding health websites and virtual health communities have been explored. However, while the breadth of technological focus highlights the relevance of information privacy in the health context, it is noted that existing studies tend to focus on one specific technology. In contrast, this study

explores the influence of citizens' HIPC on their intentions to (1) accept an EHR, and (2) personally adopt mHealth solutions. By doing so, this study provides insights into the relationship between HIPC and intentions towards both, a technology introduced by health organisations that citizens have a pre-existing trusting relationship with, and technologies provided by technology vendors with whom there is no pre-existing relationship.

Thirdly, the theoretical foundations of existing studies are noteworthy. While a number of prior studies fail to leverage existing theory (Laric *et al.*, 2009; Lafky and Horan, 2011; Vodicka *et al.*, 2013; Fischer *et al.*, 2014), the majority of studies utilised relevant theory to guide in construct selection. Technology adoption theories were harnessed in two studies, the Privacy Calculus was harnessed in four studies, one of which utilised both the Privacy Calculus and the theory of Reasoned Action (TRA) (Dinev *et al.*, 2016). Technology adoption theories such as TRA are useful for explaining the influence of individuals' beliefs on their attitudes and adoption intentions (Fishbein and Azjen, 1975). In addition, the Privacy Calculus provides a flexible lens for examining the conflicting influences of perceived benefits and HIPC or perceived risks in some instances (Li *et al.*, 2016), on individuals' adoption intentions. This study leverages the Privacy Calculus theory and the underlying assumptions of TRA, and utilises two additional theories, to explain how HIPC are developed. Neither of these theories have been previously explored in the health context. The Information Boundary theory (IBT) describes how individuals create boundaries to determine what information they are willing to disclose. Protection Motivation theory (PMT) discusses individuals' appraisals of the threats facing their data and their ability to cope with these threats. The combination of these four theories enables the comprehensive examination of information privacy in the health context including the antecedents to HIPC, the relationship between HIPC and adoption, and the trade-offs facing this relationship.

Fourthly, the majority of prior studies focus on a small number of antecedents. For instance, several studies only investigated the predictive influence of individual characteristics such as gender, age, and health conditions (Laric *et al.*, 2009; Hwang *et al.*, 2012; Vodicka *et al.*, 2013; Fischer *et al.*, 2014). While it is important to understand the role of these characteristics, studies

which focus purely on characteristics do not provide insights into the influence of individuals' perceptions and beliefs. A small number of studies investigated the influence of individuals' perceptions and experiences, but again these studies included a small number of antecedents. For instance, Bansal *et al.*, (2010) explored the influence of three relevant perceptions: perceived sensitivity, perceived trust in technology, and perceived risks associated with technology, and one experience related construct: privacy invasion experience. Similarly, Dinev *et al.*, (2016) focused on the influence of trust perceptions regarding EHR vendors, and Internet experience, while Li *et al.*, (2014) examined the role of trust and risk perceptions, and privacy invasion experience. While these studies provide actionable insights and directions for future research, the narrow focus is deemed limiting. Furthermore, some proposed antecedents are yet to be explored in the health context including trust and risk perceptions related to health professionals, and privacy media coverage awareness. The current study addresses this gap by exploring the predictive role of several constructs related to individuals' characteristics, perceptions, and experiences.

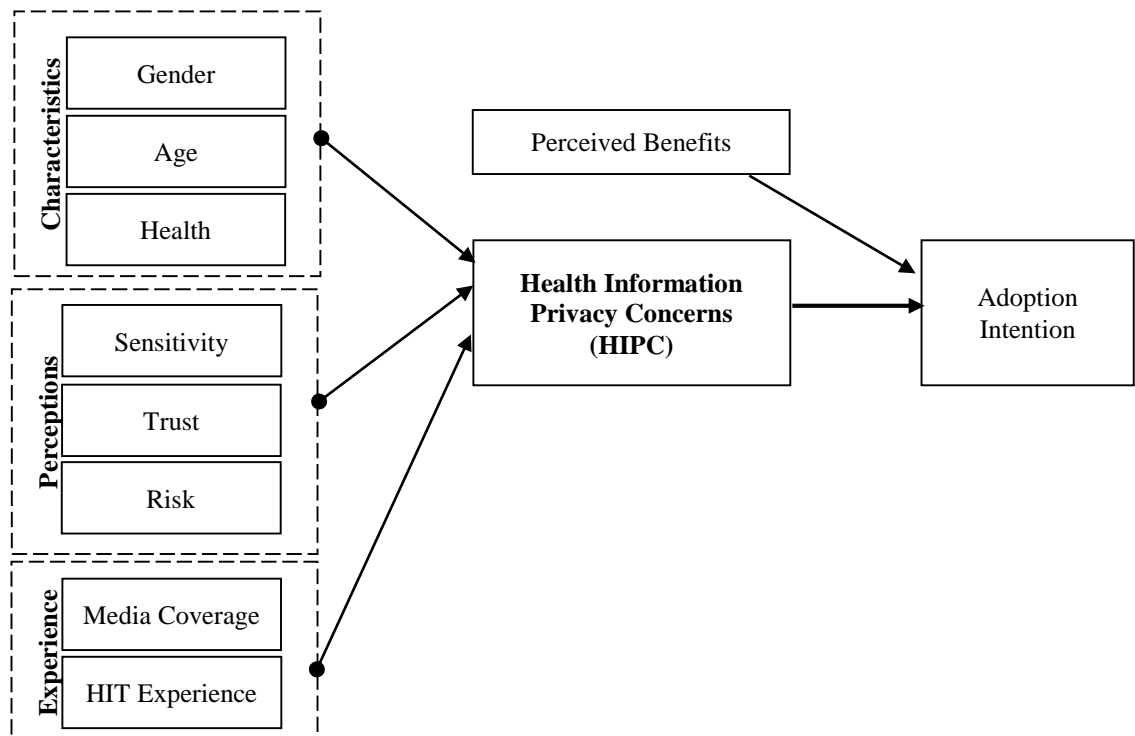
In terms of examining health information privacy concerns, many existing studies utilised a unidimensional measure of concern (e.g. Laric *et al.*, 2009; Bansal *et al.*, 2010; Vodicka *et al.*, 2013; Guo *et al.*, 2015). This approach is inappropriate as information privacy concern is a multidimensional construct, and should be measured as such (Hong and Thong, 2013). Furthermore, these studies do not provide in-depth insights into the dimensions of concern. A number of studies have utilised the four dimensional Concern for Information Privacy (CFIP) measure (Angst and Agarwal, 2009; Hwang *et al.*, 2012; Li and Slee 2014; Dinev *et al.*, 2016). These studies provide useful insights into four important dimensions of concern. However, as discussed in the previous chapter, it is argued that the six dimensions of the Internet Privacy Concerns (IPC) measure are pertinent to this context. This study thus adopts IPC to measure health information privacy concerns comprehensively across six dimensions. The study builds upon previous studies utilising CFIP, and answers calls to elucidate the role of the Control and Awareness dimensions in the health context (Kordzadeh *et al.*, 2016).

Lastly, it is important to note the outcomes and technology adoption constructs examined in previous studies. In terms of the outcomes of HIPC, the majority of studies focused on intentions, while a small number of studies examined other outcomes such as actual use, attitude, and information disclosure. Several studies also explored the role of perceived benefits or perceived usefulness (e.g. Dinev *et al.*, 2016). However, this is the first health information privacy study to include perceived benefits, self-efficacy, and social influence, thus answering calls for health information privacy studies to utilise technology adoption constructs (Angst and Agarwal, 2009). This study addresses several gaps in the literature to advance our understanding of the role of citizens' information privacy concerns in the health context.

### 3.3 Proposed Research Framework

The proposed research framework which is outlined below in Figure 3.2, was developed to address the gaps in the existing literature, and answer the study's research questions.

**Figure 3.2 Proposed Research Framework**



### ***3.3.1 Theoretical Background***

The proposed research framework harnesses a number of theories to examine citizens' HIPC. Each theory is briefly outlined in the context of the framework. The first theory, the theory of Reasoned Action (TRA) provides the underlying support for the research framework. TRA posits that individuals' behavioural intentions are formed from their attitude, which is in turn shaped by a number of salient beliefs (Fishbein and Azjen, 1975). In this research framework, TRA is combined with the overarching APCO (Antecedents → Privacy Concerns → Outcomes) model, which proposes that comprehensive information privacy studies should examine the antecedents, information privacy concerns, and outcomes (Smith, Dinev, and Hu, 2011). As a result, this research framework posits that several antecedents or salient beliefs shape individuals' HIPC, which negatively impacts their adoption intentions.

To identify the salient beliefs in the health information privacy context, two theories which explain the development of HIPC are harnessed. The Information Boundary theory (IBT), proposes that individuals create personal boundaries to determine what information they are comfortable with disclosing, and what information they wish to protect (Petronio, 1991). Individuals may express privacy concerns when information they view as sensitive is requested (Metzger, 2007). IBT is thus represented in the research framework by the perceived sensitivity construct. The second theory, Protection Motivation theory states that individuals' behavioural decisions are influenced by their appraisals of the threats to their information and their perceived ability to cope with these threats (Rogers, 1975; Li, 2012). Threat appraisal is represented by two antecedents in the research framework. Individuals' privacy media coverage awareness represents their knowledge of the breadth and severity of threats facing their health data. Perceived risk pertains to individuals' belief that these threats will become a reality upon disclosing health data to particular party i.e. health professionals or health technology vendors. Coping appraisal is comprised of trust perceptions and experience of using technology for health purposes. Trust in health professionals and health technology vendors relates to individuals' beliefs that these parties will protect their health data. Experience of using mHealth solutions and



seeking health information online suggests a comfort with using technology for health purposes. It is proposed that threat appraisal constructs will increase HIPC, whereas coping appraisal constructs are expected to reduce HIPC.

Lastly, the Privacy Calculus theory is leveraged to explain the competing influences of HIPC and perceived benefits on adoption intentions. It is proposed that individuals' HIPC will negatively influence their intentions to accept EHRs and adopt mHealth solutions. Conversely, perceived benefits are expected to positively impact adoption intentions. In the information privacy research, a number of studies have explored the relationship between information privacy concerns and behavioural intentions. However, Bélanger and Crossler (2011) asserted that information privacy researchers should not assume that behavioural intentions will always result in the intended behaviour, due to the privacy paradox. The privacy paradox is described as the contradiction between the information privacy concerns individuals report and their behaviour, which often involves disclosing personal information in return for seemingly minor benefits (Norberg, Horne, and Horne 2007; Tsai *et al.*, 2011). The importance of the privacy paradox is acknowledged, but it is argued that this contradiction does not pose a serious threat in this study for three reasons. Firstly, a host of technology adoption studies contradict the assumptions of the privacy paradox, by supporting the relationship between behavioural intentions and actual behaviour (Davis, Bagozzi and Warshaw, 1989; Venkatesh *et al.*, 2003; Legris *et al.*, 2003). In terms of this relationship in the privacy context, Li (2011) argues that there is sufficient evidence in the information privacy literature to support the relationship between intentions and behaviours, and to justify the measurement of intentions in future studies. In line with this assertion, the existing health information privacy and health technology adoption literature supports the link between intentions and behaviours (e.g. Li *et al.*, 2016). Secondly, Keith *et al.*, (2013) argue that when actual disclosure behaviour does not match intentions, this discrepancy may be explained by the fact individuals disclose false information to avail of benefits. In their study, 40% of respondents falsified information. They thus concluded that future research concerned with the privacy paradox should distinguish between the disclosure of any data and the

disclosure of accurate data. Thirdly, the Privacy Calculus theory is often utilised to explain the privacy paradox, as it argues that individuals disclose data when they believe the benefits outweigh the risks. This study harnesses the Privacy Calculus theory by examining the role of perceived benefits and HIPC on adoption intentions.

### **3.4 Hypotheses: Antecedents**

This section focuses on the proposed antecedents. Antecedents are discussed under three categories: individual characteristics, perceptions, and experiences.

#### **3.4.1 Individual Characteristics**

The individual characteristics of interest in this study are: gender, age, and health condition. Each characteristic is outlined in terms of the literature and the hypothesised relationship in the study.

##### **3.4.1.1 Gender**

Gender has been found to influence information privacy concerns in a number of contexts. For example, in the context of the Internet, females have been found to express higher concerns regarding the privacy of their personal data (e.g. Hoy and Milne 2010; Joinson *et al.*, 2010). In the health information privacy context, the influence of gender has been explored in three studies to date, which have yielded conflicting findings. These studies are briefly outlined. Firstly, Laric *et al.*, (2009) asked respondents in the U.S. and Canada to rate their concerns for the privacy of different types of health data. They found that females expressed higher concerns regarding the privacy of several health data types. Secondly, Vodicka *et al.*, (2013) measured HIPC among a U.S. sample using one item. They also found that females expressed higher concerns. Thirdly, Hwang *et al.*, (2012) examined the HIPC of Taiwanese citizens using the four dimensional Concern for Information Privacy (CFIP) measure. In contrast to the other two studies, they found that gender did not significantly influence concern. The contrasting findings of these studies may be explained by the different cultures of respondents in these studies, or the different approaches used to measure concern. However, it is clear that further examination is required to evaluate the

influence of gender on HIPC. This study explores this influence using a six dimensional measure of concern among U.S. and Irish citizens. Despite the use of unidimensional measures, the studies conducted by Laric *et al.*, (2009), and Vodicka *et al.*, (2013) illustrate the potential influence of gender in the health context, thus adding to support from the Internet context (e.g. Joinson *et al.*, 2010). Based on the findings in the Internet context and the insights gained from Laric *et al.*, (2009), and Vodicka *et al.*, (2013), it is proposed that females will express higher HIPC.

***H1: Females express higher HIPC.***

***3.4.1.2 Age***

Previous research offers strong empirical support for the positive influence of age on information privacy concerns. In a number of studies which focused on privacy in the Internet context, older respondents expressed higher concerns regarding the privacy of their personal data (e.g. Joinson *et al.*, 2010; Tsai *et al.*, 2011). In the health context, the role of age has been examined in a number of studies, which have yielded mixed results. For instance, one Taiwanese study found that age did not have a significant influence on concern (Hwang *et al.*, 2012). In contrast, Laric *et al.*, (2009) found that older respondents in the U.S. and Canada expressed higher concerns regarding the privacy of several health data types. Another study based in the U.S. offered partial support for the role of age. Kordzadeh *et al.*, (2016) found that age had a positive influence on concern among non-members of virtual health communities, but was insignificant among existing members. Again these mixed findings may be indicative of the culture of respondents, or the measures of concern used. There is a need for further investigation to clarify the role of age in the health context. Based on the empirical evidence, albeit mixed in the health context, it is argued that older individuals will express higher HIPC.

***H2. Individuals' HIPC increase with age.***

***3.4.1.3 Health Variables***

Many argue that the current health status of an individual will influence their HIPC. However, the nature and direction of this influence is the subject of much debate. Some argue that

individuals with health conditions, and as a result greater healthcare needs, will express lower HIPC due to the potential benefits resulting from physicians' use of EHRs, and their personal use of mHealth (Angst and Agarwal, 2009). On the other hand, some postulate that individuals with health conditions will express higher concerns, due to the sensitivity of their health data (Flynn *et al.*, 2003). Mixed empirical findings further obfuscate this debate. While Koradezah *et al.*, (2016) found that health status negatively impacted HIPC, Bansal *et al.*, (2010) found that 'poor health status' had a positive, indirect influence on HIPC via its influence on perceived sensitivity. Both of these studies were conducted in the U.S. and utilised a unidimensional measure of concern. There is a need to examine the influence of health status using a multidimensional measure among different populations to clarify these mixed findings. It is posited that poor health status will positively impact HIPC for two reasons. Firstly, in addition to the positive indirect influence found by Bansal *et al.*, (2010), studies have shown that individuals with health conditions express extremely high concerns regarding the privacy of their health data (e.g. Flynn *et al.*, 2003; van Heerden *et al.*, 2013). Secondly, it is argued that failure to protect the privacy of health data can impact the lives of individuals with health conditions in a number of negative ways (Anderson and Agarwal, 2011). Thus these individuals are more likely to express high concerns regarding the privacy of their personal health information.

### ***H3: Poor health status increases HIPC.***

Healthcare need is another health variable frequently examined in the technology adoption literature. The influence of healthcare need on HIPC has not been explored to date. However, it is argued that it is relevant, as greater needs for healthcare services are associated with more detailed and perhaps, more sensitive health records. Individuals with higher healthcare needs may benefit from personal monitoring using mHealth solutions, however due to the volume of their health data, they may express concerns regarding privacy. It is thus important to explore whether healthcare need influences individuals' HIPC. Examining different health variables is also imperative for developing an understanding of how health factors can influence concern in

this context. It is argued that individuals with greater healthcare needs will express higher HIPC, due to the sensitivity of their data, and the negative outcomes stemming from a lack of privacy.

***H4: Healthcare needs increase HIPC.***

### ***3.4.2 Individual Perceptions***

The perceptions explored in this study include perceived sensitivity, perceived trust, and perceived risks. This section describes each construct and outlines the hypothesised relationships.

#### ***3.4.2.1 Perceived Sensitivity***

Whilst it is widely contended that health data is more sensitive than other types of personal information, perceptions of sensitivity vary from one individual to another. It is thus often argued that higher perceptions regarding the sensitivity of health data will lead to higher HIPC (Dinev *et al.*, 2016). This relates to the Information Boundary theory (IBT), and the assumption that individuals will express higher concerns regarding the privacy of data they view as sensitive (Metzger, 2007; Li, 2012). Empirical evidence has been provided to support these assertions. For instance, perceived sensitivity of health data has been found to reduce individuals' willingness to disclose sensitive data (Caine and Hanania, 2013), to increase perceptions of the risks facing health data (Li *et al.*, 2016), and to increase individuals' HIPC (Bansal *et al.*, 2010). Building upon the findings of Bansal *et al.*, (2010), this study explores the influence of perceived sensitivity on health information privacy concerns, which are measured using a six dimensional measure as opposed to a unidimensional measure. In line with previous findings and IBT, it is postulated that perceived sensitivity will increase HIPC.

***H5: Perceived Sensitivity increases HIPC.***

#### ***3.4.2.2 Perceived Trust***

Perceived trust relates to individuals' belief in the competence, benevolence, and integrity of an organisation with regards to their information (McKnight *et al.*, 2002). A number of studies have found that perceived trust negatively influences individuals' information privacy concerns in the

Internet context (e.g. Pavlou *et al.*, 2007; Tsarenko and Tojib, 2009). In the health context, trust perceptions tie in to the Protection Motivation theory (PMT) and its assumption that individuals' behaviours are influenced by their perceived ability to cope with the risks facing their information. In other words, trust can alleviate the many concerns and fears individuals have regarding their health data. Empirical support has been provided for this assertion. Bansal *et al.*, (2010) found that trust in health websites increased individuals' willingness to engage with health technologies and overcome their concerns for the privacy of their data. This illustrates the key role trust can play in the health context. There are a number of facets of trust that warrant examination in the health context (Dinev *et al.*, 2016). Firstly, institutional trust (McKnight *et al.*, 2002) or trust in the health professionals who collect and store individuals' health data is important, as if individuals believe that health professionals will protect their data, they will express lower HIPC and may be more likely to accept an EHR system. The influence of trust in health professionals has not been empirically explored. However, researchers have asserted that trust in health professionals will reduce citizens' HIPC (Rahim *et al.*, 2013). In order to test this assertion, this study explores the role of perceived trust in health professionals among U.S. and Irish samples.

***H6a: Perceived trust in health professionals decreases HIPC.***

In addition, trust in the technology vendors providing EHR and mHealth solutions is important, as if individuals believe health technology vendors have their best interests in mind, their HIPC may be appeased. To date, one study has examined the direct influence of trust in EHR vendors on HIPC, providing empirical support for the negative influence of trust on concern among U.S. and Italian citizens (Dinev *et al.*, 2016). As this study focuses on the adoption of EHRs and mHealth solutions, examining the influence of trust in EHR vendors would not be sufficient. However, in line with the assumptions of PMT and the findings of Dinev *et al.*, (2016), it is proposed that trust in health technology vendors in a broad sense, will also reduce citizens' HIPC.

***H6b: Perceived trust in health technology vendors decreases HIPC.***

#### *3.4.2.3 Perceived Risks*

Perceived risks pertain to individuals' expectation that disclosing information to a particular organisation will lead to negative outcomes (Featherman and Pavlou, 2003; Dinev *et al.*, 2012). Studies have shown that perceived risks regarding online information disclosure positively influence information privacy concerns (e.g. Dinev and Hart, 2006; Xu *et al.*, 2011). It is argued that perceived risk is pertinent in the health context. As noted in Section 3.3.1, perceived risk relates to Protection Motivation theory, which states that individuals appraise the threats facing them and the likelihood of these threats occurring. If individuals believe that disclosing their health data to a specific party, such as health professionals or health technology vendors, will result in negative outcomes, they will express higher HIPC, and may be less willing to provide the information. While perceived risk has been examined in a small number of health information privacy studies (e.g. Li *et al.*, 2016), the direct relationship between risk perceptions and HIPC has not been examined. However, it has been argued that individuals' perception of the risks associated with health technologies will influence their privacy concerns (Fichman *et al.*, 2011). Based on the empirical evidence in the Internet context (e.g. Dinev and Hart, 2006), and the assertions of other researchers, it is argued that perceived risk is an important influence to consider when examining the antecedents to citizens' HIPC. It is posited that perceived risks associated with both health professionals and health technology vendors will positively impact citizens' health information privacy concerns.

***H7a: Perceived risks associated with health professionals increase HIPC.***

***H7b: Perceived risks associated with health technology vendors increase HIPC.***

#### *3.4.3 Individual Experiences*

The factors of interest related to experiences include: privacy media coverage awareness and health ICT experience. Each factor is briefly outlined along with the hypothesised relationships.

#### 3.4.3.1 *Privacy Media Coverage*

Privacy media coverage awareness is described as individuals' knowledge or exposure to news stories pertaining to privacy issues such as data collection, usage, and data breaches. This again relates to Protection Motivation theory and the belief that individuals' understanding of the breadth and severity of risks influences their perceptions of the threats facing their information, and their subsequent behaviour (Li, 2012). It has been argued that greater exposure to privacy-related media coverage will increase individuals' understanding of the potential risks and potential misuse of their personal data, and will thus increase their concerns for the privacy of their own information (Smith *et al.*, 1996). To date, two studies based in the U.S. have explored the relationship between individuals' privacy media coverage awareness and their information privacy concerns. These studies support the positive influence of media coverage awareness on concerns regarding personal data disclosed to organisations offline (Smith *et al.*, 1996), and to Internet organisations (Malhotra *et al.*, 2004). The role of privacy media coverage has not been investigated in the context of health information privacy. However, as noted in the previous chapter, there is a wealth of media coverage related to the privacy issues associated with health technologies. Furthermore, privacy media coverage negatively influenced EHR implementation in Wales (Greenhalgh *et al.*, 2013). It is thus argued that the role of privacy media coverage warrants investigation in the health context. Similar to the findings in other contexts, it is proposed that greater awareness of privacy media coverage, and as a result greater understanding of the risks facing individuals' health data, will increase HIPC.

***H8: Privacy media coverage awareness increases HIPC.***

#### 3.4.3.2 *Health ICT Experience*

Relevant technology experience has been studied in a number of contexts yielding mixed results. It is argued that due to the broad nature of Internet experience, it is not pertinent in the health context. However, prior experience of using the Internet as a source of health data may be relevant. The practice of seeking health information online is becoming increasingly popular, with 72% of adults in the U.S. engaging in this practice (PEW, 2013). Moreover, prior online



health information seeking has been shown to positively influence individuals' intentions to adopt mHealth technologies (Lim *et al.*, 2011; Bidmon *et al.*, 2014). Some respondents may have previous experience of using mobile health technologies, as adoption of mHealth solutions is also growing. As noted in the Introduction chapter, it was estimated that approximately 500 million people worldwide would utilise mHealth applications in 2015 (Privacy Rights Clearing House, 2013). It is posited that individuals with prior experience of seeking health data online or using mHealth solutions, are more comfortable utilising technology for health purposes, and thus will be less concerned regarding the privacy of their health data.

***H9: Health information seeking behaviours decrease HIPC.***

***H10: Mobile health experience decreases HIPC.***

### **3.5 Hypotheses: HIPC and Adoption**

This section discusses the influence of HIPC and additional constructs on individuals' adoption intentions.

#### ***3.5.1 Technology 1: EHRs***

Electronic Health Records (EHRs) are implemented by health organisations and utilised by health professionals. However, as the data stored in EHRs pertains to citizens, their consent must be sought prior to implementation. Due to the data storage and sharing that EHRs facilitate, these systems often foster concerns for information privacy. Indeed, citizen acceptance of EHRs is considered critical to successful implementation, with citizens' HIPC representing the biggest barrier to this acceptance (Chhanabhai and Holt, 2007). Despite the potentially inhibiting role of citizens' HIPC, only two studies have directly explored the influence of these concerns. Both studies (Angst and Agarwal 2009; Li and Slee, 2014) found that citizens' HIPC reduced their intentions to opt-in to an EHR. There is a need to further explore this relationship among different samples, to determine if the relationship remains significant and to explain the reasons behind this relationship. This is fundamental to developing approaches to address HIPC and increase EHR

acceptance. In line with previous findings, this study argues that HIPC will negatively influence citizens' intentions to accept an EHR. The relationship is also explored qualitatively to develop an understanding of the reasons underlying the influence of HIPC.

***H11a: Health Information Privacy Concerns decrease citizens' EHR acceptance.***

In addition to HIPC, it is likely that other factors will influence individuals' intentions to accept EHRs. Firstly, trust is viewed as an important component of healthcare delivery. Indeed, citizens tend to have a high level of trust in the competence, integrity, and benevolence of health professionals. This trust can potentially reduce their HIPC (Rahim *et al.*, 2013), and as a result increase their willingness to accept EHRs (Dinev *et al.*, 2016). In other words, if individuals believe health professionals intend to protect their health data, and are capable of this protection, they will be more willing to consent to the inclusion of their data in an EHR.

***H12a: Perceived trust in health professionals increase EHR acceptance.***

As noted in Section 3.4.2.3, technologies such as EHRs simplify processes which were previously laborious and time consuming by enabling the automatic collection, electronic storage, and instantaneous transfer of health data. This increased flow of data is accompanied by immense increases in the risks of data loss. The heightened risks can in turn intensify citizens' concerns for the privacy of their health data stored in EHRs (Fichman *et al.*, 2011). In addition, if individuals believe that providing health professionals with their health data will result in negative outcomes, they may be less accepting of health technologies (Li *et al.*, 2014) such as EHRs. It is thus argued that perceived risks will negatively influence individuals' intentions towards EHRs, with higher perceptions of risks reducing individuals' willingness to opt-in.

***H13a: Perceived risks associated with health professionals decrease EHR acceptance.***

As argued above, experience of utilising the Internet as a source of health data, suggests a level of comfort with using technology for health purposes. It is argued that individuals with prior experience of seeking health data online will be more comfortable with the electronic collection

and storage of their health data via EHRs. Therefore, it is proposed that prior online health information seeking will increase individuals' intentions to opt-in to an EHR.

***H14a: Health information seeking behaviours increase EHR acceptance.***

### ***3.5.2 Technology 2: Mobile Health Solutions***

The second technology of interest is mHealth solutions. Mobile health is an umbrella term that encapsulates a host of technological solutions which provide individuals with the ability to monitor their personal health and fitness (Eng and Lee, 2013). As noted in Chapter One, this study is interested in three mHealth solutions: mHealth applications, wearable health tracking devices, and Personal Health Records (PHRs). As is the case with EHRs, many researchers argue that citizens' HIPC represent a barrier to the growth of mHealth solutions (Whittaker, 2012; Mosa *et al.*, 2013). This relationship has received little empirical exploration due to the nascence of these technologies. However, based on the findings supporting the negative influence of HIPC on EHR acceptance, it is argued that if individuals have high concerns regarding the privacy of their health data, they will be less willing to utilise mHealth solutions which require the disclosure of this data to unknown technology vendors. In line with the findings in the EHR context (e.g. Li and Slee, 2014), and the assertions of other researchers, it is proposed that HIPC will have a negative influence on individuals' intentions to adopt mHealth solutions.

***H11b: Health Information Privacy Concerns decrease intentions to adopt mHealth.***

Trust is also an important factor when examining citizens' intentions towards mHealth solutions. As noted in Section 3.4.2.2, if individuals trust in the benevolence, integrity, and competence of health technology vendors, they are more likely to be comfortable using mHealth solutions, as they believe their data will be protected. Again, there is a dearth of empirical inquiry into the relationship between perceived trust and mHealth adoption. One study which focused on PHR adoption, provided support for the positive influence of trust in PHR technology vendors on intentions (Li *et al.*, 2014). A similar proposition is made here with regards to trust in health

technology vendors. It is proposed that higher trust in health technology vendors will positively impact individuals' intentions to adopt mHealth.

***H12b: Perceived Trust in health technology vendors increase citizens' intentions to adopt mHealth.***

Perceived risk is also expected to impact individuals' intentions to adopt mHealth. In line with Protection Motivation theory, it is argued that if individuals believe that disclosing health data to health technology vendors will lead to negative outcomes, they are less likely to adopt mHealth. Empirical support has been provided for the negative role of risk. Perceived risks associated with technology vendors have been found to reduce individuals' intentions to adopt both PHRS (Li *et al.*, 2014), and wearable health devices (Li *et al.*, 2016). Drawing on PMT and existing findings, it is postulated that individuals' perceptions of the risks associated with disclosing data to health technology vendors will negatively impact their intentions towards mHealth solutions.

***H13b: Perceived risks associated with health technology vendors decrease citizens' intentions to adopt mHealth.***

As noted in Section 3.4.3.2, studies in the technology adoption literature provide support for the positive influence of experience of using the Internet as a source of health data, and experience of using mHealth solutions on mHealth adoption intentions (Lim *et al.*, 2011; Kim and Park, 2012; Bidmon *et al.*, 2014). This study tests the influence of online health information seeking experience and mHealth experience on mHealth adoption intentions among U.S. and Irish samples to further clarify these relationships.

***H14b: Health information seeking behaviours increase citizens' intentions to adopt mHealth.***

***H15: Mobile health experience increases citizens' intentions to adopt mHealth.***

In order to develop a deeper understanding of individuals' adoption intentions, this study explores individuals' intentions towards the three mHealth solutions of interest. It is argued that

individuals' HIPC will negatively influence the frequency of mHealth use. In other words, individuals who express higher concerns for their health information privacy will only use mHealth solutions on an irregular basis.

***H16a: HIPC decrease citizens' intended frequency of use for Personal Health Records (PHRs).***

***H16b: HIPC decrease citizens' intended frequency of use for Wearable Monitoring Devices.***

***H16c: HIPC decrease citizens' intended frequency of use for mHealth Applications.***

### ***3.5.3 Additional Factors***

While the privacy paradox has not been supported in the health context, the Privacy Calculus theory is adopted to explain the complex relationships between HIPC, perceived benefits, and adoption decisions. The Privacy Calculus proposes that individuals will adopt technologies if they believe this adoption will lead to the realisation of benefits (Culnan, 1993). In the health context, a number of studies provide support for the positive influence of perceived benefits on attitudes towards EHRs (Dinev *et al.*, 2016), intentions to adopt PHRs (Li *et al.*, 2014), and intentions to use wearable devices (Li *et al.*, 2016). Based on the undisputed empirical support and the many potential benefits offered by both EHRs and mHealth technologies, it is proposed that perceived benefits will influence both citizens' acceptance of EHRs, and their intentions to adopt mHealth solutions.

***H17a: Perceived benefits of EHRs increase citizens' acceptance of EHRs.***

***H17b: Perceived benefits of mHealth increase citizens' adoption of mHealth.***

The previous Literature Review chapter discussed the potential impact of additional technology adoption constructs such as social influence and self-efficacy on individuals' acceptance of EHRs and adoption of mHealth. While these factors may influence adoption, they have no apparent link with citizens' HIPC. Thus, they are beyond the focus of this study. To account for their potential impact, both variables are included as controls, but no hypotheses are offered.

### **3.6 Hypotheses: Moderation**

The addition of moderators can increase the variance explained and offer a more complete understanding of the drivers behind individual acceptance decisions (Venkatesh *et al.*, 2003). It is thus important to explore the influence of moderating factors on the relationships between HIPC, perceived benefits, and adoption intentions. Based on the previous Literature Review chapter, several moderators related to individuals' health conditions, and privacy invasion experience are proposed.

#### **3.6.1 Health Conditions as Moderators**

As discussed above, the influence of individuals' health on their HIPC is the subject of much debate. Existing research also provides conflicting results. For example, Lafky and Horan (2011) found that all respondents irrespective of health condition expressed high privacy concerns, but individuals with chronic conditions were more willing to disclose health data than individuals with no conditions. However, Tavares and Oliveria (2016) found that individuals with chronic conditions were not more likely to adopt EHRs. It is noted that neither of these studies focused on the moderating influence of health conditions, rather they explored the direct influence of health conditions on individuals' willingness to disclose health data and intentions to accept EHRs. It is argued here that for individuals with chronic conditions, HIPC will have a stronger negative impact on their intentions for two reasons. Firstly, individuals with chronic conditions have been shown to express high concerns regarding the privacy of their data in EHRs (Fetter, 2009). In addition, these individuals have more detailed health records, and failure to protect the privacy of this data could have many negative impacts on their lives (Anderson and Agarwal, 2011). It is thus proposed that the negative influence of HIPC on individuals' intentions to accept EHRs and adopt mHealth solutions will be stronger among individuals with chronic conditions.

***H18a: Chronic illness moderates the relationship between HIPC and EHR acceptance.***

***H18b: Chronic illness moderates the relationship between HIPC and mHealth adoption.***

In addition, individuals with health conditions that they believe are sensitive or personal in nature are likely to express higher HIPC than individuals with no health conditions. In support of this assertion, studies have shown that individuals with sensitive conditions such as mental health conditions and HIV express extremely high concerns regarding the privacy of their health data (Flynn *et al.*, 2003; van Heerden *et al.*, 2013). The health records of individuals with sensitive conditions are likely to include detailed information on sensitive issues which often lead to stigmatisation (Shaw *et al.*, 2011). Thus the lives of these individuals could be drastically impacted if their health data privacy was not protected. It is therefore argued that if these individuals are concerned for their health information privacy, they will express lower intentions towards EHRs and mHealth solutions, due to the potential negative repercussions. In other words, the negative influence of HIPC on adoption intentions will be stronger among individuals with sensitive conditions.

***H19a: Sensitive illness moderates the relationship between HIPC and EHR acceptance.***

***H19b: Sensitive illness moderates the relationship between HIPC and mHealth adoption.***

In line with the Privacy Calculus theory, it is argued that individuals' adoption intentions will be influenced by their perception of the benefits associated with EHRs and mHealth solutions, and they will abstain from adoption when their HIPC outweigh the benefits, but will adopt when the benefits outweigh their concerns. As individuals with chronic and sensitive conditions have detailed health records, if the privacy of data stored in EHRs and mHealth solutions is not protected, the lives of these individuals can be negatively affected. It is thus argued that HIPC represent a stronger influence on adoption decisions than perceived benefits. Conversely, for individuals with no health conditions perceived benefits may outweigh their concerns. Therefore, it is posited that the positive influence of perceived benefits will weaken among individuals with health conditions.

***H20a: Chronic illness moderates the relationship between perceived benefits and EHR acceptance.***

*H20b: Sensitive illness moderates the relationship between perceived benefits and EHR acceptance.*

*H20c: Chronic illness moderates the relationship between perceived benefits and mHealth adoption.*

*H20d: Sensitive Illness moderates the relationship between perceived benefits and mHealth adoption.*

### **3.6.2 Privacy Invasion Experiences as Moderators**

The information privacy literature suggests that previous experience of privacy invasion can intensify individuals' information privacy concerns, as individuals believe future invasions may occur and thus feel that their data is vulnerable. Studies have found that privacy invasion experience increases individuals' concerns regarding the privacy of their personal data collected by organisations (Smith *et al.*, 1996), and online companies (Okazaki *et al.*, 2009). The influence of privacy invasion experience has also been examined and supported in one study in the health context to date. When examining individuals' privacy concerns regarding health information websites, Bansal *et al.*, (2010) found that prior health information privacy invasion experience increased these concerns. Privacy invasion experience has also been proposed as a moderator. For example, Li *et al.*, (2014) found that higher frequency of privacy invasion experience, weakened the influence of privacy control on perceived risk (Li *et al.*, 2014). In other words, for individuals who had experienced several privacy invasions, perceived control over their data did not fully appease their perceptions of the risks facing their data. In this study it is posited that for individuals with prior privacy invasion experience, HIPC will have a stronger negative influence on intentions towards EHRs and mHealth solutions. This relates to Protection Motivation theory. As these individuals have previously experienced the negative outcomes stemming from a lack of privacy, they are likely to act in ways which prevent this from occurring again, such as abstaining from adopting health ICTs. It is proposed that if individuals have experienced prior



privacy invasions, the negative influence of HIPC on adoption intentions will be stronger, as these individuals feel vulnerable and wish to prevent future invasions.

***H21a: Privacy invasion experience moderates the relationship between HIPC and EHR acceptance.***

***H21b: Privacy invasion experience moderates the relationship between HIPC and mHealth adoption.***

Similar to Section 3.6.1, and in accordance with the Privacy Calculus theory, it is argued that for individuals with prior privacy invasion experience, HIPC will represent a stronger predictor of intention than perceived benefits. While these benefits are likely to positively impact intentions, for individuals with prior negative experience, this influence will be weaker, as these individuals are likely to remain cautious against future invasions.

***H22a: Privacy invasion experience moderates the relationship between perceived benefits and EHR acceptance.***

***H22b: Privacy invasion experience moderates the relationship between perceived benefits and mHealth adoption.***

### **3.7 Summary and Next Steps**

This chapter presented the proposed research framework for this study and the hypothesised relationships in this framework. This framework meets calls for comprehensive information privacy studies (Smith *et al.*, 2011), by examining the factors leading to HIPC, examining concern across six dimensions, and exploring the relationship between HIPC and health technology adoption intentions. The framework also leverages several theories. By doing so, this study can address a number of gaps in the literature and improve understanding of the information privacy construct in the health context. The hypothesised relationships in the research framework are quantitatively tested using two models. In addition, qualitative interviews are conducted to

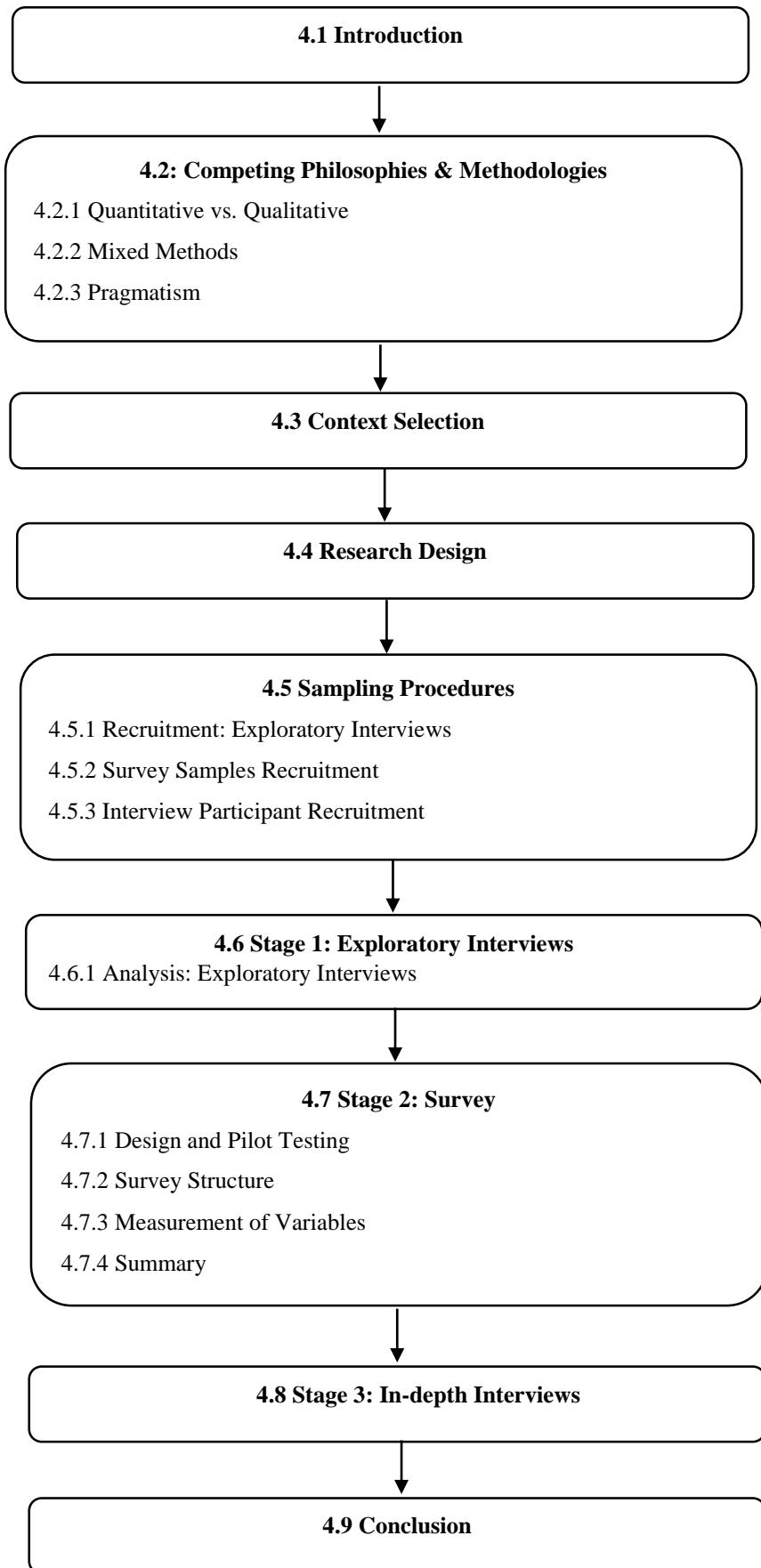
develop insights which explain these relationships. The methodology followed in the study is detailed in the following chapter.

## **CHAPTER FOUR: RESEARCH METHODOLOGY**

### **4.1 Introduction**

This chapter focuses on the research methodology applied in the study. The chapter structure is illustrated below in Figure 4.1 (pg. 97). The chapter commences with an outline of the competing philosophical paradigms and research methodologies. It then describes the appropriateness of a mixed methods approach to address the study's research questions and provides an overview of the steps involved in the research process. The sampling strategies employed are then outlined. The remainder of the chapter discusses the three stages of data collection; exploratory interviews, the survey, and in-depth interviews.

**Figure 4.1 Chapter Structure**



## **4.2 Competing Philosophies & Methodologies**

The researcher's worldview represents how they view the world. As all research is influenced by the researcher's philosophical foundations, it is important to understand and acknowledge the implicit worldviews or philosophical paradigms that the researcher brings to their study (Creswell and Plano Clark, 2007). There are three broad research methodologies associated with a number of conflicting philosophical paradigms. Traditionally Management Information Systems (MIS) research has been dominated by two of these research methodologies, quantitative and qualitative methodologies. The third broad research methodology, mixed methods, suffers from a paucity of studies. The two prevailing methodologies are first reviewed, prior to discussing the suitability of the third methodological approach to this study.

### ***4.2.1 Quantitative vs. Qualitative Methodologies***

Quantitative methodologies dominate several disciplines including MIS, and are predominately associated with the positivist worldview (Sarker, Xaio, and Beaulieu, 2013). Founded by August Conte, positivism is described as a science of knowledge and facts (Teddle and Tashakkori, 2009). Positivists argue that there is one truth which can be observed and measured using quantitative methods. There are many advantages associated with positivism and the application of quantitative methods. For instance, surveys enable researchers to delineate minor differences in individuals' perceptions, develop repeatable measures of a phenomenon, and gain insights into the relationships of interest (Bryman and Bell, 2007). However, there are also many weaknesses which must be noted. Firstly, despite causality claims made by quantitative researchers, theories based on inductive logic, assuming X will predict Y, can never be fully proven. Regardless of how many times X predicts Y, one cannot be certain that the next time it is examined X will predict Y again (Teddle and Tashakkori, 2009). Secondly, quantitative researchers' overreliance on numerical measures creates a disconnect between research and reality (Bryman and Bell, 2007). Thirdly, these measures create a static view of individuals' lives (Bryman and Bell, 2007). Quantitative methods also fail to acknowledge the biases of the researcher and can limit the

understanding of the research context (Creswell and Plano Clark, 2007). In an effort to combat these criticisms, post-positivism emerged in the 1960s led largely by Campbell and Stanley (1963), Hempel (1965), and Kuhn (1962) (Teddlie & Tashakkori, 2009). Post-positivism acknowledges that research is influenced by the philosophical paradigm of the researcher, and accepts that theory can never prove causation (Teddlie and Tashakkori, 2009).

As noted, qualitative MIS studies are not as widely published as quantitative studies. However, in recent decades, qualitative studies have become widely accepted as legitimate scientific investigations among the MIS community (Sarker, Xiao, and Beaulieu, 2013). Qualitative research methodologies are synonymous with the constructivist or interpretivist paradigm. Constructivism assumes that researchers construct the meaning of the phenomenon under investigation, or that they interpret the data to explain this phenomenon (Teddlie and Tashakkori, 2009). It is noted that some qualitative MIS studies often deviate from the assumed paradigm and follow positivist approaches to explore case studies or combine qualitative paradigms with others such as critical realism (Conboy *et al.*, 2012). Irrespective of paradigm, the primary advantage offered by qualitative methods relates to developing a deep understanding of a phenomenon through the views and experiences of participants (Creswell, 2003). Qualitative studies also provide in-depth accounts of the research context. Criticisms of qualitative methods include subjectivity, difficulties associated with replication, validation, and generalisability, and problems with researcher bias (Bryman and Bell, 2007; Creswell and Plano Clark, 2007). To overcome these limitations, researchers have developed guidelines to ensure that qualitative studies employ the same level of rigour as quantitative studies, and achieve generalisability in terms of describing the phenomenon of interest (Sarker *et al.*, 2013; Conboy *et al.*, 2012).

#### ***4.2.2 Mixed Methods, the Third Methodological Movement***

There is a paucity of MIS studies which utilise the third broad research methodology, mixed methods. Mixed methods studies combine quantitative and qualitative methods and represent a fruitful avenue for MIS research as they enable researchers to develop an in-depth, holistic

understanding of a phenomenon (Venkatesh, Brown, and Bala, 2013). Mixed methods studies can facilitate the realisation of many advantages. By combining quantitative and qualitative methods, these studies offset the weaknesses inherent in single method studies (Creswell and Plano Clark, 2007). Mixed methods are viewed as a superior avenue to conduct research in three areas: (1) to answer research questions other methods cannot answer, (2) to develop stronger inferences from data, and (3) to present divergent views which force the re-examination of assumptions underlying the qualitative and quantitative components of a study (Tashakkori and Teddlie, 2003). Mixed methods can also facilitate both the confirmation of hypotheses and theory through quantitative methods, and the generation of theory through qualitative methods (Teddlie and Tashakkori, 2009; Tashakkori and Teddlie, 2003). The primary disadvantage of mixed methods relates to the greater time and effort required (Tashakkori and Teddlie, 2003).

While mixed methods studies are needed and encouraged in MIS, they present many challenges and must only be conducted when appropriate (Venkatesh, Brown and Bala, 2013). A mixed methods research design was chosen in this study due its applicability with the study's aim, research questions, and context. Firstly, the study aims to provide an in-depth understanding of citizens' information privacy concerns in the health context. This aim follows the completeness approach, where one method (qualitative) is used to deepen the insights gained from the other method (quantitative) (Venkatesh, Brown and Bala, 2013). Secondly, the research questions which form the basis of this study are:

RQ1: What are the factors that influence HIPC?

RQ2: What dimensions of information privacy concern are most influential in the health context?

RQ3: Does HIPC influence citizens' acceptance and adoption of health ICTs?

Each question can be explored quantitatively to test the relationships between constructs. However, our limited understanding of HIPC, the nascence of health ICTs, and the extension of constructs and theories to this context for the first time, points to the need for qualitative investigation. The narrative data generated through qualitative methods provides deeper

explanations of these constructs and relationships. Consequently, this study requires a mixed methods approach to answer these research questions.

#### ***4.2.3 Pragmatism as a Research Philosophy***

While paradigmatic positions are often assumed with quantitative (positivist) and qualitative (constructivist) methods, there is much debate regarding what paradigm is suitable for mixed methods studies. Some argue that paradigms cannot be combined, rendering mixed methods research impossible (Tashakkori and Teddlie, 1998, 2003). However, this view has been widely critiqued and debunked. It has also been proposed that mixed methods studies can be conducted by following the dominant paradigm for each component of the study, provided they are kept separate (Venkatesh, Brown and Bala, 2013). However, this approach is inherently difficult. Others suggest that one paradigm should serve as the basis for mixed methods research, with pragmatism proposed as the most appropriate paradigm by many (Datta, 1994; Tashakkori and Teddlie, 2003). The history of pragmatism can be traced to the close of the 19<sup>th</sup> century and the writings of American philosopher Charles Sanders Pierce. His views were elaborated on by William James, John Dewey, and Arthur F. Bentley (Maxey, 2003). The pragmatism paradigm combines the ontological views of post-positivism and constructivism, assuming that singular and multiple realities can exist, as opposed to arguing for one reality. Pragmatism is a practical, applied research philosophy which utilises abductive reasoning to move iteratively from deductive to inductive reasoning (Venkatesh, Brown and Bala, 2013). This approach provides meaningful insights into the phenomenon of interest. Adopting the pragmatist paradigm involves deciding on appropriate methods based on the research question, context, and practical considerations (Greene and Caracelli, 2003). Additional characteristics of pragmatism include the view that theories are instruments judged by how well they currently work, and advocating action over philosophy (Teddlie and Tashakkori, 2009). The flexibility of pragmatism is evidenced when it is compared with the other research paradigms as shown in Table 4.1 below.



**Table 4.1 Comparison of Paradigms**

	<i>Post positivism</i>	<i>Constructivism</i>	<i>Pragmatism</i>
Ontology (Nature of reality)	Singular reality: hypotheses are rejected or accepted.	Multiple realities: quotes utilised to illustrate differing perspectives.	Singular and multiple realities: test hypotheses and present multiple perspectives.
Epistemology (Relationship between researcher and researched)	Distance and impartiality: Data is objectively collected.	Closeness: Researchers visit sites to collect data.	Practicality: data is collected by ‘what works’ to address research questions.
Axiology (Role of values)	Unbiased: checks are utilised to eliminate bias.	Biased: researchers discuss bias and interpretations.	Multiple stances: biased and unbiased perspectives included.
Methodology (Process of research)	Deductive: a priori theories are tested.	Inductive: begin with participants’ views and build up to theory.	Combination: quantitative and qualitative data are collected and mixed.
Rhetoric (Language of research)	Formal: use agreed upon variable definitions.	Informal: researchers write in literary style.	Formal or Informal: researchers can employ both styles of writing.

*Source: Creswell and Plano Clark (2007)*

Pragmatism is the research philosophy applied in this study, due its flexibility and practical nature. To realise the benefits of mixed methods and produce deep insights into the health information privacy phenomenon, the recommendations for conducting mixed methods studies outlined by Venkatesh, Brown and Bala (2013) are followed. In line with the first recommended step, this section illustrated the appropriateness of mixed methods and chose pragmatism as the underlying research philosophy. Additional recommendations offered by Venkatesh *et al.*, (2013) are discussed throughout the chapter.

### **4.3 Context Selection**

This section provides an overview of the context of the study. This study focuses on personal health information. As all citizens are patients at one time or another, health information is pertinent to all citizens in a country (Payton *et al.*, 2011). To gain a better understanding of citizens’ HIPC, it was decided to explore the views of citizens in two countries. The Republic of Ireland was chosen as the first country. Ireland currently trails its European counterparts, ranking 14th among 28 EU member states for healthcare (Björnberg, 2013). This ranking is in part

attributable to an underinvestment in health ICTs, which accounts for approximately 0.85% of Ireland's healthcare expenditure, considerably less than the European average of 2-3% (Department of Health, 2013). The United States was chosen as the second country for three reasons. Firstly, the health systems in these two countries are very different. Healthcare in the United States is largely private, whilst Ireland operates a model which combines public and private health services. This disparity is evident in government spending on healthcare which accounted for 48.0% of all healthcare spending in the U.S. for 2012, compared to 68.5% of spending in Ireland for the same year (OECD, 2015). Secondly, citizens in the United States have greater exposure to electronic health records (EHRs), with 78.4% of U.S. physicians using EHRs by 2013 (Hsiao and Hing, 2014). In contrast, Ireland is yet to introduce a national EHR despite announcing plans to do so (Department of Health, 2013). Thirdly, a large proportion of previous information privacy research has focused exclusively on U.S. samples, leading to calls for European studies (Bélanger and Crossler, 2011). It is thus argued that collecting data from these two countries will strengthen the testing of several constructs in the health context for the first time, and add to the body of knowledge by providing interesting comparisons.

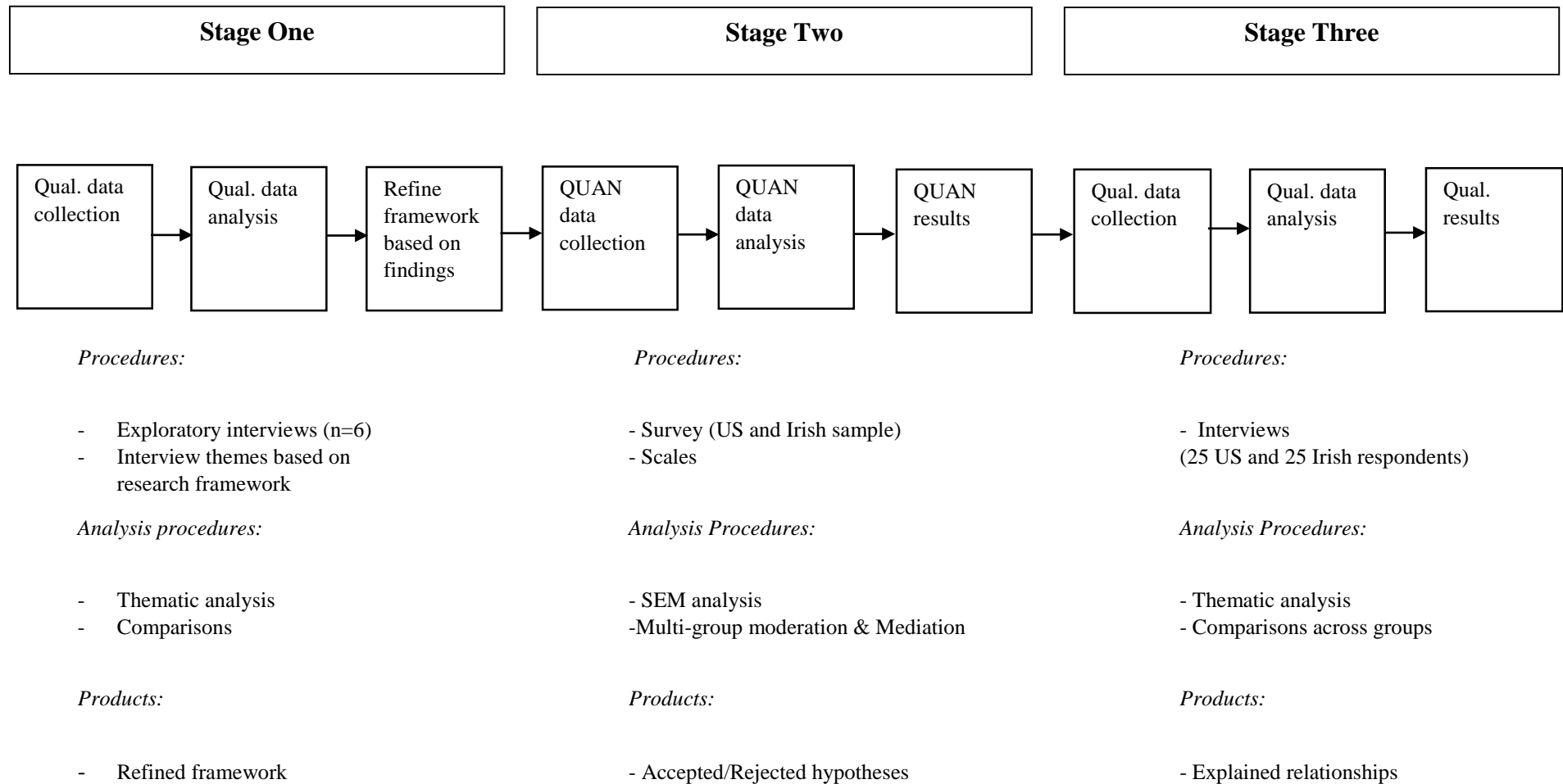
#### **4.4 Research Design**

Mixed methods studies are often critiqued for failure to adequately explain all aspects of the research (Venkatesh, Brown, and Bala, 2013). To overcome this weakness, this study follows the GRAMMS (Good Reporting of a Mixed Methods Study) method outlined by O'Cathain, Murphy and Nicholl (2008). In line with GRAMMS, this study discusses the research design in terms of the methods of inquiry, the research strategy, and the phases involved in the research. Firstly, in accordance with pragmatism, the most appropriate methods of inquiry to answer the research questions are chosen. These methods are derived from the typology of research purposes developed by Newman *et al.*, (2003), which suggests that methods of inquiry should be based on the purposes of the study. The first purpose involves 'generating new ideas' using a research framework developed from the literature. This aim is usually achieved through qualitative methods. Thus exploratory interviews are chosen to test the framework. The second aim requires

the testing of these new ideas or the proposed relationships in the framework. This is achieved using a quantitative survey. The third aim relates to understanding the complex phenomenon of HIPC. In-depth understanding is gained from in-depth interviews.

Secondly, a strategy for conducting the study must be determined (Venkatesh, Brown and Bala, 2013). The first component of the research strategy involves deciding whether the study follows a sequential or concurrent design (Teddlie and Tashakkori, 2009). This study employs a sequential approach, with three stages of data collection. The weighting of each component in the research design is then decided. Weightings are depicted visually using uppercase for dominant components and lowercase for minor components (Teddlie and Tashakkori, 2009). The stages of this study are described as: qual→QUAN→qual. In the first stage, exploratory interviews are conducted to refine the research framework. In the second, dominant, stage, a survey is circulated to test the hypothesised relationships. In-depth interviews are then conducted to explain the relationships. Lastly, the study is described in terms of the research design followed. There are a large number of research designs utilised by mixed methodologists (e.g. Creswell, 2003). This study combines the exploratory and explanatory approaches discussed by Creswell and Plano Clark (2007), and is described as a sequential exploratory-explanatory study. This study begins with a small exploratory study to test the research framework developed from the literature. Stages two and three of the research follow the explanatory approach with a survey used to test the relationships, and interviews conducted to develop in-depth explanations of these relationships. The findings of stages two and three are integrated to develop deeper insights. The stages of the study are depicted below in Figure 4.2 (pg. 105).

**Figure 4.2 Stages of the Research**



## 4.5 Sampling Procedures

A purposive sampling strategy was pursued. When using this non-probability sampling technique, samples are derived from a set of criteria developed by the researcher to identify participants (Kemper, Stringfield, and Teddlie, 2003). This study explores the relationship between HIPC and health ICT adoption. The aim of the sampling criteria was to ensure that individuals who were likely to express varying levels of HIPC and adoption intentions were included. While purposive sampling is traditionally synonymous with qualitative studies, it is often found in quantitative studies and is commonly used in mixed methods (Kemper *et al.*, 2003).

The criteria used to identify participants are briefly outlined. The first criterion is age. Numerous studies have found that older individuals express higher HIPC than younger individuals (Laric *et al.* 2009; King *et al.*, 2012), and a host of studies have revealed that older individuals have lower intentions to adopt health ICTs (Or and Karsh, 2009). Thus, to capture varying levels of HIPC and intention, a wide age range was required. The second criterion relates to the education level of respondents. King *et al.*, (2012) found that college graduates expressed the lowest level of HIPC. Additionally, several studies have found that individuals with higher levels of education express higher intentions to adopt health ICTs (e.g. Bidmon *et al.*, 2014). To explore the role of education, individuals of varying education levels were required. The third criterion relates to health status. The influence of health status on HIPC has attracted much debate. Some argue that individuals with health conditions will express lower levels of HIPC due to the benefits associated with health ICTs (Angst and Agarwal, 2009). On the other hand, it is often argued that these individuals will express higher HIPC due to the sensitivity of their health data (Flynn *et al.*, 2003; van Heerden *et al.*, 2013). To investigate the influence health status on HIPC and adoption, individuals of varying health status are required. The fourth and final criterion relates to technology experience. Technology experience has had a mixed impact on information privacy concern. Some studies have found that Internet experience reduces concern (Bellman *et al.* 2004; Dinev and Hart 2005), while others have found experience increases concern (e.g. Yao *et al.*, 2007). Prior experience with the Internet and similar technologies have been found to increase

health ICT adoption intentions (Bidmon *et al.* 2014; Lim *et al.* 2011). To explore the influence of technology experience on HIPC and health ICT adoption, individuals with varying levels of technology experience are required. To capture these criteria, the sample was broken into the three broad groups detailed below.

***The Privacy Unconcerned, Technology Enthusiasts:*** This group includes individuals aged 18-24, who are students or recent graduates from various academic disciplines. Younger individuals have been found to express lower HIPC (King *et al.*, 2012). Student samples are used in existing health technology adoption studies, as they represent the group most likely to adopt health ICTs (Li *et al.*, 2014). Furthermore, young people with some college education represent the largest group of current mHealth application users (Fox and Duggan, 2012). Individuals in this category may have used similar technologies to monitor health indicators irrespective of their health status, and are likely to be cognizant of the technical aspects of health ICTs.

***The Pragmatic Majority:*** The second group consists of individuals aged 25-49 who are employed in different industries, with varying levels of education. These individuals are likely to express medium to high levels of HIPC, but if they perceive the benefits of health ICTs to outweigh the risks, they will adopt (Westin, 2005). Individuals in this group are likely to be technically competent (Moore, 2003). Some may have recently adopted mHealth technologies for a distinct purpose such as chronic illness, recent medical crisis, or interest in monitoring health (Fox and Duggan 2012).

***The Privacy Concerned, Technology Laggards:*** In line with the World Health Organisation's definition of an older person, the final group consists of individuals aged 50 and above (WHO, 2015). This group includes employees and retirees. Individuals in this group are likely to express high concerns regarding the privacy of their health data and have limited technology experience (Westin, 2005). Individuals in this group tend to avoid adopting new technologies for as long as possible (Moore, 2003). Due to the increasing incidence of chronic illness among older individuals (Nolan and Kenny, 2014), this group can arguably benefit most from health ICTs.

However, older individuals have been found to express higher HIPC (Laric *et al.*, 2009), and are likely to avoid health ICTs due to privacy and trust concerns (Or *et al.*, 2011). As a result of this paradox, calls have been made for studies which utilise older samples (Li *et al.*, 2014).

In summary, the sample is comprised of three broad groups. Capturing the views of these groups answers calls to examine differences in information privacy concerns between student and non-student populations (Bélanger and Crossler, 2011). The remainder of this section discusses the sampling strategies employed in the three stages of data collection.

#### ***4.5.1 Recruitment: Exploratory Interviews***

Six exploratory interviews were conducted with a convenience sample. Interviewees met the sample criteria and included 3 males and 3 females of various ages, education levels, technology experience, and health status.

#### ***4.5.2 Survey Sample Recruitment***

This section outlines the approaches used to recruit survey respondents in the U.S. and Ireland. Prior to conducting research in both countries, ethical approval was granted from DCU's Research Ethics Committee (see Appendix D, pg. 288). This approval was accepted by the Institutional Review Board (IRB) at Arizona State University prior to the commencement of data collection.

**U.S. Sample:** Data were collected during a research visit to Arizona State University (ASU) in April 2015. ASU is the largest public University in the U.S. with over 83,000 students and 12,400 faculty and staff (ASU.edu, 2015). Two methods were utilised to recruit respondents. Firstly, email invitations with a plain language statement and link to the online survey were sent to students in various disciplines such as computer science and health, and to participants of previous studies at ASU who had indicated their willingness to partake in future research. These individuals varied in age, education, technology experience, and health status. Secondly, notices were posted online on student and faculty 'myASU' portal pages. These advertisements included a description of the research and a link to the survey.

**Irish Sample:** Data were collected in several stages between May and August 2015. To recruit ‘*Privacy Unconcerned, Technology Enthusiasts*’, several Undergraduate and Postgraduate classes were visited in Dublin City University (DCU) across business, computer science, and health disciplines. During these visits the study was explained to students. Email invitations were then sent to students. To capture the ‘*Pragmatic Majority*’, three approaches were utilised. Firstly, survey invitations were sent to DCU Alumni via email and Alumni groups on LinkedIn. Secondly, through personal contacts, email invitations were sent to employees in numerous industries including financial services, education, health, and ICT. Thirdly, the researcher delivered a research presentation at an event hosted by Insight, a research centre based in DCU and University College Dublin (UCD). The email invitation was emailed to Insight employees following the event. Examples of email invitations are included in Appendix, E, pg. 289.

The ‘*Privacy Wary, Technology Laggards*’ group were recruited from two initiatives at DCU. The first, the Intergenerational Learning Programme (ILP), offers a number of educational courses for older adults. ILP learners are aged 50 and over, and vary in technology experience. The researcher visited ILP classes and invited the learners to participate in the research. Hard copies of the survey were distributed at classes and email invitations were also sent. The second initiative MedEx, offers a series of supervised exercise programmes for individuals with cardiac disease, chronic respiratory disease, and poor circulation. The researcher was based at MedEx for one week. Prior to each class, the researcher, introduced by the class trainer, informed class members of the study. After each class, hard copies of the survey were distributed. Individuals who wished to complete the survey online provided their email address and a link to the survey was emailed to them.

#### **4.5.3 Interview Participant Recruitment**

In both countries, interview participants were recruited using the survey. The last question in the survey asked respondents if they were willing to participate in an interview with the researcher. Individuals who indicated their interest were asked to provide their contact details. In line with



purposive sampling, all individuals expressing interest were reviewed and a number of individuals representing each of the three groups were contacted and invited to participate in an interview. Interviews were scheduled with all individuals who responded to the researcher's invitation.

## **4.6 Stage One: Exploratory Interviews**

Six exploratory interviews were conducted with Irish citizens. These interviews aimed to (1) test the relevance of all constructs in the research framework and (2) identify additional factors pertinent to examining HIPC. To ensure all topics were discussed, a broad interview guide based on the research framework was followed. As the emphasis was on understanding participants' perceptions, participants were afforded control in how they decided to answer, with rambling answers encouraged (Bryman and Bell, 2007). Interviews were conducted in a private room at DCU. Interviews lasted between 45 and 60 minutes, were audiotaped, and were transcribed using pseudonyms to preserve interviewees' anonymity.

### ***4.6.1 Analysis: Exploratory Interviews***

Two broad analytic techniques were applied to analyse interviews; asking questions and making comparisons. Asking questions about the data is exploratory and allows the researcher to develop ideas on the meaning behind statements made by interviewees (Corbin and Strauss, 2008). Various question types described by Corbin and Strauss (2008) were asked when analysing the interviews including sensitising questions such as: *Is health privacy important to this person?* Theoretical questions included: *Does trust reduce HIPC?* Practical questions were also asked such as: *Would older individuals feel different?* Guiding questions were developed such as: *What type of health information is most sensitive to you?* Asking these types of questions aided in refining the constructs in the research framework. Comparisons illuminate similarities and differences across interviewees. Constant comparisons were made to explore whether older individuals expressed different views, or whether individuals with health conditions had different experiences.

In line with the first research question, the relevance of all antecedents was explored. Support was provided for the inclusion of all antecedents. The primary findings and the refinements made to each antecedent are outlined below in Table 4.2.

**Table 4.2 Antecedents: Findings**

<b>Antecedent</b>	<b>Primary Findings</b>	<b>Amendments</b>
Health Status	<ul style="list-style-type: none"> <li>• Different health conditions influence HIPC differently. All individuals expressed a desire for health data privacy.</li> <li>• Individuals with chronic illness recognised the benefits of sharing data. <i>‘I’m asthmatic, I don’t want that to be public knowledge but if doctors knew, it could help in an emergency’</i> (Joe, Student, 21).</li> <li>• Individuals with sensitive illnesses expressed a higher desire for privacy: <i>‘I don’t want anyone to know I’ve struggled with an eating disorder’</i> (Rachel, 28, Business professional).</li> </ul>	The moderating influence of chronic illness and sensitive illness are examined.
ICT Experience	<ul style="list-style-type: none"> <li>• Interviewees stressed the need for caution when searching online for health information. <i>‘I have Googled health stuff, but I try to limit it and only use respected sites and be careful not to self-diagnose’</i> (Mary 66, retired teacher).</li> </ul>	Extended to include different health ICTs.
Perceived sensitivity	<ul style="list-style-type: none"> <li>• Interviewees viewed health information as more sensitive than other information. <i>‘All health information is sensitive, because it relates to me and my body, there’s nothing more personal’</i> (Joy, Masters Student, 24).</li> <li>• Perceptions of the sensitivity of different health data types varies across individuals.</li> </ul>	Perceived sensitivity of different health data types is explored.
Awareness of privacy news coverage	<ul style="list-style-type: none"> <li>• Interview participants were more aware of privacy news coverage regarding personal information than health information. <i>‘There’s a lot of stories in the news, I remember the Sony breach pretty well, they handled it so poorly, it makes me worry they really don’t care about my information’</i> (Joe).</li> <li>• Some interviewees were aware of health news stories but discussed such events with little detail: <i>‘I’ve heard about clinics in the US being hacked or employees looking at things’</i> (Paul, 27, Financial Services professional).</li> </ul>	Awareness of general privacy news coverage and health specific privacy news are both included.
Risk beliefs	<ul style="list-style-type: none"> <li>• Individuals viewed the risks differently for health professionals and technology vendors. <i>‘I don’t think health professionals would misuse my information, but tech companies you just don’t know their motives’</i> (Paul).</li> <li>• <i>‘I think health professionals would have better intentions’</i> (Sean, I.T. Professional, 52).</li> </ul>	Risk beliefs regarding health professionals and technology vendors vary greatly.
Trust beliefs	<ul style="list-style-type: none"> <li>• Individuals expressed different levels of trust in health professionals and technology vendors. <i>‘I’ve had great experiences with health professionals, I completely trust my doctor, she has shown herself to be competent and respectful [...] but technology companies I’ve no trust in them, their goal is to make money’</i> (Mary).</li> </ul>	Trust in health professionals and technology vendors varies greatly.

In addition, due to repeated occurrence in interviews, one new factor was added to the survey.

Table 4.3 briefly explains and justifies the inclusion of this factor.

**Table 4.3 Additional Antecedents**

Factor	Description	Example from data	Hypothesis
Perceived ownership	Interviewees repeatedly expressed ownership over their health data.	<ul style="list-style-type: none"> <li>• <i>'It's information about MY health, it's MINE</i> (Rachel)</li> <li>• <i>'Health information is inherently linked to you, it represents your health, your physical or mental condition and I feel like that belongs to me'</i> (Joe)</li> </ul>	Individuals with high levels of perceived ownership will express high HIPC.

To address the second research question, the dimensions of HIPC were explored through open questions such as: *What privacy concerns do you have regarding your health information?* This approach enabled interviewees to discuss concerns in their own words. To ensure each dimension was addressed, any dimensions not discussed during open questioning were described and the interviewee was asked whether it presented a current or potential future concern. Based on the findings, all six dimensions are deemed relevant to the health context. Table 4.4 provides examples of support for each dimension.

**Table 4.4 Dimensions of HIPC**

Dimension	Quote illustrating relevance
Collection	<i>'It worries me when I get asked for information about my health or illnesses that seems irrelevant or excessive'</i> (Mary).
Unauthorised Secondary Use	<i>'I wonder what else will they use it for, like the thoughts of my health data being used for marketing or research without my knowledge is very scary'</i> (Joe).
Improper Access	<i>'I worry about anyone from my neighbour, to my boss or the government somehow accessing my health information'</i> (Joy).
Errors	<i>'I don't know what my health record contains and I can't correct false information, there's always a risk of mistakes and false information leaking that could have damaging impacts'</i> (Sean).
Control	<i>'I can't control how my health information is used and I wish I could control who can access it or what it can be used for, that would make me feel better'</i> (Paul).
Awareness	<i>'It really bothers me that I don't know who sees my health information, like I've literally no idea who can see it'</i> (Rachel).

Concerns mentioned by interviewees which did not bear obvious resemblance to any of the HIPC dimensions were also reviewed. There were two concerns in this ‘Unidentified’ category. The first concern mentioned by two interviewees, related to fear of being monitored by companies and governments. Upon listening back to these interviews and using questioning and comparison techniques, it became apparent that the Unauthorised Secondary Use dimension in HIPC encompasses this concern. Monitoring individuals’ activities and passing data on to government bodies can be considered additional uses for health data which may concern an individual. The second concern related to ‘possible repercussions’ of access to health data and included fears of identity theft and fear of employers using health data when making hiring decisions. While these concerns are valid, they cannot be described as concerns for health data privacy, but rather concerns regarding possible repercussions stemming from improper access to health data. This is as an outcome of Improper Access, but not a dimension of concern in itself.

The third research question investigates the relationship between HIPC and citizens’ intentions to adopt health ICTs. The interviews provided some initial support for the negative influence of HIPC on intentions, as evidenced in the following quote. Paul stated: *‘Apple Health wanted allergy and health information, I see the benefit in an emergency but I decided not to use it because I’ve no idea why Apple want that information and how they would use it and once you give it to them, it is out of your control’*. This quote illustrates the consideration given by Paul to the benefits and risks associated with health ICTs before deciding not to adopt, thus also supporting the inclusion of the Privacy Calculus theory in the research framework.

## **4.7 Stage Two: Survey**

In stage two of the study, a survey was conducted to test the proposed relationships in the refined research framework among the U.S. and Irish samples (Johnson and Turner, 2003).

#### **4.7.1 Survey Design and Pilot Testing**

Due to the time constraints imposed on data collection, all variables were measured at the same time using the same set of respondents. This approach can generate fears regarding common method bias (CMB). CMB can inflate or deflate the observed relationships resulting in Type I and Type II errors (Podsakoff *et al.*, 2003). In order to reduce the potential negative effects of CMB, various procedural remedies recommended by MacKenzie, Podsakoff, and Podsakoff (2011) were applied during survey design. These remedies include psychologically separating endogenous and exogenous variables, offering descriptions of new terms and technologies, ensuring all items were unambiguous, notifying respondents that there were no right or wrong answers, varying scale anchors, guaranteeing anonymity, and guaranteeing personal details volunteered would only be used to schedule interviews. Statistical measures to explore the presence of CMB were also applied, and are discussed in the following chapter.

To further validate the instrument, the survey was pilot tested on several groups (Johnson and Turner, 2003). In the first instance, the survey was piloted among a group of academics with expertise in survey development in MIS and Health disciplines in the U.S. and Ireland. These experts provided advice on rewording items, clarifying section descriptions, and the inclusion of additional items. The survey was refined based on these recommendations. Following this, the survey was pilot tested among a sample of 10 Irish citizens representing the three sample groups. These individuals provided feedback on unclear questions or instructions. The survey was again refined based on this feedback. For example, as 7-point scales caused confusion among older respondents, all scales were reduced to 5-points. The updated survey was again reviewed by academics and amended until it was deemed satisfactory.

### 4.7.2 Survey Structure

The survey (see Appendix F, pg. 290) is comprised of the following six sections:

- Section 1: Technology Experience
- Section 2: Privacy Experiences & Perceptions
- Section 3: Health Experiences & Perceptions
- Section 4: Health Information Privacy Concerns
- Section 5: Technology Adoption Intentions
- Section 6: Personal Characteristics

### 4.7.3 Measurement of Variables

This section discusses the measurement of variables in each section of the survey. The majority of items were adapted from previously validated scales. Due to the application of variables in the health context for the first time, many items required rewording. While the majority of variables were measured using multiple item scales, a small number were measured using single item scales, due to the lack of multi-item measures in the existing literature. The chosen one item scales are deemed sufficient as these variables have been previously measured with one item and are all distinct and easily understood (Hair *et al.*, 2010). The sources for all survey items are outlined in Appendix G, pg. 307.

**Section I: Technology Experience:** The first section gauged respondents' level of experience with the Internet and using Internet technologies for health purposes. The section began with the question '*Approximately how long have you been using the Internet?*' with five options ranging from less than 1 year to over 15 years. The following four questions formed the health information seeking variable based on Kim and Park (2012) and included items such as '*I search online for information related to disease diagnosis*'. Five options were provided ranging from 'never', to '4 times a week - everyday'. While Kim and Park (2012) examined whether or not individuals engaged in these activities, this survey tested the frequency of engagement as this gives a greater insight into individuals' utilisation of the Internet as a source of health information. Based on

feedback received, a question was added to test if individuals use social media to source health information.

The next question was interested in individuals' use of mHealth applications. Again the frequency was gauged using the same intervals. Categories of mHealth applications derived from Fox and Duggan's (2012) were included to explore diversity of use. Lastly, individuals were asked to indicate their experience of using personal health records and wearable devices.

**Section II: Privacy Experience and Perceptions:** This section was comprised of several variables. Firstly, individuals experience of privacy invasion was explored. Following the exploratory interviews, it was decided to examine individuals' experience of privacy invasion in terms of personal information and health information. In order to capture both experiences of privacy invasion, two items were developed based on Bansal *et al.*, (2010). Individuals were asked to indicate the frequency of their experience across 5 points ranging from 'never' to 'very often'. The second variable related to individuals' privacy media coverage awareness. This variable also focused on information privacy issues in general, and health privacy issues. The variable consisted of two items taken from Smith *et al.*, (1996). Based on pilot testing, two items were added to explore individuals' knowledge of privacy legislation regarding (1) personal information and (2) health information. Individuals were asked to rank their knowledge across five points ranging from 'none' to 'very extensive'.

The next variables related to perceptions of trust and risk. Items for these variables were derived from Li *et al.*, (2014), and Hong and Thong (2013). Trust perceptions regarding health professionals and technology vendors were examined separately. In both instances, trust was measured using six items such as: *'I know health professionals are always honest when it comes to using my health information'*. Risk perceptions were also examined separately for health professionals and technology vendors. In both instances, risk was measured using 4 items such as: *'There would be high potential for loss associated with disclosing my health information to technology vendors'*. For trust and risk variables, individuals were asked to indicate their agreement using a 5-point Likert scale ranging from 'strongly disagree' to 'strongly agree'.



**Section III: Health Information & Perceptions:** This section included several health variables. The first variable, healthcare need, was measured using three items from Wilson and Lankton, (2004), and Angst and Agarwal (2009) including: '*How many prescriptions do you take?*'. Answers for these questions were on a numeric scale ranging from 0 to 10+. Due to the sensitivity of these questions, the option 'I'd rather not say' was added. The second variable, health status was examined with three items from Bansal *et al.*, (2010). These items focused on individuals' pain with higher scoring indicating poorer health. All items were measured on five-point Likert scales, with options for the first two items ranging from 'strongly disagree' to 'strongly agree', and options for the third item ranging from 'excellent' to 'poor'.

Two questions were included which asked respondents to indicate if they had (1) a chronic illness and (2) an illness they deemed sensitive. Stigmatisation was then explored separately for chronic illnesses and sensitive illnesses using two questions, one focusing on individuals' past experience of differential treatment due to their illness (5-point frequency scale 'never' to 'very often'), and the other focusing on fear of possible differential treatment (5-point agreement scale). The final variable related to perceived sensitivity. Individuals were asked to indicate the sensitivity of different health data types on a scale ranging from 'not sensitive at all' to 'extremely sensitive'. Twelve data types were included based on Laric *et al.*, (2009), and Caine and Hanania (2013).

**Section IV: Health Information Privacy Concerns:** This section explored individuals' HIPC. The Internet Privacy Concerns (IPC) measure which was developed, rigourously tested, and validated by Hong and Thong (2013) was chosen due to its comprehensiveness. The measure was adapted to the health context and termed HIPC. The measure included six dimensions: Collection (4 items), Unauthorised Secondary Usage (3 items), Improper Access (3 items), Errors (3 items), Control (3 items), and Awareness (3 items). This study was the first to apply the IPC measure to the health context, but four of the six dimensions had been tested in this context by Angst and Agarwal (2009). While their study supports the relevance of these dimensions, the wording conventions utilised by Hong and Thong (2013) were followed, as opposed to those used by Angst and Agarwal (2009). Hong and Thong noted that items in older measures of concern

were worded in terms of individuals' perceptions of what organisations *should* or *should not* do with their information. In IPC, they reworded these items to reflect individuals' concerns regarding what organisations *actually do*. They found that the reworded items were more effective in measuring concerns. For example, an item from Angst and Agarwal (2009) in the Improper Access dimension is: '*Health care entities should take more steps to make sure that unauthorised people cannot access personal information in their computers*'. In this study the corresponding item is: '*I am concerned that health care entities do not take enough steps to make sure that unauthorised people cannot access my personal health information in their computers*'. For each item, individuals were asked to indicate their level of agreement on a five-point Likert scale. In their study, Hong and Thong (2013) tested 12 factor order structures for the IPC measure before concluding that a third order factor structure was most suitable. In this study, a second order factor structure was tested, with the six dimensions of HIPC treated as first order factors, which load onto a second order general factor representing overall HIPC. Second factor structures have been tested and supported in many information privacy studies (e.g. Stewart and Segars, 2002; Malhotra *et al.*, 2004). In addition, third order factor structures are often critiqued for being too obscure.

**Section V: Technology Adoption Intention:** This section examined individuals' health ICT adoption intentions. A neutrally framed summary of EHRs was first presented. Based on this description, individuals' intention to accept the EHR was measured using three items from Bansal *et al.*, (2010). Individuals were also asked how often they would access their EHR. Next, brief descriptions of mHealth applications, PHRs, and wearable devices were presented. Individuals' intentions to adopt mHealth was explored broadly using three items from Venkatesh *et al.*, (2003). For individuals with prior experience using mHealth solutions, intentions to continue use were examined with these three items. Individuals were then asked how frequently they would use each of the three mHealth technologies described. Perceived benefits of EHRs and mHealth were measured based on Wu *et al.*, (2007), and Or *et al.*, (2011).

**Section VI: Personal Characteristics:** A number of personal questions were included such as gender, age, employment status, academic discipline (students), and industry (employed/self-employed). Based on the recommendations received during pilot testing, a question was added which asked respondents to rate their concerns if their health information was not protected. The options included; losing my job, having my identity stolen, and financial theft.

**Control variables:** The influence of a number of variables on adoption intentions were controlled for, due to the study's focus on the relationship between HIPC and adoption. The first control variable, perceived self-efficacy was measured in terms of individuals' ability to use mHealth to manage their health using 5 items based on Kim and Park (2012) and Or *et al.*, (2011). Secondly, social influence related to EHRs and mHealth was examined separately using 3 items each based on Or *et al.*, (2011).

**Additional variables:** Following exploratory interviews, perceived ownership of health data was also included in the survey. Perceived ownership was measured using three items derived from the psychological ownership construct which has been operationalised in organisational behaviour studies such as Avey *et al.*, (2009). These items included; *'I feel a very high degree of ownership over information related to my health'*. Individuals were asked to indicate their agreement with each statement on a 5 point Likert scale.

**Differences in U.S. and Irish Survey:** The minor differences in the survey circulated among U.S. and Irish samples are briefly noted. Firstly, the U.S. survey followed U.S. English grammar and spelling. Secondly, individuals in the U.S. were asked to rank their knowledge of HIPAA as opposed to health legislation in general in the Irish version. Lastly, EHRs are used by many U.S. healthcare providers. To accommodate this, a question was added to section 5, based on Angst and Agarwal (2009), which asked individuals if their healthcare providers currently used an EHR. Individuals who answered negatively or expressed uncertainty, received the same questions as the Irish sample to gauge their intentions to accept an EHR. Those who indicated that their healthcare providers already used EHRs did not receive these questions.

#### **4.7.4 Summary**

Surveys contain potential weaknesses including length restrictions, possibility of missing data, non-response to some items, possibility of social desirability, and low response rates (Johnson and Turner, 2003). Bearing that in mind, this survey was designed in ways which limit these weaknesses. Only important variables were included to limit the length, and only complete responses were used in analysis. Instructions and descriptions were worded neutrally to limit any possible social desirability effects. As many of the variables were tested in the health context for the first time, extensive pilot testing was conducted. The following chapter details the extensive testing of the quantitative data to ensure internal and external validity, and reliability thresholds were met in line with recommendations (Venkatesh *et al.*, 2013; Straub *et al.*, 2004).

### **4.8 Stage Three: In-depth Interviews**

The final stage of data collection involved semi-structured interviews. The aim of these interviews was to develop a deeper understanding of the relationships of interest. A total of 50 interviews (25 in Ireland and 25 in the U.S) were conducted. Each set of interviewees represented the three sample groups outlined in Section 4.5. All interviews were conducted in person with the exception of three interviews conducted via Skype due to the location of participants (1 in Ireland, 2 in the U.S.). Irish interviews took place in a private room at the University. Interviewees were asked to sign a Research Consent form prior to commencing the interview (See Appendix H, pg. 311). The majority of U.S. interviews were conducted in a private office at ASU's Tempe campus, with a smaller number conducted on the Downtown campus. Interviews lasted between 20–60 minutes.

Interviews followed a broad interview guide (see Appendix I, pg. 312). The interview guide was prepared to ensure all topics were encapsulated, unambiguous language was used when introducing questions, all questions were neutral and not leading, topics were broad so as not to influence answers, and questions regarding individuals' background were included to provide context (Bryman and Bell, 2007). This interview guide was pilot tested on 3 Irish citizens. Based

on feedback received during pilot testing, the interview guide was refined to ensure all questions were clear, and explanations of new concepts were provided. Interviews addressed all constructs measured in the survey, but on a deeper level digging into interviewees' personal experiences and perceptions. Each interview was audiotaped following the guidelines outlined by Poland (1999) to achieve clear, high quality recordings. Several guidelines were followed throughout interviews to create a comfortable atmosphere and gain as much insight from each interview as possible. These included clearly explaining the purpose of the interview, asking the interviewee if they had any questions, allowing the interviewee time to finish answers, and clarifying the meaning of answers (Kvale, 1996; Bryman and Bell, 2007).

Each topic was represented by various question types such as introductory, follow-up, probing, and specifying questions covering various phenomena from beliefs to behaviour (Kvale, 1996). For example, open-ended questions were used to explore individuals' HIPC, their perceptions, and their experiences relevant to each antecedent, and their attitudes towards health ICTs. These questions were supplemented with close-ended questions to gauge individuals' intentions to use health ICTs, any conditions they would impose on this use, and the importance they place on privacy. Memos were written throughout and immediately after each interview to note points stressed by the interviewee and develop new questions for subsequent interviews. Each interview was analysed using questioning and comparison techniques. As qualitative methods are often critiqued for failure to demonstrate validity, a number of methods were utilised to ensure the data met design validity, analytical validity, and inferential validity thresholds (Venkatesh *et al.*, 2013). Analysis techniques applied, primary qualitative findings, and validation methods are discussed in the qualitative analysis chapter.

## **4.9 Conclusion**

This chapter outlined the philosophical assumptions and methods supporting the research. Mixed methods research presents many benefits and opportunities to enhance knowledge. It is argued that the mixed methods approach presented in this chapter represents the most appropriate means

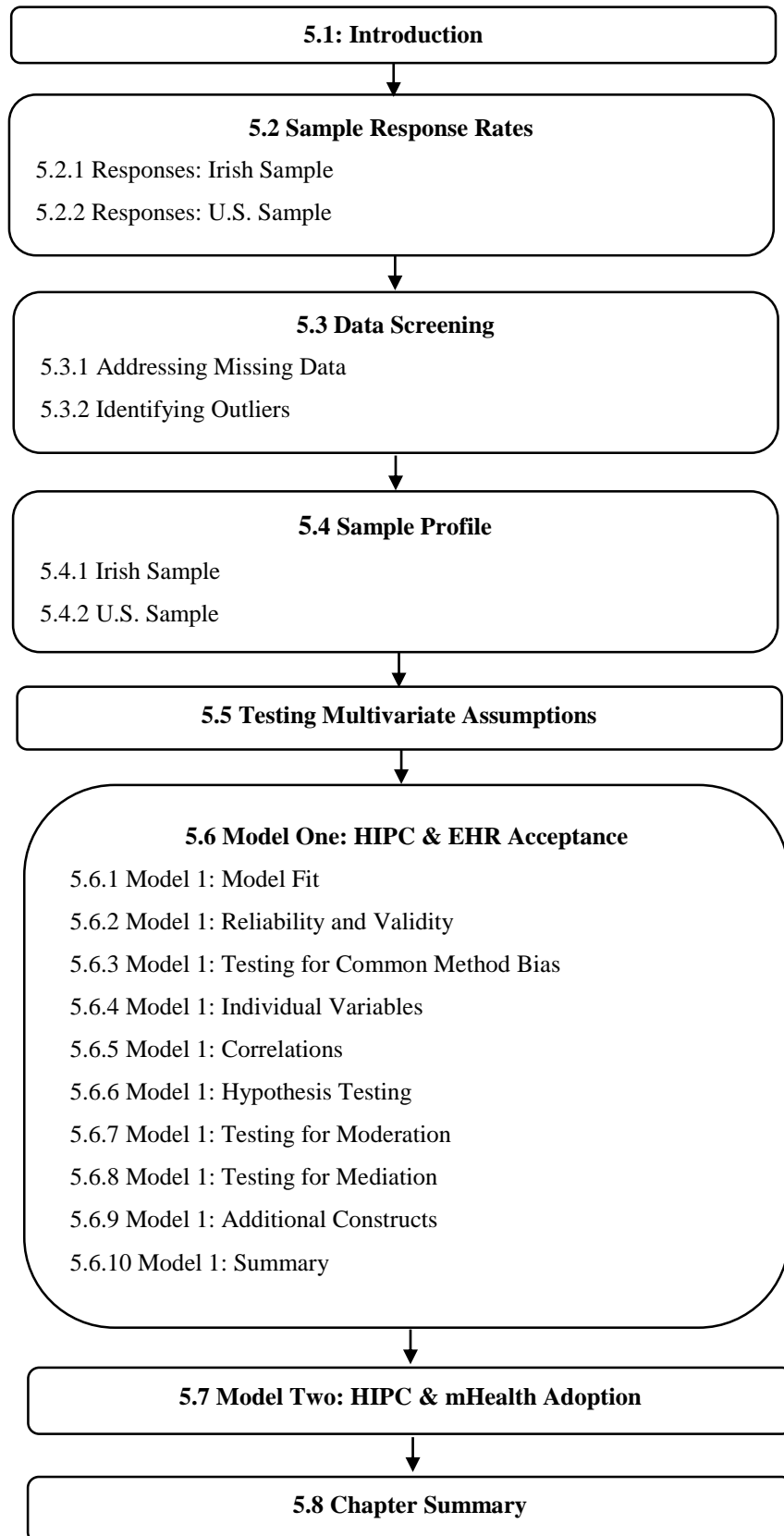
to answer the study's research questions. Data were collected in three stages. Firstly, exploratory interviews were conducted to refine the research framework. Secondly, the survey was rolled out in the U.S. and Ireland. Lastly, in-depth interviews were conducted to delve into the issues of interest on a deeper level. As mixed methods studies are often critiqued for being less rigorous than single method studies, it is imperative to conduct each component with rigour (Morse, 2003). Both quantitative and qualitative data were subject to rigorous testing and analysis, prior to the integration of the data. Integration enables the development of meta-inferences, which provide rich insights into the constructs of interest. Meta-inferences were also subject to rigorous validation following the guidelines of Venkatesh *et al.*, (2013). These integrated insights can advance understanding of the relationship between citizens' HIPC and health ICT adoption. The following two chapters discuss the quantitative, qualitative, and integrated findings, along with the methods used to validate the data.

## **CHAPTER FIVE: QUANTITATIVE DATA ANALYSIS**

### **5.1 Introduction**

This chapter provides a detailed account of the study's quantitative analyses and findings. The structure of the chapter is visually depicted below in Figure 5.1 (pg. 125). The chapter begins with a discussion of the data screening processes carried out. The sample response rates are then discussed, along with an overview of the sample characteristics. The research framework developed from the Literature Review and exploratory interviews is tested using two models. Each model is discussed individually in terms of the reliability and validity of the model, the factor structure, and the proposed relationships. The chapter concludes with an overview of the main hypotheses and quantitative results.

**Figure 5.1 Chapter Structure**





## **5.2 Sample Response Rates**

This section outlines the study response rates. As noted in the previous chapter, three age groups were included in the Irish and U.S. samples. The first group is comprised of individuals aged 18-24, many of which are third level students or recent graduates. These individuals are technologically savvy, and are likely to express lower Health Information Privacy Concerns (HIPC). The second group consists of individuals aged between 25 and 49, who are employed in various industries. The third group is represented by older individuals aged 50 and above, who are either employed or retired. These individuals are likely to express high HIPC.

### ***5.2.1 Responses: Irish Sample***

The response rates for the Irish sample are discussed in this section. Responses for the first two age groups were collected online. As email invitations were sent to a number of different groups, an approximate response rate is calculated. Email invitations were sent to students on various Business, Information Technology, and Health Undergraduate and Postgraduate programmes by the Head of the Course. Due to students' familiarity with the Head of Course, it is argued that their endorsement of the study may increase responses (Dillman, 2007). The email invitation was sent to an estimated 360 students. A total of 48 complete survey responses were received from students. This equates to an approximate response rate of 17.14%. For the second group, the survey invitation was administered through email lists and LinkedIn Alumni groups. Email invitations to alumni of Dublin City University (DCU) were sent by the Access Office and emails sent to individuals at the Insight research centres were sent by an Insight employee, again due to familiarity. It is estimated that a total of 420 individuals representing the second group received the email invitation. From this group, 111 complete responses were received. This equates to a 26.42% response rate.

To distribute the survey to the third age group, the researcher attended classes at MedEx and the Intergenerational Learning Programme (ILP) at DCU. Individuals in these classes could complete the survey online or via hard copy. In total, 128 individuals at MedEx received either a hard copy

of the survey or an online link via email. Of these individuals, 65 complete responses were received yielding a response rate of 50.7%. The survey was also administered to 37 learners at ILP, resulting in 20 completed surveys and a response rate of 54.1%. The high response rates among the MedEx and ILP groups may be attributed to the support from staff at ILP and MedEx. This endorsement is likely to have validated the research in the eyes of participants. The researchers' presence to answer questions may have also played a role. Across the three groups, 302 surveys were started, and 247 were fully completed, representing a completion rate of 81.78%.

### **5.2.2 Responses: U.S. Sample**

In the U.S., all responses were collected online. Two sampling strategies were followed. Firstly, advertisements for the research were posted on ASU student and faculty portal pages. Secondly, email invitations were sent to 214 individuals of various ages and backgrounds who had partaken in previous research, and approximately 250 students on Business, Information Technology, and Health Undergraduate, Postgraduate, and M.B.A programmes at ASU. As it is not possible to determine how many people viewed the advertisements, an approximate response rate cannot be calculated. However, with 280 surveys started and 202 completed, the completion rate was 72.5% for the U.S. sample.

## **5.3 Data Screening and Preparation**

Prior to testing the proposed models, the data must be screened and cleaned. This section discusses the processes involved in data preparation including screening for missing data and handling outliers.

### **5.3.1 Addressing Missing Data**

The first element of data screening involves identifying and rectifying any issues associated with missing data. Missing data was addressed in accordance with the four step process recommended by Hair *et al.*, (2010). The first step involved determining whether missing data was ignorable or

non-ignorable. Ignorable missing data was found in variables which did not target all respondents. For example, questions pertaining to stigmatisation were only answered by respondents with chronic or sensitive illnesses. Missing data across these variables was expected and was thus deemed ignorable. The second type of missing data is missing for an unknown purpose and cannot be ignored. All missing data which was not anticipated was deemed non-ignorable. The second step involved determining the extent of the non-ignorable missing data, the aim being to ensure missing data would not affect the overall results. First, missing data across each variable was reviewed. The extent of the missing data for each item was minor, accounting for a mere 1% of the overall sample. Individual cases with missing data were then reviewed. With no obvious pattern emerging in the missing data and no individual case missing over 10%, the missing data was unlikely to represent a problem (Hair *et al.* 2010). Step three involved diagnosing the randomness of missing data using missing value analysis in SPSS. As no significant differences were found between complete cases and cases with missing data, the missing data was labelled missing completely at random (MCAR). The last step involved deciding upon the appropriate imputation method for the missing data. The maximum number of missing cases for any item was 6 or approximately 1% of the sample, thus any imputation method could be chosen. Replacement values were calculated using the mean value for the item, as this is a commonly chosen imputation method.

### **5.3.2 Identifying Outliers**

Outliers must also be detected and addressed. The distribution of each variable was reviewed using boxplots to explore the presence of univariate outliers. As all variables were measured on ordinal scales with five points, there were no *truly* extreme values. However, all cases with values which could be considered extremely high or low were reviewed individually to establish possible reasons for these values. In line with best practice (Hair *et al.*, 2010), the aim was to retain all cases unless evidence suggested the case was aberrant. Two aberrant cases were identified. Both of these cases had an exceptionally low standard deviation in their answers across all variables. These cases can be described as unengaged respondents (Gaskin, 2012a). Both cases were thus

removed. All remaining cases with extreme values were retained, as the extreme responses could be theoretically justified. For instance, it was unsurprising that individuals with a sensitive illness responded highly on HIPC items.

## **5.4 Sample Profile**

This section provides an overview of the U.S. and Irish sample profiles. A total of 449 complete responses were received. As noted above, two cases were removed, resulting in a sample of 447.

### ***5.4.1 Profile: Irish Sample***

Of the 245 complete responses received, 51.4% were male and 48.6% were female. The sample varied in terms of employment status with 19.6% students, 50.2% employees, 26.5% retired, and 3.7% jobseekers or homemakers. A total of 20.0% were aged between 18 and 24 representing the first group, 45.7% were aged between 25 and 49 representing the second group, and the remaining 34.3% were aged 50 and over, representing the third group. Individuals of varying educational backgrounds were included: 29.8% of respondents had reached Postgraduate level or beyond, 29.0% had an Undergraduate degree, 19.6% had completed some college, and 21.6% completed part or all of Secondary school. Internet experience was high for the large majority of the sample with 31.8% of respondents stating they had 5-10 years of Internet experience, a further 28.2% and 28.6% had 10-15 years and over 15 years of experience respectively. A mere 11.4% had 1-5 years of experience. In terms of health status, 29.4% of respondents had a chronic illness, 17.1% stated they had an illness which they felt was of a 'sensitive or embarrassing nature', and 33.2% had another illness which impacted their life periodically.

### ***5.4.2 Profile: U.S. Sample***

Of the 202 responses received, 77.2% of respondents were female and 22.8% were males. With regards to employment status, 41.6% were students, 52.4% were employees and the remaining 5.9% were homemakers or jobseekers. In terms of age, 32.2% were aged 18-24 representing the first group, 54.4% were aged between 25 and 49 and were in the second group, and the third group

was comprised of the remaining 8.4% aged 50 and over. The distribution of education was as follows; 3.0% had completed some secondary level education, 40.1% had completed some third level education, a further 29.2% had Undergraduate degrees, and the remaining 27.7% had reached Postgraduate level or beyond. While data collection took place in Arizona, individuals from all over the U.S. were reached due to the large volume of online students, and the geographical distribution of individuals who had participated in previous research at ASU. In terms of Internet experience, a mere 1.0% had been using the Internet for 1-5 years, and 8.4% of respondents had 5-10 years of Internet experience. The vast majority were more experienced with 30.7% of respondents stating they had 10-15 years of experience, and the remaining 59.9% had over 15 years of experience. In terms of health status, 28.7% had at least one chronic illness, 24.3% had a sensitive illness, and 52.0% had an illness which periodically impacted their life.

## **5.5 Testing Multivariate Assumptions**

Prior to conducting multivariate analysis, the data must meet four assumptions. Firstly, the normality assumption must be satisfied. If data deviates largely from the normal distribution, findings from all subsequent analysis are deemed invalid (Hair *et al.* 2010). In order to test for normality, the distribution of each variable was visually explored using histograms. The skewness and kurtosis of all items was also reviewed. None of the items breached the kurtosis threshold of  $\pm 2.2$  required for proving normal univariate distribution (George and Mallery, 2010). However, several items across a number of variables including health information seeking (1 item), media coverage (1 item), trust in health professionals (2 items), healthcare need (1 item), and perceived sensitivity (1 item) ranged between  $\pm 1$  and 2. These items were retained as they did not breach the threshold, but were monitored for future analyses due to their borderline kurtosis statistics. Secondly, the linearity assumption must be fulfilled, as non-linear data represents a problem in multivariate analysis. Linearity was tested using the deviation from linearity test in SPSS. This test explores the linearity of relationships between dependent and independent variables in the data. If the deviation from linearity is significant for any of the relationships, this indicates that the relationship may not be linear (Gaskin, 2012a). For the first

dependent variable, intention to accept an EHR, the relationship with each of the independent variables was linear. For the second dependent variable, intention to adopt mHealth, the relationship with two independent variables (risk perceptions and healthcare need) had a significant deviation from linearity, suggesting the relationships may not be linear. To rectify this issue, the dependent variable was transformed using the log10 method. Following this transformation, the relationships met the thresholds required for linearity.

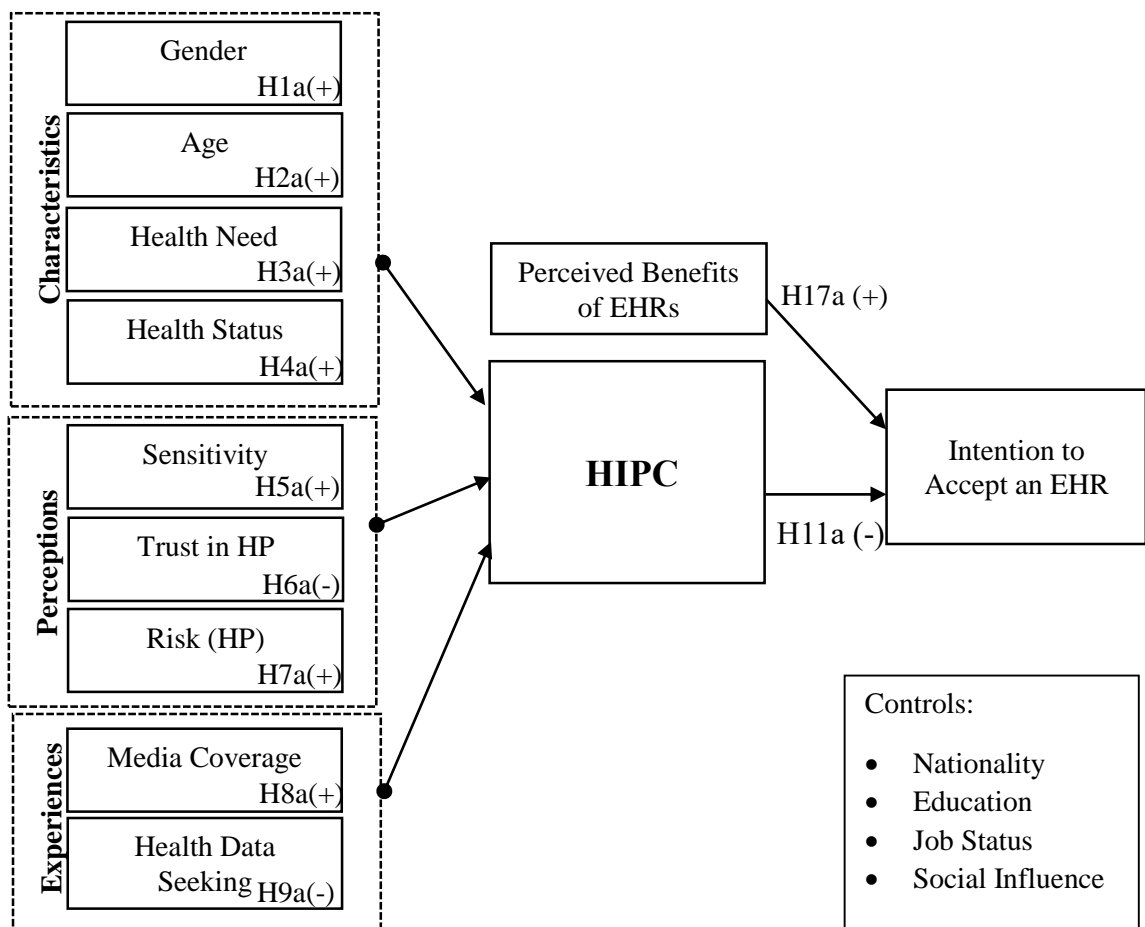
The third assumption relates to homoscedasticity. Homoscedasticity is desired and achieved when the variance of dependent variables is relatively equal across the range of the independent variable (Hair *et al.* 2010). When this variance is unequal, the relationship is heteroscedastic. The homoscedasticity of all relationships between the dependent variables and each of the independent variables was tested graphically. For each relationship, the scatterplot of the dependent variable and its residuals displayed a consistent pattern. The data therefore meets the homoscedasticity assumption. The final assumption involves detecting multicollinearity. This was tested by calculating the Variable Inflation Factor (VIF) for both dependent variables. As all VIF scores were under 3 for both dependent variables, multicollinearity is not an issue. Thus all assumptions are met and the next stages of analysis can be carried out. The remainder of the chapter discusses the testing of both models separately.

## **5.6 Model 1: HIPC and EHR Acceptance**

This section focuses on model 1, and begins with an outline of the model and the hypothesised relationships. The overall model fit is then tested using Confirmatory Factor Analysis (CFA), prior to testing the validity and reliability of the model. The procedures conducted to test for common method bias are also discussed. Each variable is then discussed individually. Lastly, the proposed structural model, moderators, mediators, and additional constructs are tested in AMOS using Structural equation modelling (SEM). The first model in the study explored the influence of citizens' Health Information Privacy Concerns (HIPC) on their acceptance of an Electronic Health Record (EHR). Model 1 included the entire Irish sample (n= 245) due to plans

to introduce a national EHR in Ireland, and U.S. respondents who stated their healthcare provider did not currently use EHRs, resulting in a sample of 320. The proposed antecedents to HIPC include individual characteristics, perceptions, and experiences. In terms of characteristics, it was hypothesised that females would express higher HIPC, and age, healthcare need, and poor health status would positively influence HIPC. In terms of perceptions, it was hypothesised that perceived trust in health professionals (HP) would reduce HIPC, perceived risks associated with disclosing health data to health professionals (HP), and perceived sensitivity would increase HIPC. In terms of experience, it was hypothesised that privacy media coverage awareness would increase HIPC, and online health information seeking would reduce HIPC. HIPC was measured using six first order constructs which all load onto a second order general factor of HIPC. It was posited that HIPC and perceived benefits of EHRs would influence intention to accept an EHR. The proposed model is outlined below in Figure 5.2, along with the main relationships.

**Figure 5.2 Proposed Model 1**



### **5.6.1 Model 1: Model Fit**

For the first step of analysis, the factor structure for the model was tested using confirmatory factor analysis (CFA) in AMOS 21. Normally, exploratory factor analysis (EFA) might be conducted prior to conducting CFA. However, HIPC, the focal variable in this study is a second order construct. With second order constructs, cross loadings across the first order factors are expected due to the assumption that all first order factors load on to the second order factor (Gaskin, 2012b). These cross loadings render it impossible to generate a clear pattern matrix. Thus, this study omitted exploratory factor analysis and tested the factor structure using CFA.

A number of items with low standardised regression weights were removed to improve the model fit statistics. Items 4 (.53) and 5 (.56) were removed from health information seeking. These two items had clear differences in wording when compared to the remaining items, as they focused on individuals' experience of purchasing health products online and using social media as a source of health information. The remaining items focus on individuals' experience of searching for health information online for purposes such as learning or diagnosis. It is thus argued that the remaining three items represent a stronger measure of individuals' health information seeking behaviours than the original measure. Items 2 (.63) and 5 (.55) were removed from trust in health professionals. These two items related to individuals' perceptions of health professionals' care for patients and ability to do their job competently, whereas the remaining items focus on individuals' perceptions of health professionals' integrity and benevolence when handling their health data. The remaining items are arguably more relevant as they relate to health data. Items 1 (.43), 2 (.59), and 3 (.43) were removed from perceived sensitivity. The removed items focused on individuals' perception of the sensitivity of 'demographic details' and 'fitness levels'. When compared to remaining items such as 'mental health' and 'sexual health', it is clear that the removed items are disparate and less representative of what might be described as health data. Item 3 (.54) was removed from health status. The final measurement model met all goodness of fit statistics prescribed by Hair *et al.*, (2010) for studies with a sample size >250 and >30 observed variables. The measurement model fit statistics are outlined below in Table 5.1.



**Table 5.1 Model fit statistics: Model 1**

<b>Model Fit Statistic</b>	<b>Model 1</b>	<b>Recommended Threshold</b>
Chi Square/Df (Cmin/df)	1.917	Less than 3 = good
CFI	0.911	Above 0.90
SRMR	0.052	.08 or less
RMSEA	0.054	Values of <.07

### **5.6.2 Model 1: Validity & Reliability Testing**

The next step involved determining the reliability and validity of model 1. Firstly, the convergent validity of the model was tested by calculating the Average Variance Extracted (AVE) for each construct. As the AVE for each construct was above .50, the distinct nature of each construct is apparent (Fornell and Larcker, 1981). Thus convergent validity is achieved. Secondly, the discriminant validity of the model was tested by comparing the square root of the AVE and the correlation between each set of two constructs (Hair *et al.*, 2010). This is illustrated in the table below; the square root of the AVE is on the diagonal in bold. All variables are deemed to be discriminately valid, as the square root of the AVE for each construct was greater than intercorrelation values (Gaskin, 2012b). Thirdly, the reliability of each construct was tested by calculating the composite reliability (CR). The CR for all constructs was above the recommended .70 value, indicating reliability (Raykov, 1997). The data is therefore both valid and reliable. Table 5.2 illustrates the findings from validity and reliability testing.

**Table 5.2 Validity and Reliability: Model 1**

	<b>CR</b>	<b>AVE</b>	<b>BEN</b>	<b>TRH</b>	<b>HIPC</b>	<b>INF</b>	<b>RSH</b>	<b>HN</b>	<b>INT</b>	<b>HS</b>	<b>SEN</b>
Benefits of EHRs (BEN)	.87	.55	<b>.74</b>								
Trust in Health Prof. (TRH)	.87	.53	.20	<b>.72</b>							
HIPC	.98	.85	-.16	-.22	<b>.92</b>						
Health Data Seeking (INF)	.75	.55	.28	-.11	-.10	<b>.74</b>					
Risk: Health Prof. (RSH)	.93	.73	-.23	-.53	.40	.00	<b>.85</b>				
Healthcare Need (HN)	.77	.53	-.11	-.12	.14	-.03	.14	<b>.73</b>			
Intention: EHR (INT)	.93	.84	.67	.12	-.27	.21	-.25	-.11	<b>.92</b>		
Health Status (HS)	.90	.80	-.01	.12	.04	-.04	-.17	.47	.06	<b>.90</b>	
Perceived Sensitivity (SEN)	.92	.73	.18	-.10	.09	.20	.00	-.22	.07	-.09	<b>.85</b>

### **5.6.3 Model 1: Testing for Common Method Bias**

As noted in the previous chapter, common method bias (CMB) is a concern when all data are collected from the same set of respondents at the same time. A number of survey design recommendations were followed to limit the potential of CMB. In addition, two statistical tests were conducted to determine whether common method bias was a major issue in the data. Firstly, the Harman's Single Factor test was conducted in SPSS. Common method bias is considered an issue if one factor can explain the majority of shared variance for all constructs in the model (Podsakoff and Organ, 1986). The first emerging factor explained 23.27% of the variance in the model, suggesting common method bias is not a major issue in the data. Secondly, the common latent factor procedure was conducted in AMOS, as recommended by MacKenzie, Podsakoff, and Podsakoff (2011) and Podsakoff, MacKenzie and Podsakoff (2012). This approach involves the addition of a first order common latent factor to the measurement model. All items in the measurement model were loaded as indicators on this common latent factor (CLF). Upon constraining the regression weights for all indicators, the common latent factor accounted for a mere 1% of total variance. This is considerably low compared to other studies, which observed an explained variance of 18% (Lance *et al.*, 2010), and 25% (Williams, Buckley & Cote, 1989). Validity and reliability thresholds were still met by all constructs in the model. In addition, the standardised regression weights for each item upon addition of the CLF were compared with those prior to its addition. None of the items experienced a great change upon addition of the CLF. It is thus concluded that common method bias does not represent a concern in this model (Gaskin, 2012b).

### **5.6.4 Model 1: Individual Variables**

Factor loadings, reliability, and validity scores for each variable in model 1 are briefly reviewed in this section beginning with the antecedents to HIPC. The first antecedent, healthcare need, was measured with three items. While the third item had a loading of .65, it was retained due to conceptual harmony with the wording of other items and the small number of items in the

construct. Furthermore, with a sample size of 320, arguments can be made for retaining factors with loadings as low as .40 (Hair *et al.*, 2010). The construct met reliability and validity thresholds with a CR of .77 and an AVE of .53. The second antecedent, health status, was also comprised of three items. The third item was dropped due to a low factor loading of .54, and conceptual disparity with other items. The CR (.90) and AVE (.80) for the revised construct met desired thresholds. The next construct measured trust in health professionals across six items. As noted, two items were dropped during CFA due to low factor loadings and their focus on health professionals' competence. The revised four item construct had a CR of .87 and an AVE of .53. The fourth antecedent perceived risks associated with health professionals was comprised of four items, all of which had high factor loadings. The construct was reliable (CR: .93), and valid (AVE: .73). The next variable measured perceived sensitivity of health data across twelve items. Three items were dropped during CFA owing to low factor loadings. The remaining nine item construct had a CR of .92 and an AVE of .73. Privacy media coverage awareness had two items with high factor loadings, a CR of .77, and an AVE of .62. The final antecedent, health information seeking (INF), originally consisted of 5 items, one of which was added during pilot testing. During the CFA, two items were dropped due to low factor loadings and conceptual disparity with other items. The amended 3 item construct had a CR of .75 and an AVE of .55.

The final independent variable perceived benefits of EHRs, consisted of 5 items. Item 5 had a moderate loading of .62 but was retained due to the large sample size. The construct was deemed reliable (CR: .87), and valid (AVE: .55). The dependent variable, intention to accept an EHR, was comprised of 3 items, all of which had high loadings. The CR and AVE for the construct were also high at .93 and .84 respectively. The focal construct, HIPC was comprised of 19 items across 6 first order constructs, all of which loaded onto a second order HIPC factor. All first order factors loaded highly onto to the second order factor; .90 (Collection), .97 (Unauthorised Secondary Use), .93 (Improper Access), .90 (Errors), .94 (Control), and .89 (Awareness). This supports the second order factor structure. The second order construct was also reliable (CR: .98) and valid (AVE: .85) offering further support for the factor structure. However, in the interest of

rigour, the second order factor was deleted and the construct was explored with a six first order factor structure. Each first order factor was reliable, with CR scores of .84 (Collection), .85 (Unauthorised Secondary Use), .89 (Improper Access), .86 (Errors), .85 (Control), and .88 (Awareness). All six first order factors also met AVE thresholds with AVE values of .57 (Collection), .66 (Unauthorised Secondary Use), .74 (Improper Access), .68 (Errors), .65 (Control), and .71 (Awareness). However, as expected, the first order factors were not distinct from each other, meaning they are not discriminately valid. Thus, the second order factor structure is supported over a first order factor structure.

**Table 5.3 Model 1: Construct Descriptives**

Items	Mean	Std. Dev	Factor Loading	Composite Reliability
<b>Healthcare Need</b>	<b>2.07</b>	<b>0.90</b>		<b>.77</b>
HN1: # Face to face visits to health professionals	1.84	1.09	.80	
HN2: # different health professionals visited	1.86	1.06	.74	
HN3: # of medications	2.42	0.87	.65	
<b>Health Status</b>	<b>2.31</b>	<b>0.87</b>		<b>.90</b>
HS1: Experience of major pains and discomfort	2.47	1.07	.89	
HS2: Severity of condition	2.15	0.76	.90	
<b>Trust: Health Professionals</b>	<b>3.56</b>	<b>0.65</b>		<b>.82</b>
TRH1: Health Professionals are always honest when using my health information	3.47	0.82	.76	
TRH2: Health Professionals are not opportunistic when using my health information	3.48	0.83	.76	
TRH3: Health Professionals are predictable and consistent when using my health information	3.47	0.78	.71	
TRH4: I trust that health professionals keep my best interests in mind when dealing with my health information	3.82	0.81	.667	
<b>Perceived Risks: Health Professionals</b>	<b>2.08</b>	<b>0.80</b>		<b>.93</b>
RSH1: It is risky to disclose health information to health professionals	2.07	0.87	.85	
RSH2: High potential for loss associated with disclosing health information to health professionals	2.14	0.92	.90	
RSH3: Too much uncertainty associated with giving health information to health professionals	2.08	0.87	.88	
RSH4: Providing health professionals with health information would involve many unexpected problems	2.04	0.93	.78	
<b>Perceived Sensitivity</b>	<b>3.54</b>	<b>1.27</b>		<b>.92</b>
SEN1: Test results	3.17	1.40	.70	
SEN2: Health history	3.05	1.39	.70	
SEN3: Mental health	3.78	1.43	.91	
SEN4: Sexual health	3.82	1.44	.89	
SEN5: Domestic abuse	3.77	1.52	.93	
SEN6: Genetic information	3.56	1.53	.89	
SEN7: Plastic surgery	3.12	1.42	.77	
SEN8: Reproductive health	3.79	1.48	.90	

Items	Mean	Std. Dev	Factor Loading	Composite Reliability
SEN9: Addiction information	3.77	1.47	.94	
<b>Awareness of Media Coverage</b>	<b>3.02</b>	<b>0.74</b>		
MED1: Media Coverage pertaining to personal information	3.39	1.21	.80	<b>.77</b>
MED2: Media Coverage pertaining to health information	2.57	1.28	.78	
<b>Health Information Seeking Behaviours</b>	<b>2.17</b>	<b>0.84</b>		
INF1: Search for information related to disease diagnosis and treatment	2.30	.975	.67	<b>.75</b>
INF2: Search for information related to health management	2.58	1.08	.85	
INF3: Search for health information for education, research, or learning purposes	2.53	1.22	.69	
<b>Perceived Benefits. EHRs would:</b>	<b>3.76</b>	<b>0.75</b>		
BEN1: Increase my involvement in my healthcare	3.58	.992	.72	<b>.87</b>
BEN2: Increase my access to my own health information	3.97	.931	.74	
BEN3: Improve my communication with health professionals	3.69	.912	.78	
BEN4: Make managing my healthcare easier for health professionals	3.98	.862	.81	
BEN5: Improve the healthcare I receive	3.59	1.00	.63	
<b>Intention to Accept an EHR</b>	<b>3.57</b>	<b>1.03</b>		
INT1: Likelihood	3.64	1.11	.94	<b>.93</b>
INT2: Probability	3.64	1.09	.91	
INT3: Willingness	3.42	1.08	.89	
<b>HIPC</b>	<b>3.48</b>	<b>0.86</b>	-	<b>.98</b>
<b>Collection</b>	<b>3.12</b>	<b>0.95</b>	-	
COLL1: Bothers me when health entities ask for health information	2.84	1.10	.66	<b>.90</b>
COLL2: I sometimes think twice before providing health information	3.14	1.21	.75	
COLL3: Bothers me to give health information to so many health entities	3.29	1.18	.84	
COLL4: Health entities are collecting too much information	3.21	1.13	.77	
<b>Unauthorised Secondary Use</b>	<b>3.33</b>	<b>1.03</b>	-	<b>.97</b>

Items	Mean	Std. Dev	Factor Loading	Composite Reliability
SU1: Concerned when I give health information to health entities for some reason, they might use it for other reasons	3.15	1.13	.74	
SU2: Concerned health entities would sell my health information to other health entities or non-health related organisations	3.25	1.225	.85	
SU3: Concerned health entities would share my health information with other health entities without my authorisation	3.57	1.15	.84	
<b>Improper Access</b>	<b>3.52</b>	<b>1.01</b>	-	<b>.93</b>
ACC1: Concerned health entities' databases containing my health information are not protected from unauthorised access	3.55	1.10	.85	
ACC2: Concerned health entities do not devote enough time and effort to preventing unauthorised access to my health information	3.48	1.10	.84	
ACC3: Concerned health entities do not take enough steps to ensure unauthorised people cannot access my health information	3.55	1.13	.87	
<b>Errors</b>	<b>3.47</b>	<b>0.98</b>	-	<b>.90</b>
ERR1: Concerned health entities do not take enough steps to ensure my health information in their files is accurate	3.48	1.08	.84	
ERR2: Concerned health entities do not have adequate procedures to correct errors in my health information	3.41	1.14	.82	
ERR3: Concerned health entities do not devote enough time and effort to verifying the accuracy of my personal information in their databases	3.53	1.11	.82	
<b>Control</b>	<b>3.60</b>	<b>0.96</b>	-	<b>.94</b>
CON1: Bothers me when I do not have control of health information that I provide to health entities	3.45	1.12	.80	
CON2: Bothers me when I do not have control or autonomy over decisions about how my health information is used and shared by health entities	3.71	1.10	.84	
CON3: Concerned when control is lost or unwillingly reduced as a result of providing health entities with my health information	3.65	1.06	.80	
<b>Awareness</b>	<b>3.84</b>	<b>0.95</b>	-	<b>.89</b>
AW1: Bothers me when I am not aware or knowledgeable about how my health information will be used by health entities	3.71	1.11	.88	
AW2: Bothers me when health entities seeking my health information do not disclose the way the data are processed and used	3.78	1.08	.86	
AW3: It is very important that I am aware and knowledgeable about how my health information will be used	4.02	.978	.79	



### 5.6.5 Model 1: Correlations

Correlations between all constructs in the model were calculated using Pearson correlation in SPSS. Bootstrapping was also applied to explore the correlations at the 95% confidence interval. As shown in Table 5.4, the majority of proposed antecedents were significantly correlated with HIPC at the .01 level. HIPC was also significantly correlated with intention to accept an EHR, and perceived benefits to the .01 level. In addition, perceived benefits was significantly correlated with intention to accept an EHR, and a number of antecedents were significantly correlated.

**Table 5.4 Model 1: Correlations**

	HIPC	HN	HS	TRH	RSH	SEN	MED	INF	BEN	INT
HIPC	1									
HN	.16**	1								
HS	.05	.54**	1							
TRH	-.25**	-.14**	.14	1						
RSH	.43**	.16**	-.18**	-.59**	1					
SEN	.09	-.25**	-.10	-.11*	.00	1				
MED	.16**	-.08	-.04	-.22**	.12*	.23**	1			
INF	-.11	-.03	-.04	-.13*	.00	.22**	.13*	1		
BEN	-.18**	-.13*	-.00	.23**	-.25**	.19**	.11*	.32**	1	
INT	-.28**	-.12*	.06	.13*	-.26**	.07	.13*	.24**	.72**	1

\* Significant at .05 level, \*\* Significant at .01 level

In summary, confirmatory factor analysis was conducted to test the factor structure proposed in model 1. The model achieved good model fit statistics and each construct met convergent validity, discriminant validity, and reliability thresholds. Common method bias was explored and ruled out as a possible major issue with the data. The second order factor structure proposed for the HIPC construct was also supported. The model was thus deemed appropriate for conducting further analysis. The remainder of this section focuses on testing the relationships hypothesised in model 1.

### 5.6.6 Model 1: Hypothesis Testing

Model 1 investigates the relationship between HIPC and intention to accept an EHR (INT). The first stage in hypothesis testing involved testing the structural model using structural equation modelling (SEM) in AMOS. SEM was deemed appropriate as it enables the representation of

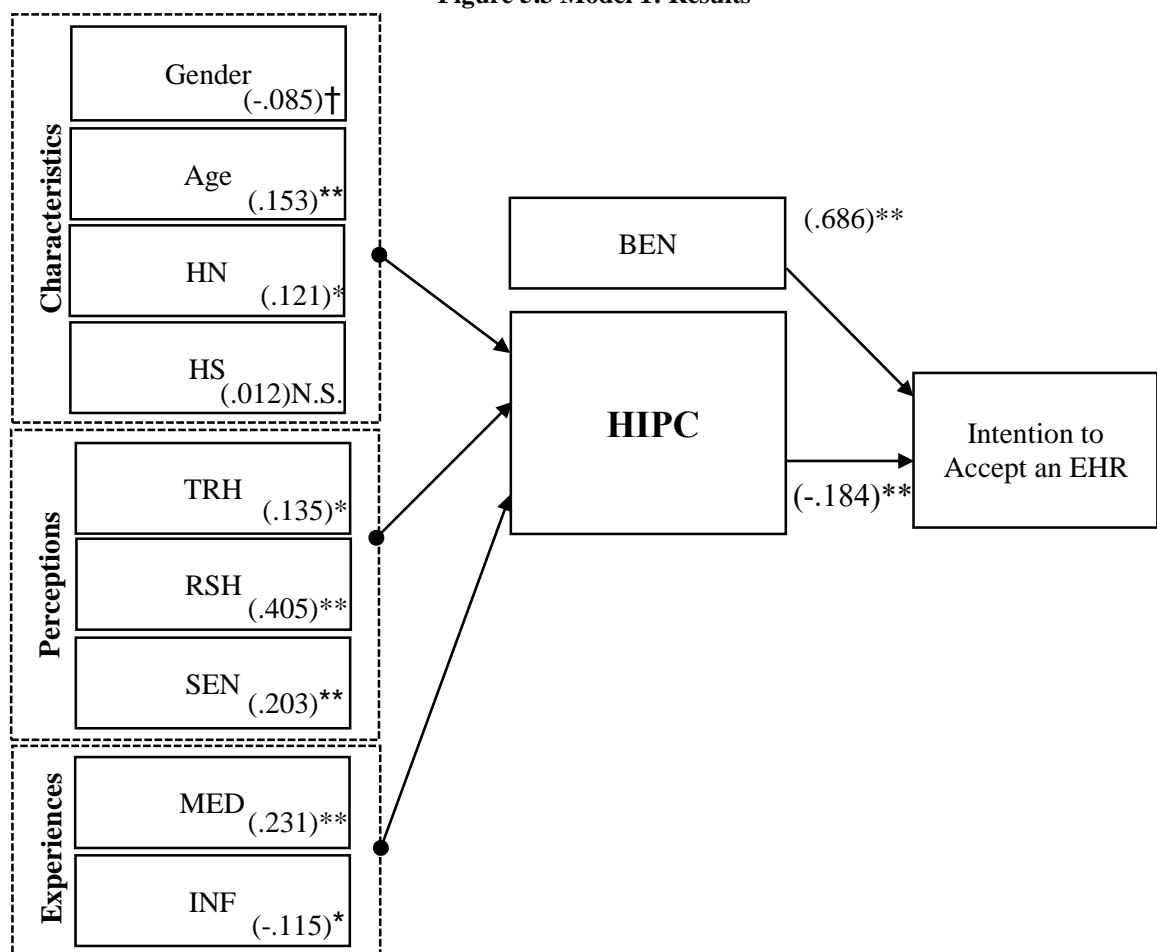
unobserved or latent constructs, corrects for measurement error, and facilitates the examination of multiple, interrelated relationships (Hair *et al.*, 2010). The structural model for model 1 outlined in Figure 5.2 on pg. 132, was tested in AMOS using composites generated during the CFA. The model indicates good fit;  $\chi^2/df$ : 2.419, CFI: .986; SRMR: .026, RMSEA: .067.

The findings for the proposed antecedents to HIPC are first discussed. The influence of individual characteristics was examined in H1a-H4a. Firstly, H1a proposed that females would express higher concerns than males. However, gender was found to have a negative, insignificant influence on HIPC ( $\beta = -.084$ ,  $p = .093 > .05$ ), meaning males expressed higher concerns. H1a is therefore not supported. H2a hypothesised that age would positively impact HIPC. The path analysis revealed the expected positive, significant relationship between age and HIPC ( $\beta = .153$ ,  $p < .01$ ), supporting H2a. It was posited that greater healthcare needs would be associated with higher HIPC in H3a. This relationship was supported in the data ( $\beta = .121$ ,  $p < .05$ ). Similarly, H4a proposed that poor health status would positively influence HIPC. However, this relationship was insignificant ( $\beta = .012$ ,  $p = .838 > .10$ ). Thus, H4a is not supported.

The role of individual perceptions was explored in H5a-7a. Firstly, H5a asserted that perceived sensitivity would positively influence HIPC. This relationship was positive and significant ( $\beta = .203$ ,  $p < .01$ ), supporting H5a. It was proposed that trust in health professionals would negatively influence HIPC. In contrast, SEM analysis revealed that trust had a positive, significant influence on HIPC ( $\beta = .135$ ,  $p < .05$ ). In other words, greater trust led to greater concerns regarding the privacy of health data. H6a is not supported. It was hypothesised that perceived risks regarding health professionals would increase HIPC. This relationship was evidenced in the data ( $\beta = .405$ ,  $p < .01$ ), supporting H7a. Individuals' experiences were investigated in H8a-H9a. It was hypothesised that privacy media coverage awareness (MED) would increase HIPC. The path analysis revealed a significant, positive relationship between MED and HIPC, supporting H8a ( $\beta = .231$ ,  $p < .01$ ). Lastly, H9a proposed that health information seeking behaviours (INF) would reduce individuals' HIPC. A significant, negative relation was evidenced in the data, supporting H9a ( $\beta = -.115$ ,  $p < .05$ ). The remaining hypotheses focused on individuals' intentions to accept

an EHR (INT). H11a proposed that HIPC would reduce intentions. The path analysis revealed that HIPC negatively influenced INT to a significance level of  $<.01$ , offering strong support for H11a ( $\beta = -.185$ ). It also was hypothesised that trust would positively influence intentions, and risk would have a negative influence on intentions. The data revealed that trust had a significant, negative influence on INT ( $\beta = -.142$ ,  $p > .01$ ). Thus, H12a is not supported. Risk had a negative ( $\beta = -.093$ ), and slightly significant influence ( $p = .059$ ), thus offering partial support for H13a. Health information seeking behaviour was expected to positively impact intentions, but this relationship was insignificant, rejecting H14a. Lastly, perceived benefits (BEN) were expected to increase intentions (H17a). The path analysis showed that BEN did positively influence INT to a significance level of  $<.01$  ( $\beta = .690$ ). H18a is therefore strongly supported. The results of the path analysis for the main hypotheses are outlined below in Figure 5.3.

**Figure 5.3 Model 1: Results**



N.S: Not Significant, † = Significant to .10 level, \* = Significant to .01 level, \*\* = Significant to .01 level.

In summary, many of the proposed relationships in model 1 were supported. The model explained 34.7% of the variance in HIPC, and 57.6 % of variance in INT. These results are strong. The next stages of analysis tested the influence of a number of moderators, and additional variables added following the exploratory interviews. Table 5.5 provides a summary of the main findings.

**Table 5.5 Model 1: Findings**

<b>Hypothesis</b>	<b>Variables</b>	<b>Supported</b>
H1a: Females express higher HIPC	GENDER → HIPC	<b>X</b>
H2a: Age positively influences HIPC	AGE → HIPC	✓**
H3a: Healthcare need positively influences HIPC	HN → HIPC	✓*
H4a: Poor health status positively influences HIPC	HS → HIPC	<b>X</b>
H5a: Perceived sensitivity positively influences HIPC	SEN → HIPC	✓**
H6a: Trust in health professionals negatively influences HIPC	TRH → HIPC	<b>X*</b>
H7a: Perceived Risk positively influences HIPC	RSH → HIPC	✓**
H8a: Privacy Media Coverage positively influences HIPC	MED → HIPC	✓**
H9a: Health Information seeking negatively influences HIPC	INF → HIPC	✓*
H11a: HIPC negatively influences Intention to accept an EHR	HIPC → INT	✓**
H17a: Perceived Benefits positively influences Intention to accept an EHR	BEN → INT	✓**
H12a: Trust in health professionals positively influences EHR acceptance	TRH → INT	<b>X*</b>
H13a: Perceived risk negatively influences EHR acceptance	RSH → INT	✓
H14a: Health Information seeking positively influences EHR acceptance	INF → INT	<b>X</b>

✓ Supported at the .10 level, ✓\* Supported at the .05 level, ✓\*\* Supported at the .01 level, **X** not supported, **X\*** Significant but not in hypothesised direction

#### **5.6.7 Model 1: Testing Moderation Effects**

For model 1, two moderators related to individuals' privacy invasion experiences, and health conditions were proposed. Multi-group moderation was conducted in AMOS to compare the HIPC-INT, and BEN-INT relationships across the various groups. Regression weights were

compared across the groups and Z scores were examined to identify any significant differences. Each moderator is now discussed individually.

#### 5.6.7.1 *Model 1: Chronic Illness*

The first proposed moderator was chronic illness. H18a proposed that the negative influence of HIPC on INT would be stronger among individuals with chronic conditions. In addition, it was hypothesised that the relationship between BEN and INT would be weaker among those with chronic conditions (H20a). To test H18a and H20a, the data was divided into two groups, those with chronic conditions and those with no chronic conditions. Upon dividing the data into the two groups, the model fit remained satisfactory: cmin/df: 2.228, CFI: .957, SRMR: .078, RSMEA: .062. The findings are outlined below in Table 5.6.

**Table 5.6 Model 1: Moderating Effects of Chronic Illness**

	Chronic Illness		No Chronic Illness		Z-score
	RWG	P	RWG	P	
HIPC→ INT	-0.265	0.000	-0.185	0.000	0.930
BEN→ INT	0.718	0.000	0.770	0.000	0.533

As shown above, the relationship between HIPC and INT was significant for both groups, but the negative influence of HIPC on INT was greater among individuals with chronic conditions. The difference between the two groups was not significantly different, thus H18a is partially supported. The relationship between BEN and INT was also significant for both groups, but weaker among those with chronic conditions. Again the difference between both groups is not significant, and H20a is partially supported.

#### 5.6.7.2 *Model 1: Sensitive Illness as a Moderator*

The second moderator tested the role of sensitive illness. H19a posited that the relationship between HIPC and INT would be stronger among individuals with sensitive illnesses, and H20b proposed that the BEN-INT relationship would weaken among these individuals. To test these propositions, the data was divided into two groups, individuals with illnesses they described as

sensitive and individuals with no sensitive conditions. Upon dividing the sample, the model fit remained sufficient; cmin/df: 1.750, CFI: .975, SRMR: .0343, RMSEA: .048. Table 5.7 below compares the relationships between both groups.

**Table 5.7 Model 1: Moderating Effects of Sensitive Illness**

	Sensitive Illness		No Sensitive Illness		Z-score
	RWG	P	RWG	P	
HIPC→ INT	-0.123	0.106	-0.224	0.000	-1.121
BEN→ INT	0.351	0.000	0.788	0.000	3.739**

\*\* Supported to .01 level.

As shown, the relationship between HIPC and INT is not significant among individuals with sensitive illness. Thus, H19a is not supported. While this is surprising, risk perceptions had a significant, negative influence on INT among individuals with sensitive conditions, suggesting risk influences intentions among this group more than HIPC. Benefits influenced INT among both groups, but this influence was far weaker among individuals with sensitive illness. There was a significant influence between both groups thus supporting H20b.

#### 5.6.7.3 Model 1: Personal Privacy Invasion as a Moderator

The third proposed moderator was experience of privacy invasion regarding personal information. The data was broken into two groups based on the frequency of individuals' personal privacy invasion experience (High or Low frequency). It was hypothesised that the HIPC-intention relationship would be stronger among the high group (H21a), and the BEN-intention relationship would be weaker among this group (H22a). Upon splitting the data, the model fit remained strong: cmin/df: 1.953, CFI: .967, SRMR: .049, RMSEA: .055.

**Table 5.8 Model 1: Moderating Effects of Personal Privacy Invasion**

	Low Frequency		High Frequency		Z-score
	RWG	P	RWG	P	
HIPC→ INT	-0.199	0.000	-0.214	0.002	-0.165
BEN→ INT	0.804	0.000	0.614	0.000	-1.785†

†Supported to .10 level.

As illustrated in table 5.8, the negative influence of HIPC on INT was significant among both groups, and stronger among individuals with experience of frequent privacy invasions. The difference between both groups was not significant, thus H21a is partially supported. The relationship between benefits and intention is weaker among the high frequency group. There is also a slightly significant difference between both groups, supporting H22a.

#### 5.6.7.4 Model 1: Health Privacy Invasion as a Moderator

The fourth proposed moderator was experience of privacy invasion regarding health information. The data was broken into two groups based on the frequency of individuals' health privacy invasion experience (High or Low frequency). It was hypothesised that the HIPC-intention relationship would be stronger among the high group (H23a), and the BEN-intention relationship would be weaker among this group (H24a). The model fit statistics remained strong: cmin/df: 1.899, CFI: .969, SRMR: .039, RMSEA: .053.

**Table 5.9 Model 1: Moderating Effects of Health Privacy Invasion**

	Low Frequency		High Frequency		Z-score
	RWG	P	RWG	P	
HIPC→ INT	-0.169	0.000	-0.450	0.000	-2.242*
BEN→ INT	0.784	0.000	0.476	0.000	-2.144*

\* Supported to .05 level.

HIPC had a significant, negative influence on INT. However, this influence was far stronger among individuals with higher experience of health privacy invasion. The HIPC-INT relationship was significantly different across the two groups, supporting H23a. Benefits had a significant, positive influence on intention for both groups. As expected, this influence was weaker among individuals in the high frequency group. This relationship was again significantly different across the two groups. Thus H24a is also supported.

In summary, four moderators were tested for model 1. The intentions of individuals with chronic conditions were influenced more by HIPC than perceived benefits. Perceived benefits also had a weaker influence on intentions among individuals with sensitive conditions. The frequency of

personal privacy invasion strengthened the HIPC-INT relationship, and weakened the BEN-INT relationship as hypothesised. Additionally, frequency of health privacy invasion significantly moderated the HIPC-INT and BEN-INT relationships.

### 5.6.8 Model 1: Testing Mediation Effects

Due to the sensitivity of health data, it was proposed that HIPC would represent the strongest influence on intention. Mediation tests were therefore conducted to determine if HIPC could mediate the influence of the other predictors of intention including perceived benefits, trust, and risk. The mediating influence of HIPC was tested in AMOS following the four step process outlined by Baron and Kenny (1986). The steps are as follows:

1. The relationship between the independent variable and the dependent variable is first tested without the mediator ( $X \rightarrow Y$ ). It is suggested that this relationship should be significant, but this is not required.
2. The relationship between the independent variable and the mediator ( $X \rightarrow M$ ) should be significant.
3. The relationship between the mediator and the dependent variable ( $M \rightarrow Y$ ) should be significant.
4. The relationship between the independent and dependent is tested with the mediator added ( $X \rightarrow M \rightarrow Y$ ). The relationship should change when the mediator is added.

In addition to these four steps, bootstrapping was used to determine the indirect effect size, and the Sobel test was utilised to determine the significance of this effect (Preacher and Hayes, 2004; Zhao *et al.*, 2010). The results for mediation testing are outlined below in Table 5.10.

**Table 5.10 The Mediating Role of HIPC**

Relationship	$X \rightarrow Y$	$X \rightarrow M$	$M \rightarrow Y$	$X+M \rightarrow Y$	Bootstrap (Indirect effect)	ZSobel	Mediation
BEN→HIPC→ INT	(.700)**	(-.110) n.s.	(-.185)**	(.686)**	(.020)n.s.	(1.408)n.s.	None
TRH→HIPC→ INT	(-.144)*	(.135)*	(-.185)**	(-.143)**	(-.025)*	(-1.832)†	Indirect
RSH→HIPC→ INT	(-.095)*	(.405)**	(-.185)**	(-.093)†	(-.075)**	(-3.707)**	Indirect

† Significant to .10 level, \*Significant to .05 level, \*\* Significant at the .01 level, n.s. Not significant



The mediation influence of HIPC on the relationship between perceived benefits and intentions was first tested. As shown in the table above, BEN significantly influenced intention prior, and subsequent to the addition of HIPC (the mediator). BEN did not have a significant indirect influence on intention via HIPC. Thus HIPC does not mediate the BEN-INT relationship. Secondly, the mediating role of HIPC on the trust-intention relationship was explored. Trust significantly influenced intention prior to the addition of the mediator. Upon adding HIPC, this influence remained significant, although it weakened slightly. Bootstrapping revealed that trust had a significant, indirect influence on INT, via its relationship with HIPC. The Sobel test revealed that this indirect relationship was slightly significant. It is thus concluded that trust indirectly influences INT via HIPC. Lastly, the mediating influence of HIPC on the relationship between risk perceptions and INT was investigated. Prior to the addition of the mediator, risk had a negative, significant influence on INT. Upon adding the mediator, this relationship reduced in significance. This indicates partial mediation. Bootstrapping revealed that risk had a significant, indirect influence on INT, via its influence on HIPC. The Sobel test showed that the indirect effect was significant to the .01 level. It is thus concluded that HIPC partially mediates the relationship between risk and INT, and risk indirectly influences INT via HIPC.

### ***5.6.9 Model 1: Additional Constructs***

The final stage of analysis involved testing the role of two additional constructs, which were added following the exploratory interviews. Firstly, perceived ownership of health data was examined using three items. One item was dropped due to low loading (.11) and conceptual disparity. The resultant two item measure was reliable (CR: .76). H25a posited that perceived ownership would positively influence HIPC. Secondly, awareness of health legislation was measured using one item. It was hypothesised that greater awareness of health legislation would negatively influence HIPC (H26a). Upon adding these two constructs to the model, the model fit remained strong: cmin/df: 2.365, CFI: .967, SRMR: .035, RMSEA: .065. The path analysis revealed a positive, significant relationship between perceived ownership and HIPC ( $\beta = .225$ ,  $p < .01$ ). This offers strong support for H25a. The negative relationship between legislation

awareness and HIPC was present, but only slightly significant ( $\beta = -.084$ ,  $p = .087$ ,  $< .10$ ), H26a is not supported. The revised model explained 37.1% of variance in HIPC, and 56.1% of variance in intentions.

#### ***5.6.10 Model 1: Summary***

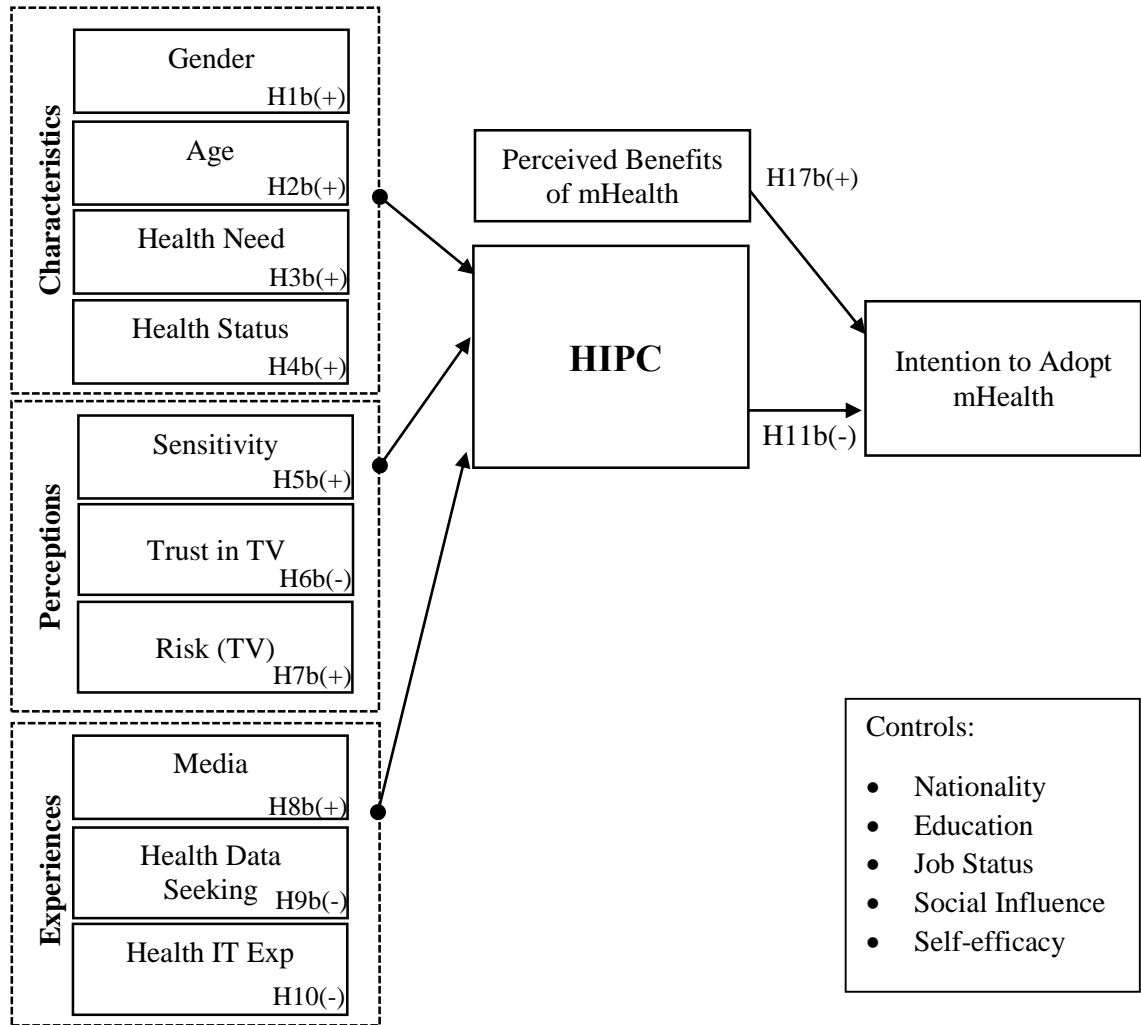
Model 1 examined the influence of HIPC on individuals' intentions to accept EHRs. The proposed model achieved strong model fit. All constructs met reliability and validity thresholds. Hypothesis testing was conducted in four stages. First, the main relationships were tested. Support was achieved for several antecedents including individual characteristics such as age and healthcare need, perceptions related to risk and sensitivity, and experiences such as media coverage awareness, and health information seeking behaviours. The negative influence of HIPC on intention was supported, as was the positive influence of perceived benefits on intention. The data provided some surprising findings including the positive influence of trust in health professionals on HIPC. In the second stage, several moderators were tested. The findings supported the moderating influence of chronic illness on the HIPC-INT, and BEN-INT relationships. Sensitive illness also moderated the BEN-INT relationship. Frequency of personal privacy invasions, and health data privacy invasions moderated the HIPC-INT, and BEN-INT relationships. In the third stage, the mediating influence of HIPC was explored. The findings showed that HIPC did not mediate the influence of BEN on intentions. Trust had an indirect influence on intention via HIPC. In addition, HIPC partially mediated the influence of risk perceptions on INT. In the final stage, two additional antecedents were tested. The data supported the positive influence of perceived ownership on HIPC. The findings show that HIPC and perceived benefits influence citizens' intentions to accept an EHR. However, these influences can be moderated by chronic and sensitive illnesses, and personal and health privacy invasion experience. The remainder of this chapter focuses on the findings pertinent to model 2.

## **5.7 Model 2: HIPC and mHealth Adoption**

The second model explored the influence of HIPC on citizens' intentions to adopt mHealth technologies. The model included the entire U.S. and Irish samples (n=447). The antecedents to HIPC also included individual characteristics, perceptions, and experiences. Similar to model one, individual characteristics included gender, age, healthcare need, and health status. Perceptions included perceived sensitivity, perceived trust in technology vendors (TV), and perceived risks associated with disclosing data to health technology vendors (TV). Experiences included media coverage awareness and health information seeking behaviours from model 1. Previous health ICT experience was also added. It was hypothesised that HIPC would negatively influence individuals' intentions to adopt mHealth solutions. In addition, it was posited that HIPC would negatively impact intended frequency of use for three mHealth solutions: mHealth applications, wearable tracking devices, and Personal Health Records (PHR). Lastly, it was proposed that perceived benefits of mHealth would positively influence intentions. Perceived self-efficacy was added as an additional control variable.

This section begins by testing the model fit using CFA, prior to testing the validity and reliability of the model. The procedures conducted to test for common method bias are also discussed. Each variable is then discussed individually. The proposed structural model is tested in AMOS using Structural equation modelling (SEM). Lastly, the role of moderation, mediation, and additional variables are explored. The main hypotheses in model 2 are outlined below in Figure 5.4 (pg. 153).

**Figure 5.4 Proposed Model 2**



### 5.7.1 Model 2: Model Fit

Confirmatory factor analysis (CFA) was conducted in AMOS to test the proposed structure of the model. In order to improve model fit, a number of items with low factor loadings were dropped. Item 3 was dropped from health status (.52) due to low loading and disparity in the wording compared to other items. This item was also dropped in model 1. Item 5 was dropped from trust in technology vendors, again due to low loading (.57). Two items were dropped from perceived sensitivity. Both items had low loadings of .44 (item 1) and .46 (item 3), and were also dropped in model 1. Similarly, two items which had been dropped in model 1 were again removed from health information seeking. Items 4 (.53) and 5 (.59) differed slightly from the remaining items. Items 2 (.54) and 8 (.54) were dropped from perceived benefits of mHealth. These items focused

on whether mHealth solutions were ‘fun’ and ‘easy’ to use, whereas the remaining items focused on how mHealth solutions could aid in personal health management. Thus the conceptual disparity is evident. Lastly two items were dropped from mHealth self-efficacy. Items 1 (.44) and 2 (.47) pertained to current ability to use mHealth, whereas the remaining items relate to the individuals’ perceived ability to use mHealth in the future. The resultant model demonstrated good model fit, meeting all recommended fit statistics for samples >250 with >30 observed variables (Hair *et al.* 2010). Table 5.11 below provides an overview of the model fit statistics.

**Table 5.11 Model 2: Model fit statistics**

Model Fit Statistic	Model 2	Recommended Threshold
Chi Square/Df (Cmin/df)	2.018	Less than 3 = good
CFI	.923	Above .90
SRMR	.048	.08 or less
RMSEA	.048	Values of <.07

### **5.7.2 Model 2: Validity & Reliability Testing**

The convergent validity, discriminant validity, and reliability of all constructs were tested following the same procedures outlined in model 1. Firstly, the AVE of each construct was calculated. The AVE of each construct exceeded the recommended threshold of .50, thus supporting the convergent validity of all constructs (Fornell and Locker, 1981). Secondly, the square root of the AVE was compared with the interrelation between each set of two constructs to explore discriminant validity. As the square of the AVE (shown on the diagonal in Table 5.12 below) was greater than the correlation in each comparison, discriminant validity was confirmed (Hair *et al.*, 2010). Lastly, the reliability of each construct is also apparent, as the composite reliability for each construct exceeded .70. Table 5.12 below illustrates the findings from validity and reliability tests.

**Table 5.12 Validity and Reliability: Model 2**

	<b>CR</b>	<b>AVE</b>	<b>TRT</b>	<b>RST</b>	<b>HIPC</b>	<b>INF</b>	<b>MED</b>	<b>HN</b>	<b>HINT</b>	<b>HS</b>	<b>SEN</b>	<b>BEN</b>
Trust in Technology (TRT)	.87	.57	<b>.75</b>									
Risk –Technology (RST)	.92	.74	-.50	<b>.86</b>								
HIPC	.97	.87	-.24	.38	<b>.93</b>							
Health Data Seeking (INF)	.82	.60	.07	-.14	.00	<b>.77</b>						
Media Coverage (MED)	.77	.62	-.27	.13	.26	.21	<b>.79</b>					
Healthcare Need (HN)	.77	.54	.09	.06	.17	.08	.02	<b>.73</b>				
Intention: mHealth (HINT)	.96	.88	.18	-.23	-.04	.31	.06	.13	<b>.94</b>			
Health Status (HS)	.88	.79	.04	.00	.06	.06	.03	.47	.03	<b>.89</b>		
Perceived Sensitivity (SEN)	.96	.69	-.20	.11	.15	.22	.22	-.10	.05	-.01	<b>.83</b>	
Benefits of mHealth (BEM)	.93	.64	.13	-.16	-.10	.26	.09	-.02	.52	-.02	.13	<b>.80</b>

### **5.7.3 Model 2: Testing for Common Method Bias**

In line with model 1, two tests were conducted to explore the presence of common method bias. Firstly, the Harman's single factor test was conducted in SPSS. The first emerging factor explained 20.46% of variance for the model. This indicates that CMB is unlikely to represent a major issue. Secondly, the common latent factor approach was followed in AMOS by adding a common latent factor (CLF) to the model. All observed items were loaded on to the common latent factor. Factor loadings for all observed items were constrained to explore the shared variance due to method. Upon adding the common latent factor, the model fit improved slightly as expected; cmin/df: 1.868, CFI: .929, RMSEA: .044, SRMR: .0487. The common latent factor explained 1.6% of variance in the model. In addition, the standardised regression weights for each item upon addition of the CLF were compared with those prior to its addition. None of the items experienced a great change upon addition of the CLF. It is thus concluded that common method bias is not an issue in model 2 (Gaskin, 2012b).

### **5.7.4 Model 2: Individual Variables**

This section briefly reviews the validity and reliability of each construct in model 2. Firstly, the antecedents to HIPC are outlined. Healthcare need was measured using three items, all of which loaded highly. The construct was both reliable (CR: .77) and valid (AVE: .54). The second construct, poor health status, was measured with three items. Item 3 was dropped due to low loading. The resultant two item construct was deemed reliable (CR: .88) and valid (AVE: .79). The next antecedent measured trust in technology vendors across six items similar to those in the trust in health professionals (TRH) construct in model 1. Item 5 was dropped from trust in technology vendors. The final five item construct demonstrated validity (AVE: .57) and reliability (CR: .87). The next construct, risk perceptions associated with technology vendors (RST), was measured with four items based on the risk perceptions associated with health professionals construct. The four item construct exceeded validity (AVE: .74) and reliability thresholds (CR: .92). Perceived sensitivity was also measured in model 1. During confirmatory

factor analysis, two items were dropped due to low factor loadings. These items were also dropped from model 1. The final ten item construct was both valid (AVE: .69), and reliable (CR: .96). Media coverage was also measured in model 1 and consisted of two items. The construct met convergent validity (AVE: .62) and reliability requirements (CR: .77). The final antecedent, health information seeking was measured in model 1. Two items were dropped based on their low factor loadings. These items were also dropped in model 1. The remaining three item construct had an AVE of .60 and a CR of .82, illustrating its validity and reliability. The final independent variable, perceived benefits of mHealth (BEM) was not measured in model 1 and originally consisted of 9 items. Three items which had been added during pilot testing were dropped during CFA due to low loadings and conceptual disparity with the remaining items. For example, item 2 focused on individuals' perception of whether mHealth solutions would be easy to use. In contrast, the other items focus on perceptions of how mHealth could lead to the realisation of benefits such as greater health awareness and health management. The refined seven item construct met validity (AVE: .64) and reliability thresholds (CR: .93). Intention to adopt mHealth (HINT) was measured with three items, all of which had high factor loadings. The construct was valid (AVE: .88), and reliable (CR: .96).

HIPC was also the focal construct in model 2. The factor loadings for the six first order factors were extremely high; Collection (.92) Unauthorised Secondary Use (.96), Improper Access (.92), Errors (.91), Control (.96), and Awareness (.91). The second order construct was both reliable (CR: .98), and valid (AVE: .87). Model 2 offers further support for the proposed second order factor structure. In the interest of rigour, the second order factor was deleted and a six first order factor structure was tested. For the first order factor structure, each first factor had a composite reliability (C.R.) score above .70, indicating reliability: Collection (.86), Unauthorised Secondary Use (.86), Improper Access (.91), Errors (.87), Control (.85), and Awareness (.88). All six first order factors had AVE values above .50: Collection (.60), Unauthorised Secondary Use (.66), Improper Access (.76), Errors (.69), Control (.66), and Awareness (.71). However, the correlations between each of the factors was higher than the square root of the AVE, indicating



that these factors are not distinct from each other. Therefore, as expected, the second order factor structure was deemed more appropriate. Table 5.13 below provides an outline of all constructs in the model.

**Table 5.13 Model 2: Construct Descriptives**

Items	Mean	Std. Dev	Factor Loading	Composite Reliability
<b>Healthcare Need</b>	<b>2.50</b>	<b>0.90</b>		<b>.77</b>
HN1: # Face to face visits to health professionals	2.01	1.22	.80	
HN2: # different health professionals visited	1.92	1.08	.77	
HN3: # of medications	2.46	0.90	.61	
<b>Health Status</b>	<b>2.72</b>	<b>0.94</b>		<b>.88</b>
HS1: Experience of major pains and discomfort	2.56	1.09	.89	
HS2: Severity of condition	2.18	0.74	.90	
<b>Trust: Technology Vendors</b>	<b>2.62</b>	<b>0.94</b>		<b>.87</b>
TRT1: Technology Vendors are always honest when using my health information	2.24	0.81	.77	
TRT2: Technology Vendors care about customers	2.51	0.88	.72	
TRT2: Technology Vendors are not opportunistic when using my health information	2.24	0.84	.76	
TRT3: Technology Vendors are predictable and consistent when using my health information	2.51	0.84	.71	
TRT4: Technology Vendors keep my best interests in mind when dealing with my health information	2.36	0.93	.81	
<b>Perceived Risks: Technology Vendors</b>	<b>3.86</b>	<b>0.96</b>		<b>.92</b>
RST1: Risky to disclose my personal health information to technology vendors	3.69	0.90	.86	
RST2: High potential for loss associated with disclosing my health information to technology vendors	3.47	0.94	.86	
RST3: Too much uncertainty associated with giving my health information to technology vendors	3.64	0.93	.87	
RST4: Providing technology vendors with my health information would involve many unexpected problems	3.40	0.95	.85	
<b>Perceived Sensitivity of Health Data:</b>	<b>3.54</b>	<b>1.27</b>		<b>.96</b>
SEN1: Current Health Status	3.25	1.34	.64	
SEN2: Test results	3.32	1.40	.74	
SEN3: Health history	3.19	1.38	.74	
SEN4: Mental health	3.90	1.41	.91	
SEN5: Sexual health	3.91	1.39	.91	
SEN6: Domestic abuse	3.83	1.51	.91	
SEN7: Genetic information	3.64	1.50	.89	

Items	Mean	Std. Dev	Factor Loading	Composite Reliability
SEN8: Plastic surgery	3.17	1.42	.73	
SEN9: Reproductive health	3.89	1.43	.88	
SEN10: Addiction information	3.87	1.45	.92	
<b>Awareness of Media Coverage</b>	<b>2.58</b>	<b>0.85</b>		<b>.77</b>
MED1: Media Coverage pertaining to personal information	3.49	1.22	.83	
MED2: Media Coverage pertaining to personal health information	2.68	1.29	.75	
<b>Health Information Seeking Behaviours</b>	<b>2.82</b>	<b>0.92</b>		<b>.75</b>
INF1: Search for information related to disease diagnosis and treatment	2.46	1.03	.72	
INF2: Search for information related to health management	2.76	1.11	.86	
INF3: Search for health information for education, research, or learning purposes	2.78	1.27	.73	
<b>Perceived Benefits: Mobile Health technologies would:</b>	<b>4.64</b>	<b>0.97</b>		<b>.93</b>
BEM1: Improve my access to my health information	3.80	0.88	.80	
BEM2: Improve my ability to manage my health	3.67	0.86	.85	
BEM3: Make managing my health fun	3.19	1.00	.63	
BEM4: Make managing my health easier	3.68	0.87	.83	
BEM5: Help me be more informed about my health	3.77	0.91	.84	
BEM6: Improve my health management	3.60	0.91	.87	
BEM7: Improve the quality of my health	3.39	0.98	.78	
<b>Intention to Adopt mHealth</b>	<b>3.28</b>	<b>0.98</b>		<b>.96</b>
HINT1: Likelihood	3.32	1.06	.94	
HINT2: Probability	3.30	1.06	.97	
HINT3: Willingness	3.44	1.05	.95	
<b>HIPC</b>	<b>3.88</b>	<b>0.98</b>	-	<b>.98</b>
<b>Collection</b>	<b>3.18</b>	<b>0.87</b>		<b>.90</b>
COLL1: Bothers me when healthcare entities ask for health information	2.87	1.12	.67	
COLL2: I sometimes think twice before providing health information	3.22	1.24	.77	

Items	Mean	Std. Dev	Factor Loading	Composite Reliability
COLL3: Bothers me to give health information to so many healthcare entities	3.38	1.21	.86	
COLL4: Concerned healthcare entities are collecting too much information	3.24	1.16	.79	
<b>Unauthorised Secondary Use</b>	<b>3.69</b>	<b>0.98</b>	-	<b>.96</b>
SU1: Concerned when I give health information to health entities for some reason, they might use it for other reasons	3.20	1.14	.75	
SU2: Concerned health entities would sell my health information to other health entities or non-health related organisations	3.29	1.26	.83	
SU3: Concerned health entities would share my health information with other health entities without my authorisation	3.58	1.18	.86	
<b>Improper Access</b>	<b>3.64</b>	<b>0.98</b>	-	<b>.92</b>
ACC1: Concerned health entities' databases containing my health information are not protected from unauthorised access	3.63	1.13	.87	
ACC2: Concerned health entities do not devote enough time and effort to preventing unauthorised access to my health information	3.50	1.13	.86	
ACC3: Concerned health entities do not take enough steps to ensure unauthorised people cannot access my health information	3.59	1.14	.88	
<b>Errors</b>	<b>3.36</b>	<b>0.88</b>	-	<b>.91</b>
ERR1: Concerned health entities do not take enough steps to ensure my health information in their files is accurate	3.53	1.17	.84	
ERR2: Concerned health entities do not have adequate procedures to correct errors in my health information	3.49	1.11	.82	
ERR3: Concerned health entities do not devote enough time and effort to verifying the accuracy of my personal information in their databases	3.57	1.14	.83	
<b>Control</b>	<b>3.60</b>	<b>0.96</b>	-	<b>.96</b>
CON1: Bothers me when I do not have control of health information that I provide to health entities	3.53	1.14	.80	
CON2: Bothers me when I do not have control or autonomy over decisions about how my health information is used and shared by health entities	3.81	1.12	.85	
CON3: Concerned when control is lost or unwillingly reduced as a result of providing health entities with my health information	3.69	1.08	.79	
<b>Awareness</b>	<b>3.84</b>	<b>0.95</b>	-	<b>.91</b>
AW1: Bothers me when I am not aware or knowledgeable about how my health information will be used by health entities	3.78	1.14	.89	

<b>Items</b>	<b>Mean</b>	<b>Std. Dev</b>	<b>Factor Loading</b>	<b>Composite Reliability</b>
AW2: Bothers me when health entities seeking my health information do not disclose the way the data are processed and used	3.83	1.08	.86	
AW3: It is very important that I am aware and knowledgeable about how my health information will be used	4.08	0.98	.79	

### 5.7.5 Model 2: Correlations

The correlations between all variables in model 2 are outlined below in Table 5.14. Again, the majority of antecedents to HIPC were significant to the .01 level. Surprisingly, HIPC and intention to adopt mHealth were not significantly correlated. However, perceived benefits, health information seeking, and trust in technology vendors were significantly correlated with intention.

**Table 5.14 Model 2: Correlations**

	HIPC	HN	HS	TRT	RST	SEN	MED	INF	BEM	HINT
HIPC	1									
HN	.20**	1								
HS	.07	.54*	1							
TRT	-.26**	-.10**	.04	1						
RST	.40**	.07	.04	-.55**	1					
SEN	.16**	-.11*	-.01	-.22*	.12*	1				
MED	.30**	.02	.03	-.32**	.15**	.25**	1			
INF	-.00	-.09	.07	.08	-.16**	.24**	.25**	1		
BEM	-.11*	-.02	-.02	.14**	-.17**	.14**	.11*	.29**	1	
HINT	-.04	-.14**	.03	.20**	-.24**	.05	.06*	.34**	.54**	1

\* Significant at .05 level, \*\* Significant at .01 level

### 5.7.6 Model 2: Hypothesis Testing

Model 2 examines the influence of HIPC on individuals' intentions to adopt mHealth solutions. There were four stages of hypothesis testing beginning with testing the structural model outlined in Figure 5.4 on pg. 153. This model was tested using SEM in AMOS. The model demonstrated strong fit: cmin/df: 2.215, CFI: .981, SRMR: .027, RMSEA: .052. The findings for the hypothesised relationships are discussed starting with the proposed antecedents.

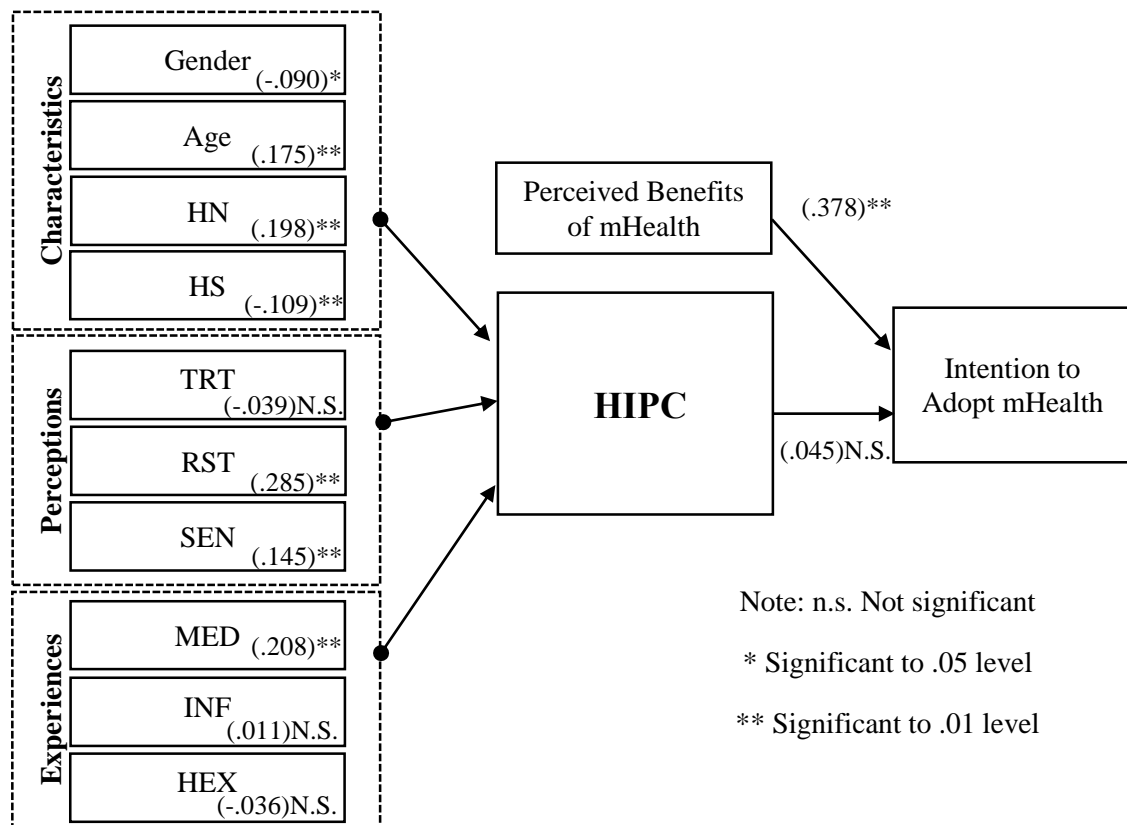
The first set of antecedents related to individual characteristics. H1b posited that females would express higher HIPC. However, as was the case in model 1, the path analysis revealed that males expressed higher HIPC. This relationship was significant to the .05 level ( $\beta = -.090$ ). Thus H1b is not only rejected, but refuted. It was posited that age would positively influence HIPC. This relationship was evidenced in the data to a significance level of .001, offering strong support for H2b ( $\beta = .175, p < .01$ ). H3b was hypothesised that healthcare need would positively impact HIPC. This was supported in the data ( $\beta = .198, p < .01$ ). H4b posited that health status would positively

influence HIPC. However, the path analysis revealed that health status negatively influenced HIPC. This relationship was significant to the .05 level ( $\beta = -.109$ ,  $p < .05$ ). Thus H4b is rejected. In terms of perceptions, H5b proposed a positive relationship between perceived sensitivity and HIPC. The findings from the path analysis for model 2 showed a significant, positive relationship with a significance level of .01 ( $\beta = .145$ ). Therefore, H5b is supported. H6b posited that trust in technology vendors would negatively impact HIPC. This negative relationship was evidenced in the data but was not significant. H6b is not supported. It was hypothesised that risk perceptions regarding technology vendors would positively influence HIPC. The path analysis revealed a positive, significant relationship between risk and HIPC ( $\beta = .285$ ,  $p < .01$ ), supporting H7b. In terms of experiences, it was hypothesised that awareness of privacy media coverage (MED) would positively impact HIPC. The data revealed a positive association between MED and HIPC, which was significant to the .01 level ( $\beta = .208$ ). Therefore, H8b is supported. As was the case in model 1, it was proposed that health information seeking behaviour (INF) would negatively influence individuals' HIPC. The SEM path analysis revealed that INF was not significantly related to HIPC ( $\beta = .011$ ,  $p > .10$ ). Thus H9b is not supported. It was posited that previous experience using health ICTs would negatively influence HIPC. A negative relationship was present in the data. However, this relationship was insignificant. H10 is therefore rejected.

Similar to model 1, the relationship between HIPC and intention was of great interest. It was hypothesised that HIPC would negatively impact individuals' intentions to adopt mHealth (HINT). Surprisingly, the findings revealed that this relationship was positive and insignificant ( $\beta = .045$ ,  $p > .10$ ). Thus, H11b is rejected. Model 2 proposed that a number of additional constructs would influence intention. Firstly, the hypothesised positive relationship between trust and intention was evidenced, but this relationship was insignificant thus rejecting H12b ( $\beta = .052$ ,  $p > .10$ ). Support was provided for the hypothesised negative influence of risk on intention supporting H13b ( $\beta = -.112$ ,  $p < .05$ ). It was hypothesised that health information seeking behaviour would positively influence intention. This relationship was positive and slightly significant, offering partial support for H14b ( $\beta = .082$ ,  $p = .056 < .10$ ). It was also hypothesised that

previous health ICT experience would positively influence intention. This relationship was positive and significant, supporting H15 ( $\beta = .233, p < .01$ ). Lastly, H17b posited that perceived benefits would positively influence intention. This relationship was significant, supporting H17b ( $\beta = .378, p > .01$ ). The final set of hypotheses focused on individuals' intentions towards different mHealth solutions. Firstly, H16a posited that HIPC would negatively influence intentions to use Personal Health Records (PHRs). This relationship was negative but insignificant, thus rejecting H16a ( $\beta = -.024, p > .10$ ). Secondly, it was proposed that HIPC would negatively impact intention to use wearable devices. This relationship was insignificant thus rejecting H16b ( $\beta = -.003, p > .10$ ). Thirdly, H16c posited that HIPC would negatively influence intentions to use mHealth applications. This relationship was negative and significant, supporting H16c ( $\beta = -.079, p < .05$ ). The SEM path analysis offered support for a number of hypothesised relationships in model 2. The model explained 22.8% of variance in HIPC, 43.5% of variance in intention, as well as 22.8% of variance in intention to use PHRs, 38.1% of variance in intention to use wearables, and 55.8% of variance in intention to use mHealth applications. Figure 5.5 below provides an overview of the main relationships in model 2.

**Figure 5.5 Model 2: Results**





The results for the primary hypotheses in model two are outlined in Table 5.15 below.

**Table 5.15 Model 2: Findings**

<b>Hypothesis</b>	<b>Variables</b>	<b>Supported</b>
H1b: Females express higher HIPC	GENDER → HIPC	<b>X*</b>
H2b: Age positively influences HIPC	AGE → HIPC	<b>✓**</b>
H3b: Healthcare need positively influences HIPC	HN → HIPC	<b>✓*</b>
H4b: Poor health status positively influences HIPC	HS → HIPC	<b>X*</b>
H5b: Perceived sensitivity positively influences HIPC	SEN → HIPC	<b>✓**</b>
H6b: Trust in technology vendors negatively influences HIPC	TRT → HIPC	<b>X</b>
H7b: Perceived risk positively influences HIPC	RST → HIPC	<b>✓**</b>
H8b: Privacy media coverage positively influences HIPC	MED → HIPC	<b>✓**</b>
H9b: Health information seeking negatively influences HIPC	INF → HIPC	<b>X</b>
H10: Health ICT Experience negatively impacts HIPC	HEXP → HIPC	<b>X</b>
H11b: HIPC negatively influences Intention to adopt mHealth	HIPC → HINT	<b>X</b>
H17b: Perceived benefits positively influence Intention to adopt mHealth	BEM → HINT	<b>✓**</b>
H12b: Trust in technology vendors positively influences Intention to adopt mHealth	TRT → HINT	<b>X</b>
H13b: Perceived risk negatively influences Intention to adopt mHealth	RST → HINT	<b>✓*</b>
H14b: Health information seeking behaviour positively influences Intention to adopt mHealth	INF → HINT	<b>✓</b>
H15: Health ICT Experience positively influences Intention to adopt mHealth	HEXP → HINT	<b>✓**</b>
H16a: HIPC negatively influences Intentions to use Personal Health records	HIPC → PHR	<b>X</b>
H16b: HIPC negatively influence Intentions to use Health Monitoring Devices	HIPC → MON	<b>X</b>
H16c: HIPC negatively influences Intentions to use mHealth applications	HIPC → APP	<b>✓*</b>

**✓** Supported at the .10 level, **✓\*** Supported at the .05 level, **✓\*\*** Supported at the .01 level, **X** not supported, **X\*** Significant in opposite direction

### 5.7.7 Model 2: Testing Moderation Effects

Similar to model 1, four moderators were tested in model 2. Moderation effects were explored using multi-group moderation in AMOS to compare the relationships of interest across the various groups. The regression weights were compared across groups and Z scores were examined to identify any significant differences.

#### 5.7.7.1 Model 2: Chronic Illness as a Moderator

The first proposed moderator was chronic illness. H19b proposed that the negative influence of HIPC on HINT would be stronger among individuals with chronic conditions. It was also posited that HIPC would have a stronger influence on intentions regarding PHRs (H19c), monitoring devices (H19d), and mHealth applications (H19e) among individuals with chronic illness. In addition, it was hypothesised that the relationship between perceived benefits and intention would be weaker among those with chronic conditions (H21c). To test these assertions, the data was divided into two groups, those with chronic conditions and those with no chronic conditions. Upon dividing the data into the two groups, the model fit remained strong: cmin/df: 1.982, CFI: .970, SRMR: .041, RSMEA: .047. The findings are outlined below in Table 5.16.

**Table 5.16 Model 2: Moderating Effects of Chronic Illness**

	Chronic Illness		No Chronic Illness		Z-score
	RWG	P	RWG	P	
HIPC→ HINT	0.164	0.038	-0.008	0.868	-1.855†
HIPC→ PHR	-0.089	0.234	0.007	0.857	1.133
HIPC→ MON	-0.284	0.017	0.075	0.247	2.656**
HIPC→ APP	-0.147	0.108	-0.112	0.044	0.330
BEM→ HINT	0.459	0.000	0.375	0.000	-0.711

† Supported at .10 level, \*\* Supported at .01 level

As shown above, HIPC had a positive and significant influence on intention to adopt mHealth for individuals with chronic conditions. Thus H19b was rejected. However, the relationship between HIPC and intention to use different types of mHealth solutions was negative for all three solutions

as expected. HIPC had a significant, negative influence on intention to adopt monitoring devices. There was a significant difference in this relationship between the two groups. Thus H19d is strongly supported. Perceived benefits had a significant influence on intention for both groups. This relationship was stronger among individuals with chronic illness thus rejecting H21c.

#### 5.7.7.2 Model 2: Sensitive Illness as a Moderator

The second moderator was sensitive illness. H20b posited that the relationship between HIPC and HINT would be stronger among individuals with sensitive illnesses. It was also proposed that the negative influence of HIPC on intentions regarding PHRs (H20c), monitoring devices (H20d), and mHealth applications (H20e), would be stronger among this group. Lastly, H21d posited that the relationship between benefits and intention would be weaker among individuals with sensitive conditions. To test these hypotheses, the data was divided into two groups, individuals with illnesses they describe as sensitive, and individuals with no sensitive conditions. Upon dividing the sample, the model indicated good fit; cmin/df: 1.350, CFI: .989, SRMR: .038, RMSEA: .048. Table 5.17 below compares the relationships between both groups.

**Table 5.17 Model 2: Moderating Effects of Sensitive Illness**

	Sensitive Illness		No Sensitive Illness		Z-score
	RWG	P	RWG	P	
HIPC→ HINT	0.057	0.507	0.022	0.660	-0.356
HIPC→ PHR	-0.152	0.063	0.009	0.824	1.768†
HIPC→ MON	0.083	0.551	-0.034	0.594	-0.763
HIPC→ APP	-0.164	0.134	-0.110	0.038	0.450
BEM→ HINT	0.356	0.002	0.400	0.000	0.328

† Supported at .10 level, \*\* Supported at .01 level

As shown, the relationship between HIPC and HINT remained insignificant among both groups. Thus, H20b was not supported. The relationship between HIPC and intention to use PHRs was negative and slightly significant among individuals with sensitive illnesses, but positive and insignificant among the other group. The slightly significant difference between both groups offers partial support for H20c. The relationship between HIPC and intention to use wearables

was positive and insignificant among individuals with sensitive conditions, and negative but insignificant among individuals in the other group. Thus H20d is rejected. HIPC had a negative influence on intention to use mHealth applications for both groups. Interestingly, this relationship was only significant among individuals with no sensitive illnesses. As a result, H20e is not supported. Lastly, perceived benefits had a positive and significant relationship with intention for both groups. This relationship was weaker for individuals with sensitive conditions. As there was no significant difference between the groups, H21d is partially supported.

### 5.7.7.3 Model 2: Personal Privacy Invasion as a Moderator

The third proposed moderator was experience of privacy invasion regarding personal information. The data was broken into two groups based on the frequency of individuals' personal privacy invasion experience (High or Low frequency). It was hypothesised that the HIPC-intention relationship would be stronger among the high frequency group (H21b), and HIPC would have a stronger influence on intentions to use PHRs (H21c), monitoring devices (H21d), and mHealth applications (H21e). It was also hypothesised that the benefits-intention relationship would be weaker among this group (H22b). Upon splitting the data, the model fit remained strong: cmin/df: 1.681, CFI: .978, SRMR: .049, RMSEA: .039. Table 5.18 outlines the differences between the groups.

**Table 5.18 Model 2: Moderating Effects of Personal Privacy Invasion**

	Low Frequency		High Frequency		Z-score
	RWG	P	RWG	P	
HIPC→ HINT	0.061	0.283	0.023	0.708	-0.455
HIPC→ PHR	0.005	0.920	-0.057	0.279	-0.871
HIPC→ MON	0.041	0.559	-0.094	0.335	-1.124
HIPC→ APP	-0.072	0.223	-0.190	0.012	-1.228
BEM→ HINT	0.331	0.000	0.483	0.000	1.294

As shown above, the HIPC-HINT relationship remained positive and insignificant across both groups, rejecting H21b. HIPC had a negative influence on intentions to use PHRs, monitoring

devices, and mHealth applications, among individuals with high frequency of personal privacy invasion experience, but this influence was only significant on intention to use mHealth applications. As there was no significant difference between the low and high frequency groups, H21e is partially supported. H21c and H21d were not supported. Lastly, benefits significantly influenced intention for both groups. This relationship was surprisingly stronger among the high frequency group thus rejecting H22b.

#### 5.7.7.4 Model 2: Health Privacy Invasion as a Moderator

The fourth moderator was experience of privacy invasion regarding health information. The data was broken into two groups based on the frequency of individuals' health privacy invasion experience (High or Low). It was hypothesised that the HIPC-intention relationship would be stronger among the High group (H23b), and HIPC would have a stronger influence on intentions to use PHRs (H23c), monitoring devices (H23d), and mHealth Applications (H23e). It was also hypothesised that the benefits-intention relationship would be weaker among this group (H24b). Upon splitting the data, the model fit remained strong: cmin/df: 1.588, CFI: .982, SRMR: .027, RMSEA: .036. Table 5.19 outlines the findings on the moderating role of health privacy invasion.

**Table 5.19 Model 2: Moderating Effects of Health Privacy Invasion**

	Low Frequency		High Frequency		Z-score
	RWG	P	RWG	P	
HIPC→ HINT	0.055	0.226	0.007	0.953	-0.378
HIPC→ PHR	-0.036	0.346	0.087	0.336	1.254
HIPC→ MON	0.021	0.731	-0.063	0.754	-0.398
HIPC→ APP	-0.116	0.021	-0.114	0.453	0.011
BEM→ HINT	0.368	0.000	0.635	0.000	1.490

As illustrated above, the HIPC-HINT relationship remained insignificant across both groups. H23b is therefore rejected. The HIPC-PHR and HIPC-MON relationships were also insignificant, rejecting H23c and H23d. HIPC had a negative influence on intention to use mHealth applications for both groups, but this relationship was only significant among the low frequency group. H23e

is rejected. Perceived benefits positively influenced intention for both groups. However, this relationship was stronger among the high frequency group. Thus, H24b is rejected.

In summary, four moderators were tested. Chronic illness moderates the relationship between HIPC and intentions to use health monitoring devices, and the perceived benefits-intention relationship. Sensitive illness moderates the relationship between HIPC and intentions to use PHRs, and the influence of perceived benefits on intention. Higher experience of personal privacy invasion moderates the influence of HIPC on intentions to use mHealth applications. Health privacy invasion does not act as a moderator in model 2.

#### ***5.7.8 Model 2: Testing Mediation Effects***

Due to the sensitivity of health data, it was proposed that HIPC would represent the strongest influence on intention, and that HIPC could potentially mediate the influence of the other predictors of intention including perceived benefits, trust, and risk. As noted in Section 5.5.8, mediation requires the mediator to be significantly associated with the dependent variable (Baron and Kenny, 1986). HIPC was not significantly related to HINT. Thus the mediation role of HIPC could not be tested, and was rejected.

#### ***5.7.9 Model 2: Additional Constructs***

The final stage of analysis involved testing two additional constructs from exploratory interviews. These constructs were also examined in model 1. Firstly, perceived ownership of health data was examined using two items. It was posited that perceived ownership would positively influence HIPC. Secondly, awareness of health legislation was measured using one item. It was hypothesised that greater awareness of health legislation would negatively influence HIPC. Upon adding these two constructs, the model fit remained strong:  $cmin/df$ : 1.938, CFI .984, SRMR: .025, RMSEA .046. The path analysis revealed a positive, significant relationship between perceived ownership and HIPC ( $\beta = .379$ ,  $p < .01$ ). This offers strong support for H25b. The negative relationship between legislation awareness and HIPC was present and significant ( $\beta = -.081$ ,  $p < .05$ ), H26b is supported. The revised model explained 45.6% of variance in HIPC, 43.5%

of variance in intention to adopt mHealth, 22.8% of variance in intention to use PHRs, 38.1% of variance in intentions to use monitoring devices, and 55.8% of variance related to mHealth applications.

#### ***5.7.10 Model 2: Summary***

Model 2 examined the influence of HIPC on individuals' intentions to adopt mHealth solutions. The proposed model achieved strong model fit. All constructs met reliability and validity thresholds. Hypothesis testing was conducted in four stages. First, the main relationships were tested. Support was achieved for several antecedents including individual characteristics such as age and healthcare need, perceptions of risk and sensitivity, and media coverage awareness. The negative influence of HIPC on intention was not supported. However, HIPC negatively influenced intentions to use mHealth applications. As expected, perceived benefits, health information seeking behaviour, and health ICT experience positively influenced intentions. In addition, perceived risks negatively influenced HINT. In the second stage of analysis, several moderators were tested. The findings supported the moderating influence of chronic illness on the HIPC-MON, and BEM-HINT relationships. Sensitive illness moderated the relationship between HIPC and intentions to use PHRs, and the benefits-intention relationship. Higher experience of personal privacy invasion moderated the influence of HIPC on intentions to use mHealth applications. In stage three, the mediating role of HIPC was rejected due to the absence of a significant relationship between HIPC and intention. In the final stage, the data supported the positive influence of perceived ownership, and the negative influence of legislation awareness on HIPC. The findings show that HIPC is influenced by individuals' characteristics, perceptions, and experiences. Perceived benefits, perceived risk, health information seeking behaviours, and health ICT experience influenced citizens' intentions to adopt mHealth solutions.

### **5.8 Chapter Summary**

This chapter presented the quantitative analysis procedures and findings. The chapter began with an overview of the data cleaning processes and the sample characteristics. The analysis for the

two models was discussed separately. The main findings from both models are depicted below in Table 5.20. The next chapter qualitatively explores the key relationships in both models.

**Table 5.20 Quantitative Findings**

Hypothesised Relationship		Model 1	Model 2
Females express higher HIPC		×	×
Age positively influences HIPC		✓	✓
Healthcare need positively influences HIPC		✓	✓
Poor health status positively influences HIPC		×	×
Trust perceptions negatively influence HIPC		×	×
Risk perceptions positively influence HIPC		✓	✓
Perceived sensitivity positively influences HIPC		✓	✓
Media coverage awareness positively influences HIPC		✓	✓
Health information seeking negatively influences HIPC		✓	×
Health ICT experience negatively influences HIPC		-	×
HIPC negatively influences intention	Adopt	✓	×
	PHR	-	×
	MON	-	×
	APP	-	✓
Perceived benefits positively influence intention		✓	✓
Trust perceptions positively influence intention		×	×
Risk perceptions negatively influence intention		✓	✓
Health information seeking positively influences intention		×	✓
Health ICT experience positively influences intention		-	✓
Chronic illness moderates the HIPC-intention relationship	Adopt	✓	×
	PHR	-	×
	MON	-	✓
	APP	-	×
Sensitive illness moderates the HIPC-intention relationship	Adopt	×	×
	PHR	-	✓
	MON	-	×
	APP	-	×
Health condition moderates the benefits-intention relationship	Chronic Illness	✓	✓
	Sensitive Illness	✓	✓
Privacy invasion experience moderates the HIPC-intention relationship	Personal Data	✓	×
	Health Data	✓	×
Privacy invasion experience moderates the benefits-intention relationship	Personal Data	✓	×
	Health Data	✓	×
Perceived ownership positively influences HIPC		✓	✓
Awareness of legislation negatively influences HIPC		×	✓

✓ Supported, × not supported, ×\* Significant in opposite direction

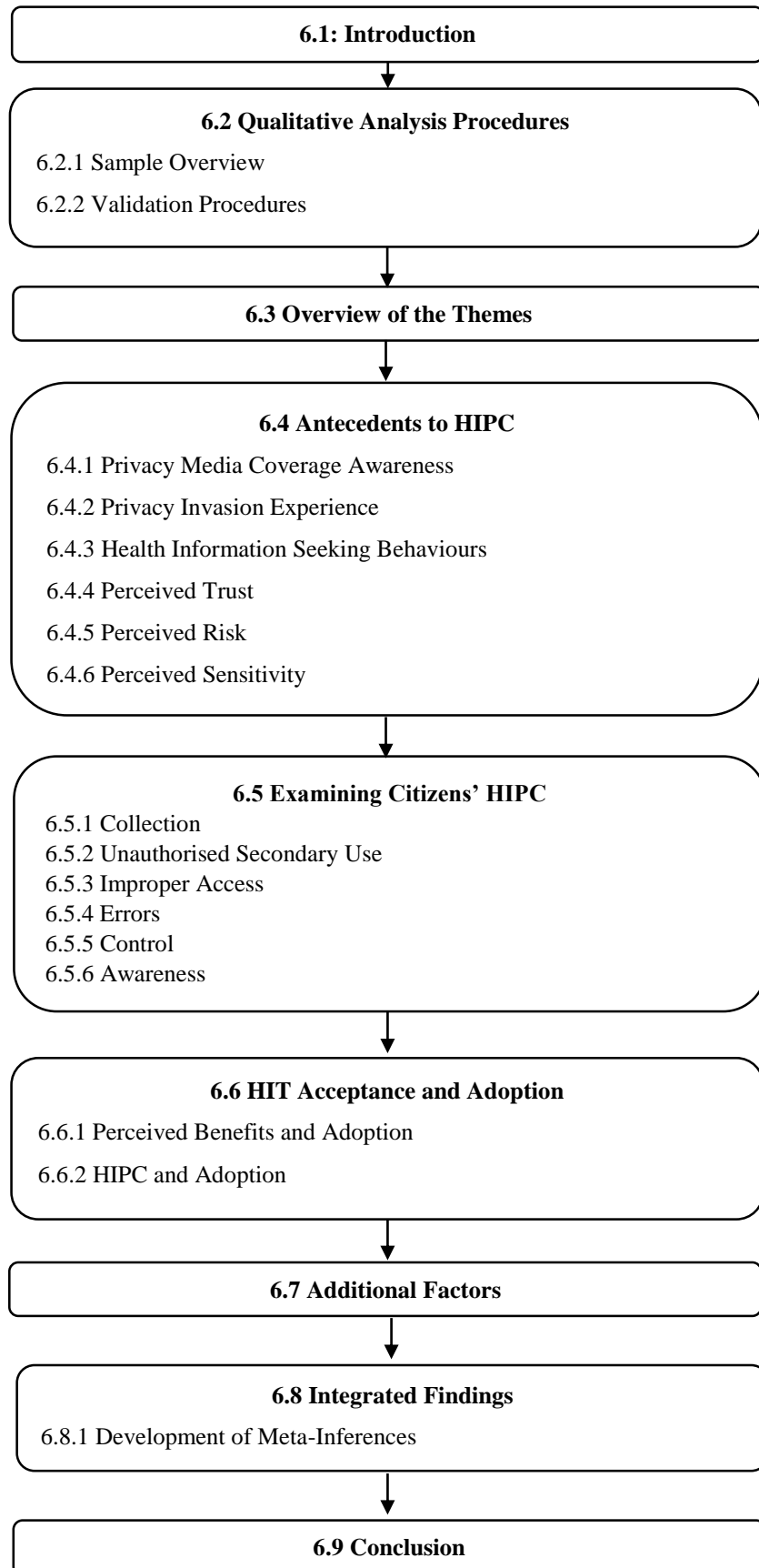


## **CHAPTER SIX: QUALITATIVE ANALYSIS**

### **6.1 Introduction**

This chapter focuses on the qualitative data collected via interviews with Irish and U.S. citizens. Qualitative data was analysed with two main aims. The first aim was to develop a deeper understanding of each construct in the research framework. The second aim was to explore the relationship between each construct and HIPC. The chapter structure is outlined below in Figure 6.1 (pg. 175). The chapter commences with an outline of the qualitative analysis procedures, a description of the sample, and an overview of data validation procedures. The chapter then discusses the main findings from qualitative analysis. In the final section, quantitative and qualitative data are integrated to provide a holistic view of citizens' HIPC.

**Figure 6.1 Chapter Structure**



## 6.2 Qualitative Analysis Procedures

This section provides an overview of the data analysis procedures. Prior to analysis, each interview was transcribed verbatim (Creswell, 2003). Each interview tape was then replayed to correct typographical errors and ensure the transcripts captured all speech, tone, and emphasis. Interview memos were also typed up at this time. The data were analysed based on the framework analysis process described by Ritchie and Spencer (1994). Framework analysis is a popular deductive analysis method which has previously been applied in the MIS discipline (Alavi *et al.*, 2006). It is particularly useful when themes or constructs have been identified prior to analysis (Ritchie and Spencer, 1994). In this study, an interview guide was followed. This guide included all constructs in the research framework outlined in Chapter 3. The research framework represented a starting point for conducting framework analysis. Framework analysis includes five steps:

1. Familiarisation
2. Identifying a Research Framework
3. Indexing
4. Charting
5. Mapping and Interpretation

The aim of the first step was to become familiar with the transcripts. To do so, all transcripts were printed and reviewed. Notes pertaining to the constructs in the framework were added to the margin of each transcript. This provided an initial insight into the views of participants (Creswell, 2003). The second step involved reorganising the data into the constructs represented in the research framework. This was achieved by rereading the transcripts and notes from step one, and categorising all sections of the transcripts based on the construct they represented. For each construct in the research framework, a broad theme and several codes to represent the different aspects or dimensions of the construct were developed prior to the interviews. New sub-codes which further explained the construct were added to the framework during step two.

Reoccurring unidentifiable ideas were also added as ‘additional themes’. This was again completed by hand. The complete coding protocol is outlined in Appendix J (pg. 318), and includes each broad theme and codes, along with the newly developed sub-codes and themes. All text related to each construct in the framework was indexed in step three. This involved dividing all of the transcripts into the themes of interest, while ensuring the overall context of the statement was not lost. The fourth step involved arranging all indexed text into tables which included the headings and explanations drawn from the research framework. Tables were developed for each construct, and are provided in the Appendices (Appendix K-Appendix, S, pg. 320). The final stage involved harnessing these tables to explore the links between constructs in the framework. These links were discussed with the supervisor of the study. The key findings from the qualitative data were then written up in line with the research questions.

An example of the coding process (steps 2-4) is outlined in table 6.1 below. As noted, for each construct, the aim was to understand the construct and explore its relationship with HIPC. The example below pertains to the ‘privacy media coverage awareness’ construct and includes one respondent’s answer. The answer is divided into the pre-existing broad codes representing personal and health data stories. In addition, several sub-codes developed during analysis are relevant in this answer including awareness of breach frequency, degree of familiarity with an injured party, and issue involvement. There is an explicit link between privacy media coverage awareness and HIPC, as the respondent expresses a desire for her data to be protected against excessive sharing.

**Table 6.1 Coding Example**

Transcript Extract	Personal: “There was the leak of photos of Jennifer Lawrence from the cloud. A breach can happen to anyone, my parents’ credit card was scammed twice within a month and they would be careful. There’s a lot of largely publicised breaches, the Sony breach a few years back and recent ones they’ve had.” Health: “I’ve heard of breaches alright. Like laptops being stolen. There’s been breaches in celebland about such a person got plastic surgery. I saw online X-ray images of someone who got a coffee jar stuck somewhere unfortunate—shared worldwide isn’t that scary? Quite horrific, imagine that was you. I certainly wouldn’t want my labour story shared with the world, graphic details definitely not.”		
Theme/Construct	Privacy Media Coverage Awareness		
Codes	Personal Data “photos of celebrities”	Health Data “(X-ray) films shared with the world”	
Sub-Codes	Awareness of frequency “lots of publicised breaches”	High degree of familiarity “my parent’s credit cards”	Issue Involvement (High) “Isn’t that scary?”
Link to HIPC	Concerns for own health data “wouldn’t want my labour story shared”		

### 6.2.1 Sample Overview

As some interviewees discussed sensitive issues related to their health, it was imperative to preserve their anonymity. Therefore, a table outlining the characteristics of interviewees is not provided. Instead the characteristics of the qualitative sample are outlined following O’Cathain *et al.*, (2014). A total of 50 interviews were conducted (25 American and 25 Irish). Interviewees included males (n=19) and females (n=31). The three age groups were represented, 18-24 (n=12), 25-49 (n=22), 50+ (n=16). In terms of education, some interviewees had completed or partially completed high school (n=9), some had partially completed their college education (n=12), many had an Undergraduate degree (n=13), and the remainder had a Postgraduate qualification (n=17). Interviewees were students (n=14), retirees (n=7), and employees in industries such as Finance (n=4), Technology (n=5), Health (n=3), Retail (n=3), and Education (n=7).

### 6.2.2 Validation Procedures

While there is no one set of guidelines for reviewing and validating qualitative research, it is imperative to validate qualitative findings. In line with the recommendations of Venkatesh *et al.*,

(2013), the study sought to ensure qualitative validity across three categories: design validity, analytical validity, and inferential validity. These categories encapsulate the recommendations of many qualitative researchers including Cook and Campbell (1979), Shadish *et al.*, (2002), and Teddlie and Tashakkori (2003).

Design validity includes descriptive validity, or the accuracy of the data in representing participants' views, experiences, and behaviours (Maxwell, 1992). To achieve descriptive validity, a number of procedures were completed. Throughout the interviews, the researcher used probing and follow-up questioning techniques to increase the comprehensiveness of participants' descriptions. In addition, when analysing and interpreting the qualitative data, transcripts were read a number of times, and tapes were replayed to listen for tone and emphasis. This added confidence to how quotes were used and how the participants' views were represented. Design validity also encompasses credibility, which involves illustrating that qualitative findings are believable from participants' perspectives (Lincoln and Guba, 1985). To ensure the credibility of the data, informal member checks were conducted. Member checking is valuable as it enables interviewees to correct errors, clarify ambiguous statements, and add further explanations (Lincoln and Guba, 1985). Member checks involved asking interviewees if the researcher's interpretation of a statement was correct. Informal member checks occurred throughout interviews as they arose, and at the end of the interview. In addition, triangulation in the form of collecting data using multiple methods supports credibility. Negative cases were given special attention as recommended by Mays and Pope (2000). When interviewees expressed competing views, these views were probed to determine the underlying reasons. Throughout analysis, negative cases were highlighted and explained further.

Design validity also includes transferability or the ability to generalise the findings to other contexts. While the generalisability of qualitative data is often questioned, and may not be the goal of the study, researchers should seek to ensure their findings are at least, in part, transferable to additional times and contexts (Venkatesh *et al.*, 2013). This study collected data in two countries, from participants of different ages and backgrounds. By exploring the relationships of

interest across this diverse set of participants, the findings represent different groups. In addition, great efforts were made to gain thick descriptions of participants' context and views. This rich description coupled with purposive sampling provide the details necessary for future researchers to re-explore these issues and determine transferability (Lincoln and Guba, 1986).

Analytical validity refers to how the qualitative data were collected and analysed. Analytical validity is comprised of theoretical validity or how well theoretical explanations fit the data. Theoretical validity requires that the concepts leveraged in theory make sense, and that the hypothesised relationships between concepts are credible (Maxwell, 1992). This study extends a number of theories to the context of health information privacy and seeks to explain these theories in this context. Thus, many of the concepts harnessed in these theories are based on previous research. Consulting the literature adds support to the chosen concepts. In addition, to ensure the hypothesised links between concepts in these theories were credible, quantitative and qualitative findings were integrated. The combination of different data types supports the credibility of the theoretical insights developed in the study (Lincoln and Guba, 1985). Analytical validity also pertains to the dependability and consistency of data. A number of external checks were conducted to ensure dependability and consistency. The researcher's supervisor reviewed the interview guide prior to the interviews. This ensured questions were appropriately phrased and addressed the issues of interest. The interview guide was also piloted on a convenience sample representing the interview participants. This further tested the neutrality and phrasing of the questions. At the analysis stage, the supervisor compared the researcher's interpretations with the original transcripts to determine their dependability and consistency. Lastly, analytical validity requires that the conclusions reached are plausible (Venkatesh *et al.*, 2013). To determine plausibility, the conclusions were reviewed in line with the overall view expressed by the participant. Conclusions were also compared with the literature to determine if they corroborated previous findings, and if not, that there was a logical explanation for this deviation.

Inferential validity refers to the accuracy of the researcher's inferences and the confirmability of findings (Venkatesh *et al.*, 2013). In order to achieve inference validity and confirmability,

several methods discussed above were followed including gathering data from multiple methods to develop a coherent justification for inferences, using thick descriptions to support inferences, and member checking. A number of methods advised by a host of qualitative researchers were followed to ensure the study's qualitative findings were valid. These findings are now discussed with confidence in their validity, trustworthiness, and credibility.

### **6.3 Overview of the Themes**

The interviews explored three research questions. To answer the first research question, a number of antecedents to HIPC were explored. In line with the second research question, the six dimensions of HIPC were investigated. To address the third research question, interviews explored the relationship between HIPC and interviewees' (1) acceptance of EHRs and (2) personal mHealth adoption. The qualitative findings pertinent to each research question are now discussed, beginning with the antecedents to HIPC.

### **6.4 Antecedents of HIPC**

The research framework included several antecedents to HIPC related to individuals' characteristics, perceptions, and experiences. This section discusses each antecedent individually.

#### ***6.4.1 Awareness of Privacy Media Coverage***

The interviews aimed to gain an understanding of interviewees' awareness of privacy-related media coverage (generally and related to health data), and the relationship between media coverage awareness and HIPC.

##### ***6.4.1.1 General Awareness of Privacy Media Coverage***

The majority of interviewees were aware of privacy media coverage. Interviewees noted a variety of sources they heard privacy-related stories from, including: TV, radio, newspapers, online news outlets, social media, and friends or colleagues. The variety of sources was matched by the diversity in stories discussed. Interviewees recalled stories of data breaches, physical loss of data



and devices, circulation of misinformation, improper access to information, and financial theft. Stories also varied in terms of the party of interest, from large corporations to individual citizens. While the majority of interviewees noted the increasing presence of these stories, some interviewees were less aware as they don't 'pay attention to the news', or don't believe such stories are 'reported in the mainstream news'.

Many interviewees were less aware of privacy media coverage regarding health data. Some interviewees noted the danger of health information misuse, and their belief that insurance companies engage in 'dodgy practices' to access health data. Others believed that misuse of health data occurs less frequently. Among these interviewees, some U.S. participants cited HIPAA, the legislation governing health data usage, as reasoning for this lower frequency. As shown below, the interviewee believes HIPAA protects health data.

*I think health information, especially with HIPAA is locked down. I've never heard of anybody losing their health information.*

*P43, Homemaker, USA.*

Individuals with an awareness of health privacy media coverage discussed a range of incidents such as access to patient data by unauthorised employees, physical loss of patient files and laptops, the leakage of patient x-rays, and large data breaches at healthcare organisations.

#### *6.4.1.2 Privacy Media Coverage and HIPC*

This section discusses the several factors within the privacy media coverage awareness construct which influenced interviewees' HIPC.

##### ***Degree of Familiarity***

Interviewees recalled stories pertaining to a host of parties. These stories varied in specificity from general stories in 'celebland', to incidents related to a specific celebrity. Organisations were also mentioned in a general sense such as 'health offices' or 'consumer companies', as were specific organisations such as Sony, and Target. In addition, many interviewees shared the experiences of their friends, family members, and colleagues. The effect of privacy experiences

on interviewees' perceptions varied along with their familiarity with the victim. The experiences of familiar individuals and organisations had a stronger influence than the experiences of an unfamiliar party. Interviewees with a high degree of familiarity with the victim of a privacy invasion, expressed higher concerns for their own privacy.

*My daughter bought Uggs off a website and she never got them or the money back, they were con artists. I wouldn't buy online; I'd be terrified that would happen to me.*

*P16, Retail employee, Ireland.*

*I remember the big breaches in stores like Target. They were particularly scary. It was definitely concerning because I have been to those stores.*

*P36, Education, USA.*

As illustrated above, high familiarity with the victim of a privacy invasion can foster fears regarding the interviewee's own data, and increase their perception of the risk to their data. Interviewees reflect on the fact that privacy breaches can affect people like themselves, and question their own vulnerability.

### ***Understanding of Risk***

Interviewees' comprehension of the risks to their own data also influenced their HIPC. Interviewees with a greater level of understanding, provided in-depth accounts of stories noting details such as the injured party, the perpetrator, the level of information loss, and the outcome. These interviewees also engaged in personal reflection, and questioning of how they might be at risk. In addition, interviewees who discussed many different examples affecting different parties, demonstrated a deeper understanding of the breadth of risks to their personal data. In the below example, the interviewee recalls an incident where X-rays were shared worldwide. She reflects on her own and her son's health data, and expresses her desire for her information to remain private. This shows the link between her awareness of privacy media coverage and HIPC.

*I saw X-ray images of someone who got a coffee jar stuck somewhere unfortunate, those films were shared worldwide isn't that scary? Quite horrific, imagine that was you. I wouldn't want my labour story shared with the world. I wouldn't want my son's information going anywhere.*

*P8, I.T. Professional, Ireland.*

### ***Issue Involvement***

Issue involvement is described as the attention paid to privacy stories and the level of cognitive effort expended to understand these stories. When issue involvement is high, individuals tend to reflect on their own experience and consider their own vulnerabilities. In the quote below, the interviewee discusses her plans in the event of a breach occurring.

*I follow the news, if Target got hacked again, I'm going to pay attention. If any other company I do business with reports a data breach, I'm going to reset passwords or do what they advise.*

*P34, Education, USA.*

In contrast, low issue involvement coincided with lower reflection on personal risks. The below quote serves as an example of this. This interviewee is broadly aware that data can be misused but is not interested in learning more or understanding the risks to her information.

*I haven't really paid attention. I know it happens to people but I'm not really tuned into it, I don't watch out for it, it's not in the mainstream news enough to make me think about it.*

*P40, Social Care Professional USA.*

### ***Discounting the Risk***

When discussing privacy media coverage, some interviewees expressed lower privacy concerns. These interviewees offered three reasons for their lower concerns. Firstly, interviewees discussed the privacy controls they utilise to limit their risk. These interviewees perceived that technical measures such as deleting cookies, as well as falsifying data disclosed, and minimising disclosure would protect them from privacy invasions. In addition, interviewees often compared themselves to others, viewing themselves as more cautious and thus less at risk. As evidenced in the quote below, this comparison enabled interviewees to discount their own vulnerability and explain their lower concerns.

*I believe most people have their information misused. I use my browser more securely, I disable tracking, I won't go on websites that track, I block them, for me it's a bit easier being in to technology.*

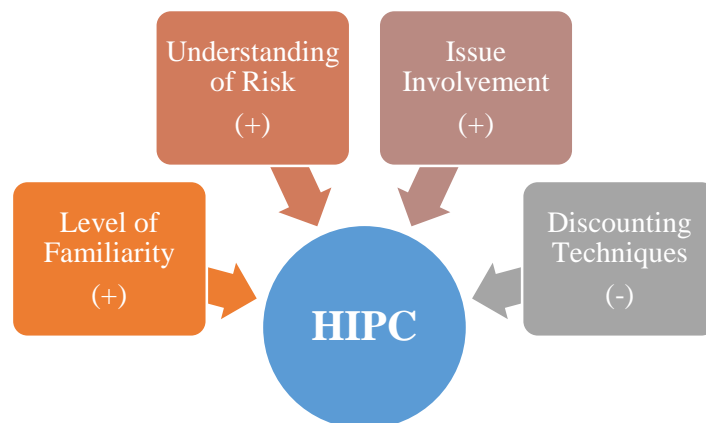
*P44, I.T. Professional, USA.*

Secondly, some interviewees stated that little health data existed about them, and as none of this data was embarrassing or sensitive, they had lower concerns. Thirdly, some interviewees felt that

as they did not utilise health technologies, their health data was safe. Other interviewees noted that they had only disclosed ‘non-sensitive’ health data when using fitness mHealth applications, or searching for health data online. If the health information disclosed was non-sensitive or minor, interviewees believed that there would be no serious repercussions if the privacy of this data was breached. This is a means of further discounting the risk. While these interviewees may be incorrect in their estimations of how little health data exists about them, or how much data they have disclosed, and the potential repercussions, it is important to note that these estimations reduce their privacy concerns. These perceptions are described as methods of risk discounting.

- **Summary Point: Privacy media coverage awareness can increase HIPC. This influence is strengthened by degree of familiarity, understanding of risks and repercussions, high issue involvement, and weakened by efforts to discount one’s personal risk.**

**Figure 6.2 Privacy Media Coverage and HIPC**



#### **6.4.2 Privacy Invasion Experience**

The interviews sought to develop an insight into interviewees’ privacy invasion experience, which was examined as a moderator in the survey, and to explore the influence of these experiences on HIPC.

##### **6.4.2.1 Interviewees’ Privacy Invasion Experience**

Interviewees’ privacy invasion experiences ranged from targeted advertising to financial loss, or social media hacking. Interviewees discussed their experience of ‘invasions’ carried out by

individual hackers, familiar organisations, and unknown third parties. The few interviewees who stated that their data had never been used excessively, believed their health data was not in circulation and thus there was no risk to their privacy. There was a clear disparity between the volume of experience individuals had with ‘invasions’ of their personal data, and ‘invasions’ of their health data. The majority of interviewees discussed experiences where their personal data was misused. A smaller number of interviewees recalled occasions where their health data privacy was invaded. These experiences are illustrated in the quotes below and included receiving communications from unfamiliar health organisations and the loss of data in a breach.

*I got this bowel screening letter, [it] said the department of social protection have given us names. That was an invasion, without your knowledge. In one way its good, but I thought how much information is out there about me, and who are they giving it to?*

*P12, Retired, Ireland.*

*I got a letter from Diabetic Ireland saying we're doing research. I ask 'why did you send for me, how did you get this information?' and they say 'from your doctor'. Diabetes Ireland is funded by people who sell products, there's a commercial aspect that I wouldn't be too cooperative on.*

*P2, Retired, Ireland.*

*I was in the Blue Cross batch that got stolen. We got a notification saying it's possible our information will be used, and they would pay for identity theft recovery which is terrifying, especially with health stuff, maybe that's going to affect how I receive healthcare in the future.*

*P39, Administrative Professional, USA.*

Several insights can be drawn from these quotes. Firstly, individuals feel invaded when their health data is shared without their knowledge. The first two interviewees note their surprise at receiving communications from unfamiliar organisations. Secondly, individuals do not want their health data to be used in ways which they disagree with. The second interviewee notes his disagreement with commercial uses. Thirdly, experience of privacy invasion causes individuals to reflect on their personal vulnerability. This is apparent in all quotes, with interviewees questioning what parties have access to their health data, what health data exists about them, possible uses for their data, and possible negative outcomes.

#### *6.4.2.2 Privacy Invasion Experience and HIPC*

This section discusses the several facets of privacy invasion experience which impacted HIPC.

### ***Surprise vs. Expectation***

Interviewees had different reactions to their experiences of privacy invasion. Some were upset, while others expressed slight irritation. Interviewees' level of surprise also varied, some were extremely shocked, while others expected such things to happen. Interestingly, individuals who expressed surprise did not differ in age with young and older (>50 years of age) interviewees expressing surprise regarding an invasion. However, for younger interviewees, this surprise was short lived and was only upon the initial realisation that their data was used in such a way. They then accepted that this could happen, or came to expect it would reoccur. For older interviewees, surprise at how their data was used led to heightened privacy concerns. The quotes below illustrate the role of surprise.

*I realised the power of data when ads targeted at gay people started coming up. It took me aback a little. I'm okay with now but I was surprised at first.*

*P49, Student, USA.*

*I got a letter from my gas company to say people had got on some site where you pay your bill. That did frighten me. I wouldn't pay direct debit, I'd pay in the post office, but I've gone online again, it's convenient. They didn't go into the risks, I didn't ask, I took it for granted it would be safe.*

*P13, Health Professional, Ireland.*

The first interviewee, an American student discusses his surprise when online ads were targeted at him due to his sexuality. He was initially shocked but now accepts these practices as the norm. In the second quote, a 55-year-old nurse from Ireland discusses her experience of being involved in a data breach. The experience resulted in fear, and she initially switched to offline payment. Her lack of understanding of the online risks, and the repercussions of privacy breaches is evident. Older interviewees were surprised that invasive practices were possible, and while many ultimately accepted these practices, they lacked an awareness of what these practices meant for their data. While younger interviewees were often initially surprised following a specific incident, they had a broad awareness of data collection and usage online. As a result, they quickly accepted these practices and understood the reasoning behind them.

### ***Low vs. High Severity***

Invasion experiences ranged in severity based on the interviewee's perception. Some interviewees discussed similar experiences but differed in their perception of severity. Two broad experiences are discussed to illustrate the role of perceived severity: targeted advertising and financial loss.

Interviewees' perception of the severity of targeted advertising varied. Some interviewees, while irritated or initially surprised by targeted advertising, dismissed its severity. Others expressed strong opposition to targeted advertising, and viewed it as a severe invasion. These individuals reflected on how targeted advertising practices influenced their privacy and reacted either passively or proactively. Passive reactions included expressing a desire to browse free from advertising, and expressing the belief that online companies should respect their privacy (P6). Proactive reactions included complaining to the organisation (P20). While reactions differed, when interviewees viewed the invasion as severe, they considered their personal privacy, felt a lack of control over their privacy, conveyed their desire for greater privacy, and engaged in actions which they believed gave them control. On the other hand, interviewees in the 'low severity' group, engaged in less reflection and dismissed this practice as an 'Internet norm'.

In terms of data and financial loss, interviewees' experiences included fraudulent charges and data loss through largely publicised breaches. Two interviewees discussed fraudulent charges, but their perception of severity differed. One interviewee expressed the view that such charges were unavoidable when shopping online, whereas the other interviewee discussed her efforts to reduce the risk of reoccurrence including limiting data disclosure, and only purchasing online from well-known companies. Two interviewees had experienced multiple privacy invasions. The first interviewee had experienced financial theft twice. The second interviewee had been involved in a number of large scale breaches at well-known organisations. Both interviewees viewed their experience as severe, but they differed in terms of self-reflection on their personal privacy. The first interviewee felt vulnerable and unsure of how to act going forward. The second interviewee also considered her privacy and possible secondary uses for her data. However, in her more recent

experiences she engaged in less reflection, as she feels safe under the identity protection insurance she received following a prior breach. These quotes support the link between severe experiences and HIPC, especially when the individual feels vulnerable to future invasions.

*Thousands of dollars were charged and I was getting credit score notifications. It's scary, do I go about business as usual or am I doing something wrong?*

*P34, Education, USA.*

*I've gotten identity protection twice from Sony. Who knows if they did anything with the information. I was also involved with Target. The first time I was afraid I thought what are they going to do with my information. Every time since then it bugs me but I worry less because I have identity theft protection.*

*P42, Student, USA.*

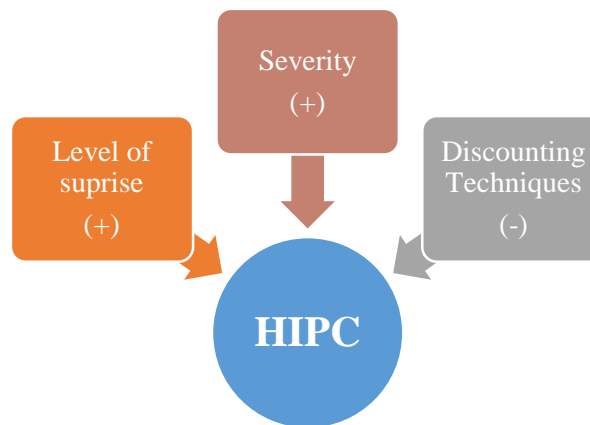
### ***Discounting the Concern***

As evidenced in section 6.4.1, individuals' HIPC is often diminished by discounting techniques. When discussing their privacy invasion experience, interviewees again noted these discounting techniques. Some interviewees falsified data, which increased their perceived control over their privacy. In addition, some interviewees believed they were aware of all data they disclosed, and when they noticed targeted ads for example, they were not concerned as they knew the data the ad related to. The misconception that only data they explicitly disclosed is pertinent to their privacy, and the assumption of control allowed interviewees to feel safer and express lower HIPC.

- **Summary Point: Privacy invasion experience can increase HIPC. This influence is strongest when invasions were unexpected and severe, but can be weakened by discounting techniques.**



**Figure 6.3 Privacy Invasion Experience and HIPC**



### **6.4.3 Health Information Seeking Experience**

Interviews aimed to gain an insight into interviewees' online health information seeking experience, and the link between this experience and HIPC.

#### *6.4.3.1 Interviewees' Health Information Seeking Experience*

The majority of interviewees had experience seeking health data online. The frequency of this use ranged from 'rarely' to 'every second day'. Many regular users described the Internet as an initial source of health information, whereas irregular users preferred to seek advice from health professionals. Some interviewees discussed seeking information for others including children, partners, friends, siblings, or clients. Interviewees also discussed seeking health information for themselves across a range of areas. For instance, several interviewees regularly sought fitness information. Many of these interviewees were younger, but two older interviewees had searched for specific diet plans online. Interviewees also discussed searching online for self-diagnosis. The majority of these problems were seemingly minor such as bug bites, cough symptoms, or muscle strains. In a number of cases, interviewees sought information as a means of comfort, or assurance that the issue was minor. Interestingly, only one interviewee discussed searching for information to help manage a current illness. This interviewee frequently searches online for information and tips for managing her condition. The final reason for seeking health information online was for educational purposes. This included students on health-related programmes and

interviewees employed in a health organisation who sought information to understand medical terms or a specific condition.

### ***Views on Credibility and Risks***

Interviewees discussed a number of dangers associated with utilising the Internet as a source of health information. The majority of interviewees were wary of the authenticity of health information online. Younger interviewees stated they would not trust the opinions offered on blogs or forums. Many older interviewees were surprised that unqualified individuals had the ability to state their opinions online. Some interviewees stated that they would not trust any information they found online, while others expressed trust in websites they deemed official such as websites related to the Mayo Clinic, the Center for Disease Control, and the National Health Service (NHS). Interviewees viewed these websites as reliable because information came from medically trained individuals and was based on research. Health websites such as WebMD were viewed more favourably among some interviewees due to their popularity. Other drawbacks mentioned by interviewees included extreme diagnoses, risk of unnecessary worry and panic, and potential to become obsessed. Many believed that extreme diagnoses could incite panic, fear, and worry. Some interviewees had experienced these negative outcomes (P26), and others stated they would not search online for health data due to a fear of these negative outcomes.

#### ***6.4.3.2 Information Seeking and HIPC***

The majority of interviewees did not mention privacy issues associated with seeking health data online. Interviewees may not consider privacy when seeking health information online, as many interviewees do not view this behaviour as active data disclosure, and thus do not see a reason to consider privacy. One interviewee stated that the Internet is “broad, it’s subjective, it’s commonality, and it’s for everybody. I wasn’t looking up my own records” (P11, Insurance professional, Ireland). This illustrates the interviewee’s perception that he did not disclose any health data when searching online. There was evidence that individuals engaged in techniques to protect their privacy. For instance, one interviewee spoke about a fertility forum she was a member of. While she found the community very valuable, she utilised a pseudonym, and limited

her data disclosure to positive experiences. This provided her with a sense of perceived privacy while also enabling her to benefit from the online community. Another interviewee limited the type of information she would search for online. She would search for fitness data but would not search for information related to her health conditions. Two interviewees explicitly discussed their privacy concerns regarding the potential secondary use of data that online companies derive from health information searches. These quotes are provided below.

*If you find a lump, you might want to Google it before going any further and now you're being targeted for breast checks, it's very upsetting, you want Google to forget you ever searched for it but they won't.*

*P8, I.T. Professional, Ireland.*

*You Google something and then Facebook is reminding you to take your contraceptive pill. It's worse if they do it with health data, that's so personal they shouldn't be using that to target advertising.*

*P5, Masters Student, Ireland.*

- **Summary Point: While many interviewees did not explicitly discuss HIPC, individuals who were aware of the privacy risks expressed concerns about invasive practices, and engaged in privacy-protective behaviours.**

#### **6.4.4 Perceived Trust**

The interviews aimed to develop an insight into individuals' trust in health professionals and health technology vendors, and to investigate the link between trust and HIPC.

##### **6.4.4.1 Overall Trust**

Many interviewees expressed high default trust in health professionals. Interviewees stated they had 'strong trust', and 'complete trust' in health professionals. The reasons for high default trust included strong relationships, the importance of trust in doctor-patient relationships, positive experience to date, and no reason 'not to trust'. A small number of interviewees expressed low trust in health professionals, due to negative experiences, or frustration with the health system in general. In contrast, the majority of interviewees expressed low default trust in technology vendors. Descriptions included: 'I wouldn't trust them', and 'I don't trust them at all'. Reasons

for this low trust predominately pertained to the commercial motivations of technology vendors. When comparing trust, many interviewees expressed higher trust in health professionals for several reasons. Firstly, interviewees preferred the personal relationship with health professionals, as opposed to the anonymity of the Internet. Secondly, interviewees discussed their lack of control over data disclosed online. Thirdly, interviewees stated that health professionals required health data, but technology vendors did not. A small number of interviewees had higher trust in technology companies, due to prior negative experiences with health professionals.

### ***Competence***

In terms of health professionals, competence related to individuals' perception of their ability to treat them. Many interviewees had high trust in health professionals' competence based on their professional qualification and extensive knowledge. However, some interviewees discussed the potential negative impacts related to human error and external factors such as understaffing and pressure. Views of competence were also influenced by experience to date, with positive experiences leading to high perceived competence, and negative experiences associated with low perceived competence. The influence of negative experiences on individuals' views of competence and overall trust varies. At the basic level, negative experience can influence perceptions of competence regarding a specific health professional. For instance, some interviewees changed their general practitioner following negative experiences, but did not express low trust in general. Ongoing, negative experiences reduced individuals' perception of the competence of all health professionals, and their overall trust. In the quote below, the interviewee discusses her experience of seeking a diagnosis and her frustration at visiting different health professionals without an answer. Her disillusion with the healthcare profession is evident.

*At this stage, I would probably trust a technology company more, well I reckon the information I get there would be equally as good.*

*P12, Retiree, Ireland.*

In terms of technology vendors, competence relates to perceptions of the validity of the health information retrieved online. This form of competence was discussed to a lesser degree, and was

generally negative. For example, one interviewee noted that due to the prevalence of ‘strange diagnoses’ she does not trust the validity of information online or in mHealth solutions.

### ***Integrity***

Integrity refers to individuals’ perceptions of how honest health professionals and technology vendors are with their health data. There was a large disparity between perceptions of health professionals’ and technology vendors’ integrity. The majority of interviewees believed that technology vendors had little integrity and health professionals had high integrity. This was generally consistent across interviewees, even those with low overall trust in health professionals believed they would uphold ethics. Interviewees cited the Hippocratic Oath and HIPAA, and noted their assumptions of confidentiality, to explain their perceptions of integrity. In addition to assuming integrity, some interviewees chose their health professionals based on a personal recommendation or research, and thus trusted their integrity. In contrast, the majority of interviewees did not believe technology vendors would treat their health data with integrity. The reasons offered for these views revolved around the commercial aims of these companies, and the view that they only seek health data for monetary reasons, whereas health professionals require this information to administer treatment. The below quote encapsulates the opinion expressed by many, that technology vendors would seek to profit from individuals’ health data. As a result, the interviewee states that he would not provide technology vendors with any health data.

*To me, big companies, no principles, no nationality, there’s no faithfulness, they’re just there to make money, and that is the bottom line. I would be short on trust as to what they would do with that information. I wouldn’t give it to them.*

*P15, Retiree, Ireland.*

Some interviewees stated that they would disclose fitness or non-sensitive data, in order to use mHealth solutions. Information Boundary theory (IBT) is supported here as individuals decide that certain information can be disclosed, but will withhold sensitive data. The Privacy Calculus is also evident, as individuals compare the benefits and risks associated with mHealth solutions. This is evident in the quote below, the interviewee uses mHealth, as she believes the benefits outweigh the risks.

*Fitness is important to me. I don't mind giving it return for what I get. I don't give anything sensitive just fitness information.*

*P27, Mature Student, USA.*

A small number of interviewees trusted the integrity of technology companies. These interviewees were inexperienced with technology and assumed that technology companies would only use their data fairly. For example, one interviewee assumed that technology vendors “*would put in a statement or ethos*” (p15). As these interviewees have no experience with providing their health data to these companies, they have no negative experiences, but they are also uninformed of the potential risks. Individuals may desire privacy, but this uninformed view of technology vendors leads to a blind trust, a potentially skewed level of privacy concern, and possible future use of technology without understanding of the risks.

### ***Benevolence***

Benevolence relates to individuals' perceptions that health professionals and technology vendors will act in their best interests when handling their data. Again, the majority of individuals believed health professionals were benevolent in their actions, but technology companies were not. The reasons for these views again relate to confidentiality assumptions and legal requirements. With regards to technology vendors, the dominant reason for low trust related to their commercial goals. In the quote below, the interviewee notes that technology companies serve to meet the interests of their shareholders not citizens. As a result, he states he would not provide technology companies with his health data.

*I don't trust them at all. Why should they be acting in my best interests, they should be acting in their shareholders' best interests. I wouldn't trust them with my health data and wouldn't give them it.*

*P21, Research, Ireland.*

### ***Institutional vs. Individual Trust***

There were notable differences in interviewees' trust in individuals and their trust on an institutional or system level. Many interviewees expressed high trust in individual health professionals including specific individuals like their GP or pharmacist, and trust in health

professionals in general. In some cases, trust waned when interviewees' discussion moved from the individual level to a broader level. In Ireland, interviewees often expressed high trust in health professionals but were less trusting of the health system. For example, in the quote below, the interviewee trusts health professionals' competence but expresses a negative view towards the overall health system in Ireland due to its inefficiencies.

*I don't think our health system is too good, the availability of beds is ridiculous. My mam had a seizure and she was waiting 7 hours to be seen. I definitely trust doctors' ability to treat and diagnose me.*

*P10, Student, Ireland.*

In the U.S., a small number of interviewees expressed lower trust in health organisations. As many healthcare organisations in the U.S. are private entities, interviewees expressed concerns regarding the methods they will use in pursuit of their financial goals. In the quote below, the interviewee trusts the integrity of health professionals, but not health organisations.

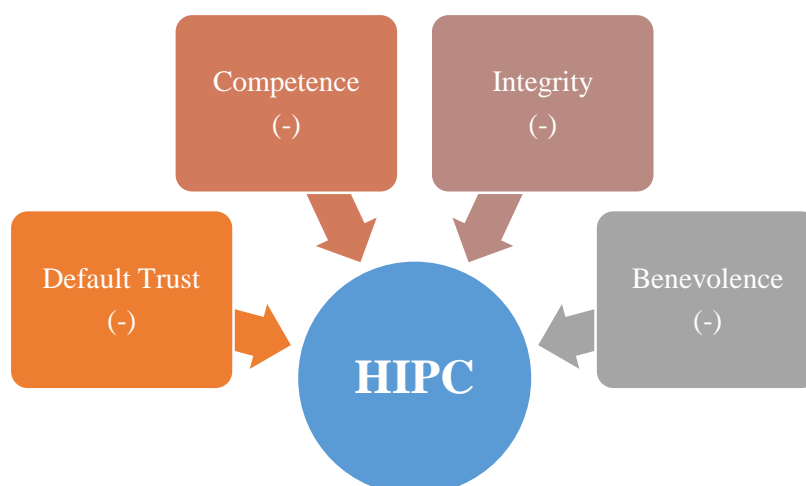
*As far as professionals, I've no problem with their integrity, it's when you start getting involved with corporations that own doctors' offices and hospitals, I have no trust in. Information sharing, its money for them.*

*P35, Naval Professional, USA.*

#### 6.4.4.2 Trust Perceptions and HIPC

There was an evident relationship between trust and HIPC. The relationship between trust and HIPC is complex, due to the number of parties involved and the various components of trust.

**Figure 6.4 Perceived Trust and HIPC**



Several assertions pertaining to this relationship are made based on the interviews. Firstly, the interviews provided evidence that high trust could reduce individuals' HIPC. Interviewees who had high default trust in health professionals, did not express high privacy concerns. Some of these interviewees assumed their data would be safe, while others noted they had no reason to question the privacy of their data, due to high trust. In terms of technology vendors, many interviewees expressed low levels of default trust. Some of these interviewees stated they would not provide such companies with health data, due to their belief it would be misused. When default trust is high, and unquestioned, individuals often express low default HIPC. The reverse is also apparent. When individuals have low default trust, they assume their data won't be private and often engage in privacy-protective behaviours.

Secondly, there is a relationship between competence and HIPC. When interviewees discussed competence in terms of diagnosis from health professionals and information received from technology vendors, privacy was often not explicitly relevant. However, some interviewees discussed competence in terms of health professionals' and technology vendors' ability to keep their data private. A number of interviewees questioned health professionals' ability to keep their data safe, as security is not their area of expertise. These interviewees expressed concerns regarding improper access to their health data. Conversely, many interviewees believed technology vendors were capable of keeping this data safe.

Thirdly, views on integrity influenced HIPC for many interviewees. These concerns pertained predominately to unauthorised secondary use. Many interviewees assumed health professionals would be honest when handling their health data. They viewed health professionals as honest and thus expressed low concerns regarding the misuse of their data. In contrast, a large number of interviewees believed that technology companies would not be honest in how they used their health data, and thus expressed concerns regarding potential secondary use.

Fourthly, opinions on benevolence also related to individuals' perceptions regarding unauthorised secondary use. Many interviewees believed that health professionals had their best interests at heart. They believed that health professionals only required health data for health purposes, and



assumed they would not misuse data as ‘there was no other reason for them to use it’. In contrast, several interviewees believed technology vendors’ intentions were purely commercial and as a result were highly concerned regarding possible secondary use of their health data.

- **Summary Point: The link between HIPC and trust is influenced by the nature of the trust; with blind trust leading to blind assumptions of privacy, and specific trust issues such as competence, integrity, and benevolence impacting concerns regarding several dimensions of HIPC.**

#### **6.4.5 Perceived Risk**

The interviews aimed to develop an understanding of interviewees’ perception of the risks associated with disclosing health data to health professionals and technology vendors, and to explore the link between perceived risk and HIPC.

##### *6.4.5.1 Perceived Risk: Health Professionals vs. Technology vendors*

Interviewees’ perception of risk can be divided into three broad views. Interviewees expressing the first view, believed there was a higher risk to data disclosed to technology vendors than data disclosed to health professionals. These interviewees believed health professionals would only use the data for the patient’s benefit, but technology companies would use data for commercial goals. The primary risks expressed by these individuals included the sale of data to third parties, sharing of data, and misuse of health data. Interviewees adopting the second view believed the risk of loss was higher with health professionals, as they were less competent in protecting this data. These interviewees noted that health professionals did not have the same level of technical expertise, and thus were vulnerable to attackers. The final view was that risk existed in both situations, but this risk differed in terms of the audience and type of risk. These interviewees noted that risk is omnipresent due to the permanency of digital data, and the potential for any server to be hacked. For example, the interviewee below compares the physical risks of access in the health setting, with the digital risks associated with data stored by technology vendors.

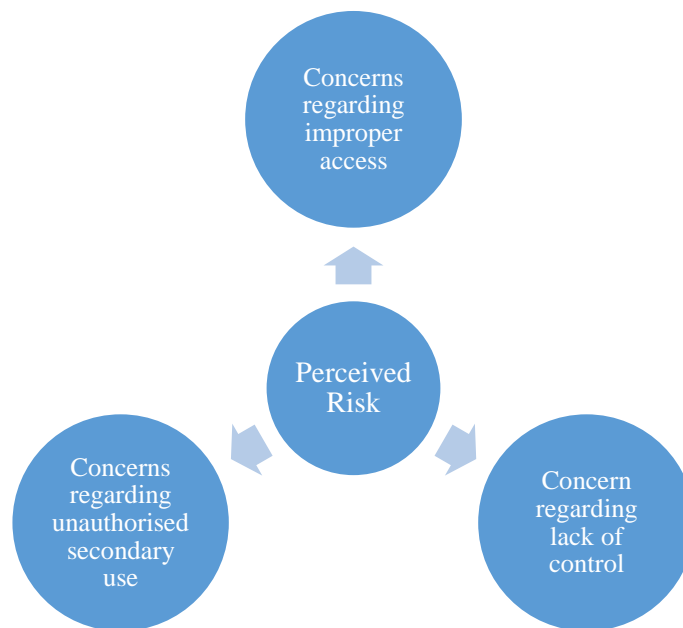
*In a doctor's office somebody can walk away with a file, or copy a file, so you're more at risk to just unethical people, whereas with the data company it's who they're sharing and selling your data to. It's a different level of risk.*

*P34, Education, USA.*

#### 6.4.5.2 Perceived Risk and HIPC

Perceived risk can increase concerns across three dimensions of HIPC, as outlined below.

**Figure 6.5 Perceived Risk and HIPC**



Firstly, perceived risk was strongly linked to concerns regarding secondary usage. When individuals believed disclosing their health data to health professionals or technology vendors would result in a negative outcome, they expressed high concerns regarding possible unauthorised secondary use. When perceived risk was low, individuals did not express high concerns regarding possible unauthorised secondary usage. Interviewees assumed health professionals would seek consent prior to secondary usage, while the common view was that technology vendors would use data without permission. Interviewees also noted their disagreement with secondary uses, indicating a high desire for privacy. Secondly, perception of risk led to concerns related to improper access. When risk perceptions were high, individuals expressed high concerns regarding improper access to their health data. This included physical risks in the form of access by employees such as receptionists, loss of data, and loss of digital devices. Some interviewees

expressed concerns about unauthorised access to data stored by both health professionals and technology vendors from external sources such as hackers. In addition, interviewees discussed their fears surrounding access by third parties such as insurance companies. Perceived risk also influenced concerns regarding control. Interviewees with high perceptions of risk, felt they lacked control over how their data may be used by technology vendors.

- **Summary Point: Perceived Risks associated with disclosing health data to health professionals and technology vendors, foster higher concerns regarding unauthorised secondary use, improper access to data, and lack of control.**

#### ***6.4.6 Perceived Sensitivity***

The interviews sought to understand interviewees' views on the sensitivity of health data, and to explore the relationship between perceived sensitivity and HIPC.

##### ***6.4.6.1 Overview of Perceived Sensitivity***

The majority of interviewees viewed health information as sensitive in the broad sense. These interviewees made comments such as 'It's very sensitive to me' (P25), and 'It's more sensitive than other types of information (P46). Interviewees offered a number of reasons for this view. Firstly, many interviewees described health data as personal and unique to them as a person. They felt more protective of this information, as health data is part of the individual in a sense, whereas other information types merely relate to individuals or their lives. This view was expressed both by individuals with illnesses and individuals who described themselves as healthy. An example of this view is illustrated below. This interviewee believes health data is inherent to an individual.

*It's so personal. I hate the idea of being labelled because I've an illness. I don't think my diabetic status should be known by anyone. Health information makes up a person.*

*P5, Masters Student, Ireland.*

Secondly many interviewees described their health data as highly sensitive, as it could have negative repercussions on their lives if used in certain ways. They believed that this data could

be misused by insurance companies and employers, or could harm their future employment opportunities. The below quote illustrates some of these fears.

*There could be stuff you're embarrassed about or stuff that could be used against you, by your employer, it might sway their decisions against you.*

*P22, Administrative Employee, Ireland.*

Thirdly, interviewees discussed fears that individuals such as employers, friends, or family could misinterpret their health data. These interviewees believed medical training was required to fully understand health data, and misinterpretation could lead to the negative outcomes discussed above. Some interviewees recounted instances where they or their family members experienced differential treatment due to inaccurate views or misinformed opinions on health conditions. A small number of interviewees expressed the view that health information was not more sensitive than other data. Interviewees offered three reasons to justify this view. Firstly, some noted that as they were of good health, there were no negative uses for their health data. Secondly, some interviewees believed that because they were an everyday citizen, there would be no interest in their health data. Lastly, two interviewees stated they had 'nothing to hide' and thus didn't view their health data as sensitive.

Many interviewees viewed certain types of health data as more sensitive than others. Mental health, eating disorders, reproductive or fertility data, sexual health, addiction, and domestic abuse were all described as extremely sensitive by a number of interviewees. Chronic illness, gastro issues, and test results were also described as particularly sensitive. A common trend among interviewees was the desire to keep sensitive data private. These interviewees explicitly stated that they did not want this information to be shared, and that only necessary parties should have access. For example, the interviewee below suffered from an eating disorder. She expresses a strong desire to limit sharing of this data.

*I wouldn't want my weight shared with many people, if any. When I was pregnant, because I have had problems with eating before I didn't want to know my weight, I spoke to my doctors and said I didn't want it in my chart. For me that's sensitive and I wouldn't want it shared with anyone.*

*P8, I.T. Professional, Ireland.*

#### 6.4.6.2 *Perceived Sensitivity and HIPC*

There was a strong link between sensitivity perceptions and broad privacy concerns. Many interviewees who described themselves as ‘healthy’ discussed circumstances when they would be concerned for their health privacy. Some of these circumstances were conditional. For example, some interviewees noted they would want their data to remain private *if* they had certain conditions like chronic illness or mental health issues. Other circumstances were concrete. For instance, some interviewees noted they *will* be more concerned regarding their health data privacy, when they have children, or as they get older.

Three dimensions of HIPC were mentioned by interviewees when discussing sensitivity. Firstly, many interviews expressed concern regarding unauthorised secondary use. The majority of interviewees were opposed to their health data being used for secondary purposes. Some interviewees assumed that secondary use did not occur, believing that health data was only used by health organisations to treat patients, and by technology vendors to provide an application. Others acknowledged that secondary use may occur, and stated they would not be happy with any additional uses. Interviewees were extremely concerned about subsequent use without their permission. When interviewees believed their health data was used without their permission, they expressed high privacy concerns and concern regarding possible outcomes.

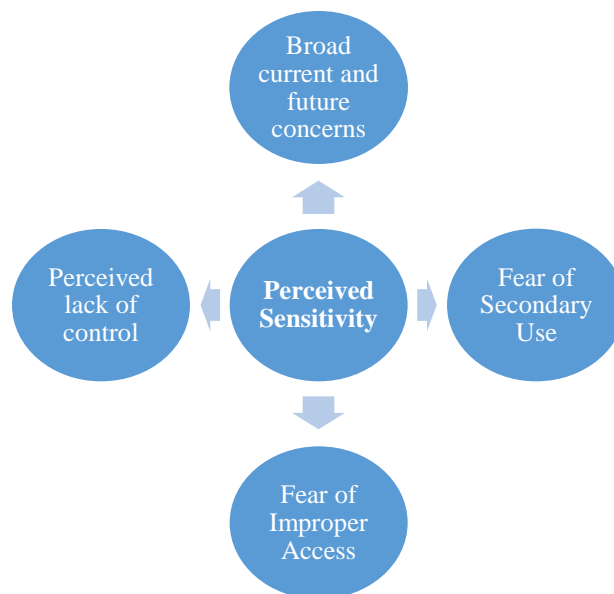
The second dimension discussed related to improper access to health data. Many interviewees expressed the desire to limit access to their health data to necessary parties. When interviewees believed unauthorised individuals or third parties could access their health data, they were extremely concerned about such access, and the potential repercussions. Many interviewees were willing to share data with other health professionals and parties that might need access such as insurance companies, but expressed strong opposition to certain parties having access such as employers. Again the dominant reasons for limiting access related to the personal nature of health data, and the potential for sensitive data to be misinterpreted and used in negative ways.

The third dimension of HIPC related to control. Many interviewees expressed a strong desire to have some control over their health data. They desired the ability to limit access to data, and limit

uses of health data. Many interviewees believed they lacked control at present. Some felt their control was limited to deciding what they disclosed in mHealth technologies, and what health professional they visited, but after data was disclosed they had no control. This lack of control caused concern regarding unauthorised secondary use and improper access to health data.

- **Summary Point: Health data is sensitive due to its personal nature, potential negative outcomes of misuse or access, and potential misinterpretation. Perceived sensitivity fosters broad current and future concerns for privacy, and heightens concerns regarding unauthorised secondary use, improper access, and control.**

**Figure 6.6 Perceived Sensitivity and HIPC**



## 6.5 Examining Citizens' HIPC

The interviews aimed to develop a deeper understanding of citizens' health information privacy concerns (HIPC). Many interviewees expressed a strong desire for privacy through statements such as 'I place utmost value on the privacy of my health information' (P7). However, some interviewees did not express high privacy concerns at present for reasons including: assuming this data was private, trust in health professionals, good health, and the belief that no negative repercussions existed. Some interviewees did not use mHealth technologies and thus did not believe their privacy was at risk. Each dimension of HIPC is discussed in this section.

### 6.5.1 Collection

Collection relates to concerns that copious volumes of health data are collected and electronically stored. Many interviewees expressed low concerns regarding health professionals' collection of data, as this was part of the healthcare process. There was a consensus that health professionals needed this data to administer treatment. Interviewees were willing to provide limitless data to their primary care doctor, as they believed all data was relevant to the doctor providing their overall care. For other health professionals such as specialists, some interviewees were only willing to provide relevant data. For technology companies, individuals were less willing to provide detailed health data. While some might provide fitness data, the majority of interviewees would not disclose health data to technology vendors. The reasons included mistrust in technology companies, and the perceived irrelevance of health data to these companies. Interviewees noted that requests for health data from technology companies would cause concern. They felt that such requests would be excessive and for the benefit of the company, whereas requests from health professionals were for the patient's benefit. The quote below illustrates this comparison.

*My dentist or my eye doctor, when they ask questions that bugs me because I came for this specific health issue, but my primary care doctor I wouldn't mind him asking about other issues. I have a relationship with him. He provides my overall care so other issues are relevant. I would feel invaded if technology companies requested it. I wouldn't give it.*

*P41, Administrative Employee, USA.*

In terms of health professionals, many interviewees acknowledged it was in their interest to maintain an electronic record, but some felt that electronic storage would lead to new risks to their privacy. Interviewees expressed concerns about the storage of their health data by technology companies.

- **Summary Point: Interviewees express low concerns when their data is requested from health professionals, whereas requests from technology companies cause concern due to the lack of a pre-existing relationship, mistrust, and the irrelevance of data requests.**

### 6.5.2 *Unauthorised Secondary Use*

Unauthorised secondary use relates to individuals' concerns that their health data is collected for one purpose and used for additional purposes without their permission. In terms of health professionals, several interviewees expressed low concerns regarding unauthorised secondary use, as they believed their health data was only used to treat them and 'stored away' at all other times. Many interviewees who adopted this view were older, but some younger interviewees also held this assumption. Some interviewees acknowledged that health data *could* be used for secondary purposes but expressed their 'hope' that this was not the case. However, the majority of interviewees either expressed concerns regarding current or future unauthorised secondary use. For data disclosed to health professionals, the main concerns related to sharing data and the use of data in research without permission. A number of interviewees discussed receiving communications from unknown third parties regarding health issues, which caused concern. These individuals also expressed concerns regarding future secondary uses. Interviewees also expressed concerns regarding the potential sharing of their health data with other parties such as law enforcement authorities as illustrated in the quote below.

*Let's say I go to a doctor and I might be experiencing short term depression. I own guns and you're worried he might report you to authorities because you might be a risk. I am worried where that goes.*

*P35, Naval Professional, USA.*

The disparity between health professionals and technology companies was evident. Some interviewees expressed low concerns regarding secondary use by technology companies as (1) they would never disclose health data to technology companies and thus there was no risk, or (2) they would only disclose data which was not sensitive. The majority of interviewees believed technology companies would use their health data in the pursuit of financial goals. As many interviewees believe that health data should only be used to treat the patient, or in research (with consent) to help others, these commercial uses conflict with the benevolent uses individuals are willing to consent to. Interviewees also believed that there was no course of redress if technology companies misused their health data, as illustrated below.



*With a doctor there is concern but it wouldn't be too high. A hospital can be held accountable but apps if they sell data or get hacked they've less accountability so I worry that my information would be misused.*

*Financial Professional, P6, Ireland.*

- **Summary Point: Concern for unauthorised secondary use was low among individuals who did not use mHealth technologies and those who assumed their data was only used to treat them. When individuals were aware of the uses for health data, or had previously experienced secondary use, they expressed high concerns. Irrespective of current concern, there was a common view that health data should not be used for secondary purposes without permission. Interviewees were willing to consent to altruistic secondary usage for research, but were staunchly opposed to use for profit.**

### ***6.5.3 Improper Access***

Improper access pertains to concerns that one's health data could be accessed by unauthorised parties. A small number of interviewees expressed low concerns regarding improper access. These interviewees assumed their health data was private, and felt that no third parties would have an interest in their data. However, the majority of interviewees expressed concerns about potential improper access to their health data. In terms of health professionals, a number of interviewees were concerned about access by individuals working in health organisations, who may not require access. This access was viewed as unnecessary and excessive, as these individuals were not 'qualified to interpret' this information. Potential access by third parties also caused concern. Interviewees discussed their fears that data might be accessed by hackers, employers, insurance companies, pharmaceutical companies, and marketing companies. Many interviewees were strongly opposed to access by external parties due to irrelevance, and the potential repercussions stemming from such access. The large majority of interviewees were against access to health data by employers. They believed this data was irrelevant to the employer and could hinder their promotion or future employment opportunities. Many interviewees acknowledged that insurance companies require access to some data, but there was a shared belief that this access should be limited to necessary data. Interviewees expressed strong opposition to

access by governments believing this could have many negative outcomes. Some interviewees acknowledged that governments may require anonymous macro-level data for statistical purposes. Many interviewees expressed concern regarding access by pharmaceutical companies. The majority of interviewees disagreed with the commercial aims and lack of transparency surrounding these companies. Lastly, the majority of interviewees were against access to health data by marketing companies, again due to their commercial motivations.

While the majority of interviewees believed that access to their health data by external parties should be strictly limited, there were differences in the level of concern individuals expressed about this access at present. Many stated they would be extremely concerned *if* this access occurred, while others were currently concerned that such access *does* occur. In terms of health professionals, individuals believed physical non-malicious access by an individual was more likely to occur than intended access by an organisation. For technology companies, interviewees expressed higher concerns regarding the sale of data to insurance and pharmaceutical companies, which they were strongly opposed to. Many interviewees were less willing to provide technology vendors with their data, as a means of protecting their privacy. However, some interviewees felt the potential personal repercussions stemming from improper access to health data stored by health professionals was greater, as this data is evidence based. In the quote below the interviewee notes that data stored by health professionals is accurate and factual, and if accessed by third parties could have real repercussions from an insurance, employment, and social standpoint.

*If you Google 'gangrene' somebody has got that information and they can link it back to you. When the ads pop up advertising cures, it's already sold. But it's not detailed and it's not reality, it doesn't mean I had gangrene. Whereas if the doctor records he has gangrene, and that's sold that's different.*

*P25, Technology Professional, USA.*

- **Summary Point: Many individuals express low to medium concerns at present due to high trust and assumptions of privacy. However, interviewees express strong opposition to irrelevant or excessive access to their health data. When individuals believe improper access is possible, they express higher concerns.**

#### **6.5.4 Errors**

The Errors dimension relates to concerns that organisations do not have the ability to identify and correct errors in individuals' health data. Concerns regarding errors were not at the forefront of many interviewees' minds, but some did express concerns that incorrect data could travel and lead to incorrect diagnoses or result in negative repercussions. Interviewees believed that errors may occur in paper and electronic records, and stressed the need to trust that health organisations had the measures in place to catch these errors. Many interviewees were not concerned with errors in data collected by health technologies, as they disclosed this data themselves. A small number of interviewees acknowledged the potential misinterpretation of their health-related information searches again discussing the gap between searching for health information and reality. They noted that technology companies may profile them based on inaccurate data.

- **Summary Point: Interviewees expressed concern regarding the possible spread of inaccurate data in ways which could have negative repercussions.**

#### **6.5.5 Control**

Control pertains to individuals' concerns that they cannot exercise control over their health data. With regards to health professionals, the majority of individuals stated they currently had little to no control over their health data. A small number of interviewees stated that they had some control as they could request access to their health record, and they assumed their consent would be sought prior to secondary use of their data. Among these interviewees, some noted that this control was often challenging to exercise, discussing the difficulties they faced in gaining access to their records, despite their 'right to access'. The majority of interviewees expressed a desire for greater control over their health data due to the personal nature of this data, and the belief that this data belonged to the individual. In addition, interviewees' current lack of control often represented their strongest privacy concern. For example, the interviewee below believes he should have this control and awareness.

*It's the lack of control that concerns me a lot. It's my information I should be informed and my permission should be sought.*

*P7, Financial Professional, Ireland.*

Interviewees expressed a strong desire for control over (1) what parties could access their health data and (2) how their data could be used. The level of desired control varied slightly among interviewees with some expressing the desire to consent prior to each use of their data, and each party who desired access. Others sought the ability to limit access to certain parties, and to ban some uses of their data such as commercial uses. In addition, some interviewees desired access to their data to correct errors. Offering some level of control has the potential to appease privacy concerns as illustrated below.

*Some control can really help reduce fears especially with information as personal as health data.*

*P20, Business Professional, Ireland.*

In terms of technology companies, the majority of individuals believed they had no control over how their health data is used. A number of interviewees stated that they could control what mHealth technologies they use, and what data they disclose, but upon disclosure all control was relinquished. Again, for many interviewees, increased control could reduce concerns. The desired control included allowing individuals to decide what parties their data could be shared with, and what they could use this data for. For other interviewees, such control did not seem possible and they stated they would protect their privacy by abstaining from mHealth technologies or limiting disclosure to non-sensitive data.

- **Summary Point: Interviewees believe they lack control over their health data. They desire greater control to determine how their health data is used and shared by health professionals and technology companies. Increasing perceived control can reduce HIPC.**

#### **6.5.6 Awareness**

Awareness relates to individuals' concerns that they lack awareness of how their health data is protected and used. In terms of health professionals, the majority of interviewees felt they lacked

awareness. A small number of U.S. interviewees stated they were aware how health professionals could use their health data and how they were required to protect it under HIPAA. The majority of interviewees however felt completely unaware of the protections afforded to their health data, and how it was used. For many interviewees, this lack of awareness led to high concerns for privacy as they felt their data could be used without their knowledge or permission. There was a strong connection between awareness and several other dimensions of HIPC. For example, interviewees expressed a desire to be aware of any secondary usage and all access requests. Interviewees felt they *should* be aware, and if they were fully aware, they could then make informed decisions to consent or refuse the request. Interviewees also stated that awareness could reduce their privacy concerns making statements such as “transparency could help with concerns”, and “awareness would be a great comfort”.

The sense of unawareness deepened when interviewees discussed technology vendors. Many had no awareness of how these companies used their data. A small number stated they had only disclosed non-sensitive data and thus didn’t believe they were at risk to severe repercussions. For others, the lack of awareness increased their privacy concerns and reduced their willingness to disclose data to technology vendors. They believed that technology vendors *should inform* users of how their health data is used. While they acknowledged that a lack of awareness is an inherent problem in today’s technology driven world, they felt health data was more personal and sensitive. Thus, they believed that technology vendors had a responsibility to ensure they were fully aware. Some interviewees noted that privacy policies are inefficient as they cannot understand the legal language. To improve awareness, interviewees felt they should be informed in layman’s terms.

- **Summary Point: Lack of awareness can lead to false assumptions of privacy. More commonly, lack of awareness generates high concerns regarding secondary use, improper access, and lack of control. Interviewees believe they should be informed and educated. Awareness and transparency regarding the uses of information, coupled with increased perceived control has potential to appease the majority of interviewees’ concerns.**

## **6.6 HIT Acceptance and Adoption**

Interviews aimed to understand citizens' adoption intentions towards EHRs and mHealth solutions on a deeper level, and to untangle the relationships between perceived benefits, HIPC, and adoption. All Irish interviewees, and American interviewees who stated their healthcare provider did not currently use EHRs, were asked if they would opt-in to an EHR. All interviewees in both countries were asked if they would use mHealth technologies.

Many interviewees expressed positive intentions to opt-in to an EHR. Interviewees discussed a number of stipulations which would have to be met prior to their acceptance. Firstly, interviewees expressed a desire to be fully educated on all aspects of an EHR including what data would be included, what parties would have access, and how their data would be protected. Suggested education methods included leaflets, media campaigns, and information sessions with health professionals. Secondly, many interviewees expressed the desire to limit access, noting that health professionals should only have access to the data they need to treat them and not the complete record. Interviewees were in support of access in emergency situations and by third parties such as insurance companies in some instances. Thirdly, individuals expressed fears regarding excessive use of their data for secondary purposes. Many believed their data should only be used in the course of treatment. Fourthly, interviewees expressed a strong desire for control. This control included the ability to opt-in prior to implementation, to decide what parties could access their data, and the ability to limit subsequent uses. Lastly, a number of interviewees highlighted the importance of securing the data.

Intentions to adopt three mHealth solutions were explored. Firstly, many interviewees noted they would try an mHealth application. The most popular applications were fitness and sleep tracking applications. Secondly, a number of interviewees noted they would use wearable fitness devices. These interviewees discussed barriers preventing their adoption such as high costs, time investment, or lack of fitness motivation. Many interviewees with previous experience using wearable devices planned to continue use, as they found them beneficial. Lastly, many

interviewees were unwilling to use Personal Health Records as they felt the information required was too excessive, they feared data misuse, and did not see the benefit of maintaining a personal record. Some interviewees would not use any mHealth technologies, due to lack of interest, or privacy concerns.

### ***6.6.1 Perceived Benefits and Adoption***

All interviewees believed there were some benefits associated with the implementation of EHRs. These benefits included improved diagnoses, reduction in redundant tests, access to patient information in emergency situations, reduction of the burden on patients' memory, improved efficiency, reduced administration, elimination of errors, environmental benefits, and enabling patient access to their data. Interviewees believed mHealth solutions could lead to improved awareness of one's health, improved ability to monitor trends, empowerment of individuals with health conditions, and encouragement of healthy behaviours. Some interviewees acknowledged the benefit of tracking one's health but were not willing to use a technological device to do so.

Perceived benefits of EHRs and mHealth solutions influenced interviewees' adoption intentions. In both cases, when interviewees believed the benefits were extensive, they expressed higher intentions to adopt. However, the link between perceived benefits and intentions was not simple. In terms of EHRs, individuals noted that many of the benefits must be balanced with patient privacy. For example, when discussing the benefit of access to patient data, many interviewees expressed a desire for access to be limited to 'necessary access' by 'relevant health professionals'. If interviewees believed the needs of the patient would be considered, they expressed positive views towards EHRs. With regards to mHealth technologies, many interviewees expressed positive intentions due to the perceived benefits. Interviewees who were currently using mHealth applications and wearable devices, expressed intentions to continue use if (1) they believed they were currently benefiting from use, and (2) the benefits were relevant and important to them. This is evidenced in the quote below. The interviewee plans to continue using an mHealth application and tracking device as they help her achieve important fitness goals.

*I will continue to use MyFitnessPal. It keeps me aware and helps me manage my diet. I will continue to monitor my exercise too because it keeps me focused to ensure I hit the goals I need.*

*P27, Mature Student, USA.*

### **6.6.2 HIPC and Adoption**

Several dimensions of HIPC negatively influenced interviewees' intentions to accept EHRs. Firstly, when interviewees expressed strong concerns regarding secondary use, their positive adoption intentions weakened. These interviewees felt the digitisation of health data would enable secondary usage without their knowledge. Secondly, fears of improper access reduced intentions. Many interviewees feared that unauthorised individuals and third parties might access their records. Thirdly, when individuals believed they would have no control over the use of their data and access to their health data, their intentions reduced. Fourthly, lack of awareness regarding how their data might be used and protected also reduced adoption intentions. Acceptance could be increased by addressing concerns. Interviewees noted they would be more willing to opt-in if they were fully aware and informed, and if they could control use and access.

For mHealth technologies which required little data disclosure, HIPC did not have a strong influence on adoption. Individuals were also less concerned about the disclosure of 'non-sensitive' health data. When mHealth technologies require sensitive health data, or the disclosure of copious volumes of health data, HIPC can influence adoption. When interviewees believed sensitive health data would be used for secondary purposes, they expressed negative intentions towards mHealth technologies. Additionally, when interviewees believed unauthorised parties may seek access to their health data, they were less willing to disclose. Lastly, interviewees expressed strong concerns regarding their inability to control health data disclosed to technology vendors. The quote below supports the link between HIPC and mHealth adoption.

*If a technology company required me to add a lot of information to join, I wouldn't. If they make it an option that would be fine but anything that's invasive, I'm going to be cautious.*

*P34, Education, USA.*

The interviews support the Privacy Calculus theory, as both perceived benefits and HIPC can influence individuals' adoption intentions. In terms of EHRs, perceived benefits have a strong



influence on acceptance. HIPC can reduce individuals' acceptance, but often the potential lifesaving benefits of EHRs outweigh individuals' concern for their own privacy. The role of the Privacy Calculus was summed up by one interviewee (P7) who stated that on a day to day basis, privacy was of paramount importance and should be protected, but in life threatening situations, the benefits of EHRs outweigh the importance of privacy. This shows that both HIPC and benefits are important, and their level of importance changes dependent on the situation. In terms of mHealth solutions, many interviewees would adopt to attain utilitarian benefits such as improved fitness and hedonic benefits such as enjoyment. However, in order to continue use, individuals must believe they are realising these benefits. HIPC can reduce individuals' intentions to adopt mHealth. Furthermore, individuals may cease use if they are concerned for their privacy, or if the application requests sensitive data.

- **Summary Point: Perceived benefits associated with EHRs increase adoption intentions especially when the benefits are potentially lifesaving. However, these benefits must be balanced with patients' privacy concerns. Perceived utilitarian and hedonic benefits of mHealth increase adoption intentions, but continued use is subject to the realisation and sustained relevance of these perceived benefits. HIPC influences individuals' choice of mHealth solution, volume and type of data disclosed, and decisions to continue or cease use.**

## **6.7 Additional Factors**

This section reviews three additional factors discussed in the interviews.

### **6.7.1 *Perceived Ownership***

Following the exploratory interviews, perceived ownership was added to the research framework. The interviews explored the link between perceived ownership and HIPC. Three broad views of ownership were discussed by interviewees. Firstly, many interviewees believed they own their health data. These interviewees made statements such as 'it's mine,' and 'I own it'. Interviewees

adopting this personal ownership view described health data as personal, sensitive, and unique to them. Secondly, some interviewees described a dual ownership, shared between them and their health provider. The weighting of this shared ownership varied slightly. Some believed they had a greater right to ownership, and health professionals were merely custodians or guardians of data who could use it for the patient's benefit. Others believed health professionals were co-creators of the data and thus equal co-owners. Thirdly, a small number of interviewees expressed the view that their health data belonged to the health professional who created the data. These interviewees expressed a desire for personal ownership. The three views are illustrated in the quotes below.

View 1 (Personal Ownership): *Me. Just me. Because it's my health.*

*P21, Research, Ireland.*

View 2 (Shared Ownership): *You have the most ownership but the health system has a degree of ownership, they're contributing to it. You would deserve it more than the health system.*

*P22, Administrative Employee, Ireland.*

View 3 (Lack of Ownership): *I'm supposed to, but the corporation that runs the doctor's office actually owns it.*

*P35, Naval Professional, USA.*

The link between HIPC and perceived ownership is noted. Interviewees who expressed the personal ownership view expressed a high desire for privacy and high concerns regarding unauthorised secondary use and improper access. Many of these interviewees were older and possibly unaware of how health data could travel. Thus they not only desired ownership of their health data, they assumed they had such ownership. Among the interviewees expressing the second view, many expressed a desire for privacy and felt health professionals had a responsibility to protect their health data. Individuals expressing the third view also had high privacy concerns in general, and expressed high concerns regarding their inability to control their health data.

- **Summary Point: Perceived Ownership influences health privacy concerns in general, as well as specific dimensions of concern.**

### **6.7.2 *Health Locus of Control***

Another recurring theme in the interviews pertained to individuals' perception of who was responsible for their health. This is described as health locus of control (HLOC). Individuals with an internal HLOC believe they can control their health, whereas individuals with an external HLOC believe health professionals are responsible for their health, or health is determined by luck (Rongen, Robroek, and Burdorf, 2014). A number of interviewees discussed the idea that they had some control over their health. These individuals expressed the need to be proactive in questioning diagnoses and prescriptions, in selecting health professionals, and to be aware of one's rights. This is described as high internal HLOC. Some interviewees believed health professionals were responsible for ensuring they were of good health. One interviewee expressed the view that health was determined by luck. These interviewees have high external HLOC.

Interviewees with high internal HLOC expressed a strong desire for health privacy and had concerns regarding lack of awareness and control. Playing an active role in their healthcare could potentially provide these interviewees with some level of comfort. For example, if they could question their health professional to improve their awareness of how their health data was protected, concerns regarding lack of awareness could be appeased. Some individuals would not use mHealth solutions, due to concern, even if they expressed high internal HLOC. They noted they could monitor their health offline (P23) or engage in healthy behaviours. However, for others, mHealth solutions provided them with the ability to monitor their health. This ties into the Privacy Calculus. Individuals with internal HLOC believe they are largely responsible for their health. Thus the ability to track one's health is very beneficial and may outweigh the risks.

- **Summary Point: High Internal HLOC can increase individuals' HIPC and influence their adoption intentions.**

### **6.7.3 *Privacy Protective Behaviours***

Another theme which was evident throughout the interviews pertained to the behaviours individuals utilise to protect their privacy. These behaviours are described as privacy-protective

behaviours, and were categorised into three groups by Son and Kim (2008): information provisions, private actions, and public actions. Many interviewees engaged in information provisions including disclosing minimal or non-sensitive data, falsifying data, and refusing to disclose data. Interviewees discussed previous occasions when they had engaged in these behaviours and hypothetical situations when they would do so. Many interviewees stated if an mHealth application requested extensive amounts of health data or sensitive data, they would either withhold or falsify data. Some interviewees had previously deleted mHealth applications which requested excessive volumes of data.

There was a clear link between HIPC and privacy-protective behaviours. A number of interviewees discussed the practices they currently engage in to protect their privacy including technical measures such as changing passwords (P3), disabling tracking (P44), and deleting cookies. These interviewees felt they were 'safer' and 'more careful' than others online. As a result, many of these interviewees expressed low current concerns for their health data privacy, as they believed these behaviours protected their data. In addition, some interviewees recalled specific instances where they had engaged in these behaviours to protect their health data.

- **Summary Point: Interviewees engage in privacy-protective behaviours including falsifying data, withholding data, and refusing to use a technology. These behaviours stem from concerns regarding secondary use, lack of control and improper access.**

## **6.8 Integrated Findings**

This section integrates the quantitative and qualitative findings to derive a conclusion for each key relationship (Teddlie and Tashakkori, 2009). Data were integrated using a triangulation protocol, which involves combining findings from two methods to develop a more comprehensive picture (O'Cathain *et al.*, 2010). Each key construct was reviewed to determine if the findings from both methods were complementary, convergent, dissonant, or silent. Complementary findings offer similar insights. Convergent findings provide a better understanding when combined. Dissonance occurs when findings offer differing views. Silence occurs when a

construct was only explored in one method. Integration required two steps. Firstly, the quantitative and qualitative findings were integrated in a triangulation protocol. Secondly, the integrated findings were leveraged to develop meta-inferences or deep explanations of the constructs of interest (Venkatesh *et al.*, 2013).

Integrated data must meet three validity criteria: integrative efficacy, integrative correspondence, and inference transferability (Venkatesh *et al.*, 2013). To achieve integrative efficacy, quantitative and qualitative findings must be consistently integrated to develop greater insights. Integrative efficacy was achieved by following the triangulation protocol outlined by O’Cathain *et al.*, (2010), to consistently weave quantitative and qualitative findings together and produce a multi-perspective understanding of each construct (Teddlie and Tashakkori, 2009). Integrative correspondence requires that the findings satisfy the study’s aims and purpose. This study aimed to develop a more comprehensive understanding of how citizens’ HIPC influence their intentions to adopt health ICTs. Due to the nascence of health technologies, the dearth of existing health privacy research, and the complex nature of privacy, mixed methods was necessary to test and explain the hypothesised relationships. This purpose is described as the completeness approach (Venkatesh *et al.*, 2013). To ensure the study’s aim and purpose were met, the relationships were quantitatively examined, and explained using qualitative data. The data was then integrated to develop meta-inferences which improve our understanding of privacy in the health context. Thus integrative correspondence was achieved by following the study’s purpose throughout the research design, data collection, and data analysis. Inference transferability refers to the degree to which meta-inferences can be transferred to other contexts. As this study was conducted in two countries, across a broad range of citizens, the meta-inferences developed are pertinent to many citizens in these countries, and could be extended in further research.

The main findings from the quantitative and qualitative data are integrated in table 6.2. The results for the hypothesised relationships in model 1 and 2 are outlined, along with the core insights gained from interviews. Based on these findings, several meta-inferences are developed.

**Table 6.2 Integrated Findings**

Relationship	Quantitative Findings		Qualitative Findings	Integration	Conclusion
	Model 1	Model 2			
Gender → HIPC (Females greater HIPC)	x	x*	Females: blind assumption of health privacy. Males: greater understanding of risks leads to concerns regarding possible secondary usage and access. All interviewees had a desire for health privacy.	Complementary	Males had a greater comprehension of the risks to health data and expressed higher HIPC. Many females had an assumption of privacy and thus lower concerns.
Age → HIPC (+)	✓	✓	Older: Lower understanding of risks coupled with an assumption of privacy often reduced HIPC, however they expressed a strong desire for privacy.	Complementary	Older individuals express higher desire for privacy and higher HIPC, but when privacy is assumed, HIPC reduces.
Media Coverage → HIPC (+)	✓	✓	Specific stories increase HIPC. Familiarity with injured parties increases HIPC. Comprehension of personal risks increases HIPC. Greater issue involvement increases HIPC.	Convergence	Privacy media coverage can increase HIPC. This influence is strengthened by specificity, familiarity, comprehension, and issue involvement.
Sensitivity → HIPC (+)	✓	✓	Interviewees felt their health data was sensitive due its personal nature. Interviewees expressed concerns regarding unauthorised secondary use, control, and improper access to health data Current, conditional, and future concerns for health privacy were expressed.	Convergence	Perception of sensitivity can increase HIPC especially regarding unauthorised secondary use, access, and control.
Healthcare Need → HIPC (+)	✓	✓	Individuals with a greater need for healthcare services expressed high concerns in the broad & specific sense of HIPC dimensions, and concerns regarding negative outcomes.	Complementary	Individuals with greater healthcare needs have higher HIPC and fear of negative repercussions.

Relationship	Quantitative Findings		Qualitative Findings	Integration	Conclusion
	Model 1	Model 2			
Health Status → HIPC (+)	x	x*	Poor health = higher HIPC except when there are no perceived negative outcomes, or privacy is assumed.	Dissonance	The role of poor health calls for further exploration.
Health Information Seeking (INF) → HIPC (-)	✓	x	Interviewees expressed varied views on the risks associated with seeking health data online Low risk: frequent online searches, sense of anonymity and control. High risk: concern for secondary use of search data, limit frequency and content of searches.	Complementary	Qualitative findings support the potential for INF to reduce HIPC. Findings show concern for secondary use can reduce INF.
Risk → HIPC (+)	✓	✓	Technology vendors: risks relate to commercial motives and intentional misuse. Health professionals: risks relate to incompetence to protect data. High perceived risks lead to concerns for secondary use, improper access, and control.	Convergence	High perception of risks lead to high privacy concerns especially regarding secondary use, access and control.
Trust → HIPC (-)	x*	x	High trust in health professionals' motives with data, lower trust in competence to protect data Lower trust in health workers, and health organisations: high concerns for access & secondary use. Low trust in motives of technology vendors: fears of secondary use, access & control. High trust can partially alleviate concerns of secondary use and access; many still have concerns regarding lack of control & awareness	Dissonance	Quan. Findings: trust in health prof. increases HIPC, Qual. Findings suggest that this positive influence could relate to low trust in health & technology organisations. Qual findings show strong links between trust and HIPC.
HIPC → Intention (-)	✓	x	HIPC can influence intentions. Individuals will adopt mHealth if they are not required to disclose any data, or will disclose non-sensitive data. Concern of improper access, lack of control, awareness & secondary use can influence subsequent use and result in falsification or withholding of data. Interviewees would adopt if they were aware and had greater control over use and access.	Convergence	Quan: mixed findings. Qual shows this relationship is not simple, & individuals may adopt but withhold or falsify data, or disclose non-sensitive data. Some will adopt if they have control and awareness.

Relationship	Quantitative Findings		Qualitative Findings	Integration	Conclusion	
	Model 1	Model 2				
Benefits → Intention (+)		✓	✓	Hedonic benefits can have a strong influence on intention to adopt mHealth, this influence on continued use is weaker. Lifesaving benefits have a strong influence on willingness to opt-in to an EHR,	Complementary	Perceived benefits can have a strong influence on intentions to adopt, especially if these benefits are substantial.
Privacy Invasion moderates HIPC → Intention	Personal	✓	✗	The influence of privacy invasion experience on HIPC depends on the number of invasions, level of surprise, severity of invasion, sensitivity of data, interviewees’ assumption of safety, and risk discounting techniques utilised by the interviewee.	Convergence	Quan: mixed. Qual: Privacy invasion has strong impact when the invasion is severe, relates to sensitive data, & vulnerability is high.
	Health	✓	✗			
Health Condition moderates HIPC → Intention	Chronic Illness	✓	✗	Chronic illness: tangible benefits more important than concerns regarding potential ‘misuse’. Sensitive illness: desire higher privacy and express higher current concerns, would not disclose any sensitive data on mHealth but may adopt solutions related to non-sensitive issues	Dissonance	Chronic illness: link between HIPC & INT is weaker due to benefits. Sensitive: May be willing to adopt ‘non-sensitive’ mHealth solutions.
	Sensitive Illness	✗	✗			
Perceived Ownership→ HIPC (+)		✓	✓	Perceived ownership linked to high desire for privacy, and high concerns regarding lack of control and awareness.	Convergence	Perceived ownership leads to concerns based on lack of control & awareness
Legislation → HIPC (-)		✗	✓	Awareness of legislation created a sense of protection and reduced HIPC.	Dissonance	Future research should explore actual knowledge and efficacy of legislation.
Health locus of control		-	-	Internal HLOC: Engage in behaviours to protect privacy & increase perceived control but high desire to engage in healthy behaviours, & high perceptions of benefits.	Silence	Need to further explore the influence of locus of control over health and health privacy on HIPC & adoption
Privacy-Protective Behaviours		-	-	Protective behaviours such as falsifying data, disclosing non-sensitive data increased perceived control & decreased HIPC.	Silence	Privacy behaviours may represent a missing link in the HIPC-INT relationship.

Note: ✓ Supported, × not supported, ×\* significant in opposite direction



### ***6.8.1 Development of Meta-Inferences***

A number of meta-inferences are developed from the integrated findings outlined above. The first meta-inference pertains to the assumption of privacy. When individuals assumed their health data was private, they expressed lower concerns. This was evident among females and among older participants aged 50 and above, who expressed a strong desire for privacy but assumed their health was private. Secondly, understanding of the risks to one's health data influenced privacy concerns. For instance, many male participants were cognizant of the risks and possible uses for health data, and thus expressed higher concerns. In contrast, many older respondents had a lower understanding of risks and expressed lower concerns, despite their desire for privacy. The third meta-inference provides support for the Information Boundary Theory, as individuals expressed higher concerns for the privacy of health data they viewed as sensitive. Individuals considered the risks to this data more carefully, expressed strong opposition to the sharing of this data, and feared negative outcomes stemming from misuse of this data.

The next set of meta-inferences support the Protection Motivation Theory (PMT). Individuals' awareness of media coverage influenced their HIPC, as it represented the breadth and severity of risks facing their health data. Individuals also reflected on their privacy invasion experiences to determine their current vulnerability. Lastly, individuals reflected on their perception of whether these risks will become a reality. In terms of coping appraisal, high trust in the benevolence, integrity, and competence of the relevant party (health professionals, or health technology companies) can appease individuals' perception of risk. In the absence of trust, individuals may engage in privacy-protective behaviours. The importance of risk and trust deepens for sensitive data, as individuals seek to protect this data.

The final set of meta-inferences pertain to the Privacy Calculus theory. This study shows that perceived benefits can influence intentions, but the type of benefit determines how long this influence will be sustained. Individuals' privacy concerns can also influence acceptance of EHRs, and adoption of mHealth solutions. The meta-inferences are summarised in Table 6.3 below.

**Table 6.3 Summary of Meta-Inferences**

<b>Meta-Inference</b>		<b>Supporting Constructs</b>	<b>Theoretical support</b>
<b>1.</b>	<i>Assumptions of privacy reduce HIPC.</i>	Gender Age	
<b>2.</b>	<i>Greater risk awareness can increase HIPC.</i>	Gender Age	
<b>3.</b>	<i>Individuals express high privacy concerns regarding health data they view as sensitive. These concerns include fears of unauthorised secondary use and improper access. Individuals express higher desire for control over sensitive data and desire to be aware of how this data is protected and used.</i>	Perceived Sensitivity	Information Boundary Theory
<b>4.</b>	<i>When individuals believe the risks to their health data are extensive, feel personally vulnerable, and believe these risks are likely to occur, they express high HIPC.</i>	Media Coverage Privacy Invasion Perceived Risks	Protection Motivation Theory
<b>5.</b>	<i>High trust in integrity, benevolence, and competence can reduce the risks individuals perceive, and partly appease their HIPC.</i>	Perceived Trust	Protection Motivation Theory
<b>6.</b>	<i>Potential lifesaving benefits have a strong influence on individuals' acceptance of EHRs. Hedonic and Utilitarian benefits can influence individuals' intentions to adopt mHealth. In order to continue use, the individual must believe they are realising these benefits, and that they are relevant and worthwhile.</i>	Perceived Benefits	Privacy Calculus Theory
<b>7.</b>	<i>Citizens' HIPC can reduce their willingness to opt-in to an EHR. Individuals may express intentions to adopt mHealth, but privacy concerns will influence the type of mHealth solution they use and the data they disclose will be limited to non-sensitive data.</i>	Health Information Privacy Concerns	Privacy Calculus Theory

## 6.9 Conclusion

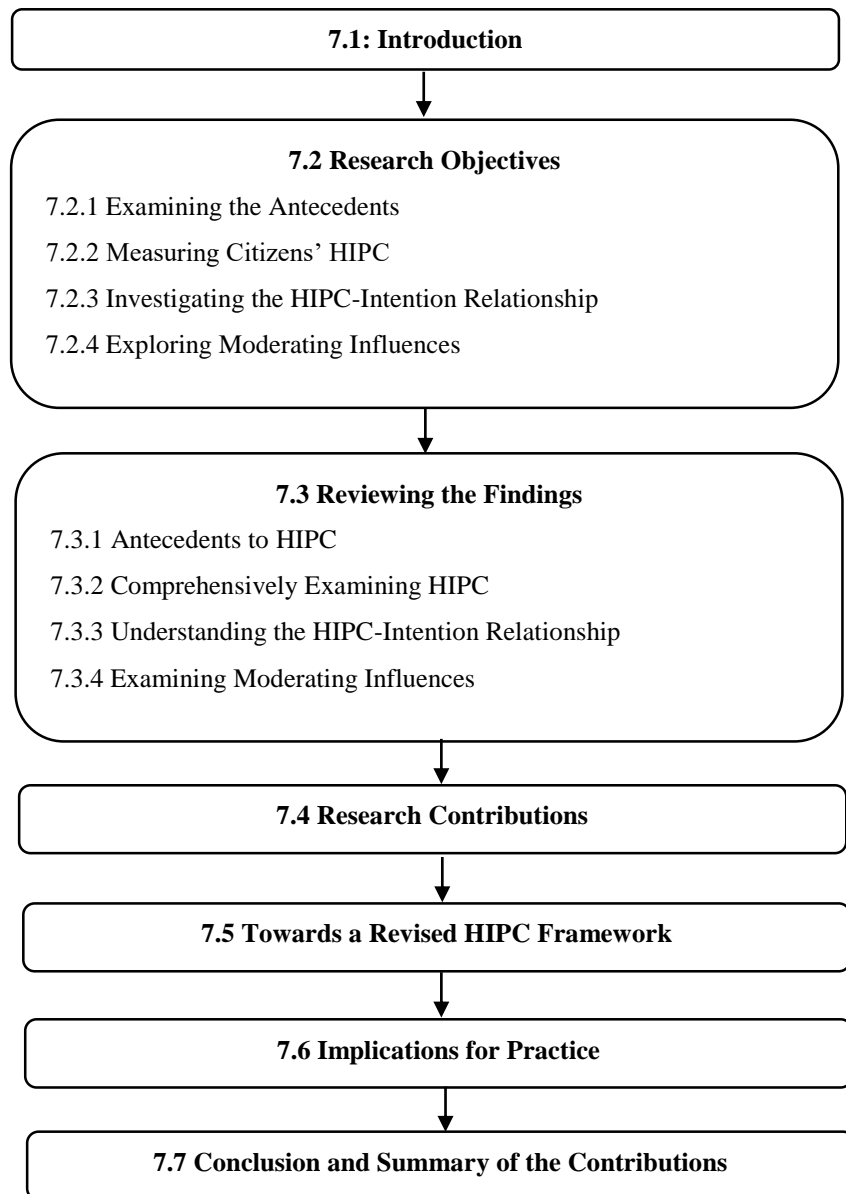
This chapter discussed the findings of 50 in-depth interviews with citizens in the U.S. and Ireland. The methods for analysing the data were briefly outlined, followed by an overview of how validity was ensured. The qualitative findings for each construct were discussed. Quantitative and qualitative findings were then integrated and a number of meta-inferences were developed to advance our understanding of citizens' HIPC. The following chapter discusses these findings further, along with their theoretical, empirical, and practical contributions.

## **CHAPTER SEVEN: DISCUSSION**

### **7.1 Introduction**

This study explores the influence of citizens' health information privacy concerns (HIPC) on their acceptance of technologies introduced by healthcare organisations, and their personal adoption of mobile health (mHealth) solutions. This chapter revisits the core objectives of the study and discusses how the integrated quantitative and qualitative findings meet these objectives. The chapter structure is outlined in Figure 7.1 below (pg. 225). The chapter begins with an outline of the research objectives. The findings and their implications are then considered in relation to these objectives. The unique contributions of the study are then discussed. A revised framework for understanding citizens' HIPC is presented, along with a number of theoretical assumptions. The implications of the findings for practice and recommendations for both healthcare organisations and technology vendors are described. The chapter concludes with an overview of the contributions the study makes in terms of empirical findings, theory, context, method, and practical implications.

**Figure 7.1 Chapter Structure**



## **7.2 Research Objectives**

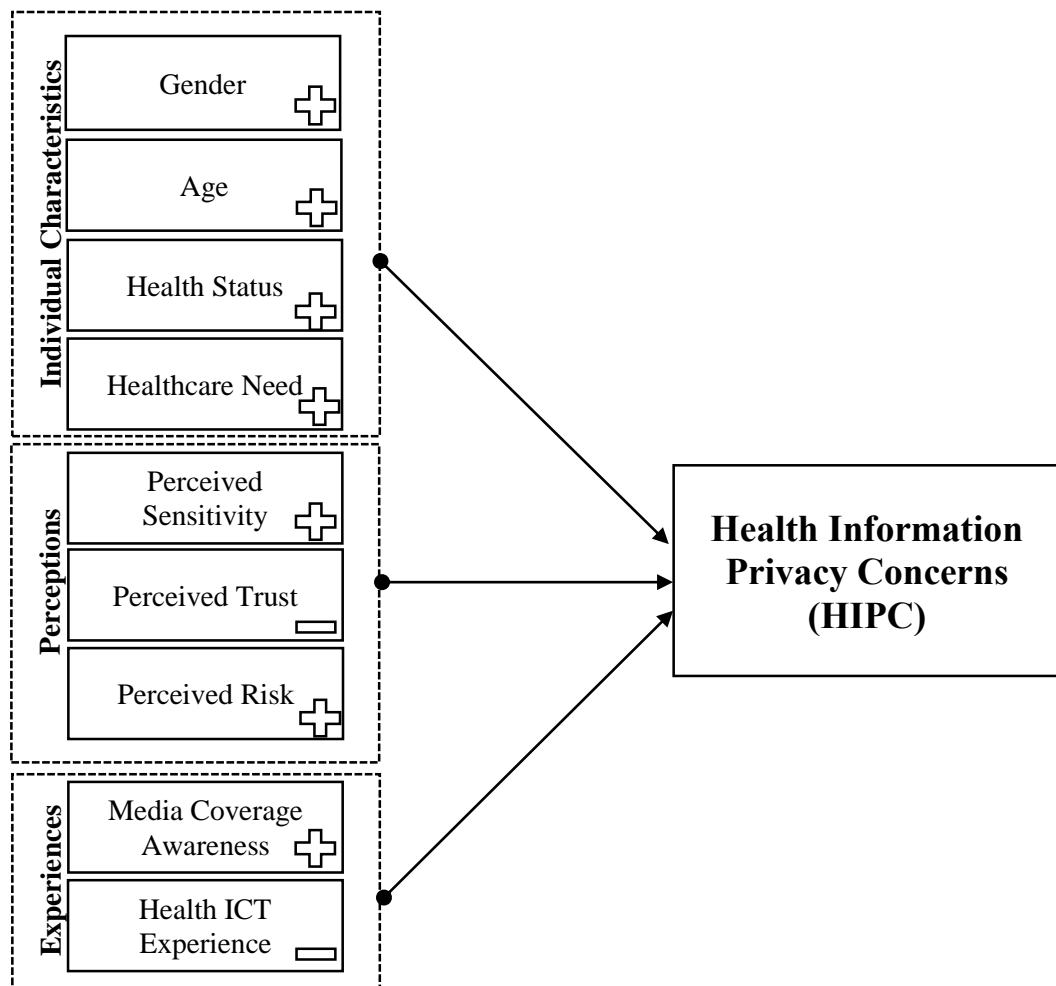
This study focuses on the information privacy concern construct in the health context. It specifically explores citizens' Health Information Privacy Concerns (HIPC) using samples from the U.S. and the Republic of Ireland. The study followed a three-stage mixed methods research design to develop a complete picture of the relationship between citizens' HIPC and their adoption of different health information technologies. The review of the information privacy, health informatics, and technology adoption literature identified many gaps in the current understanding of the information privacy construct in the health context, where empirical examination is limited. Based on this literature review, a framework for examining the drivers of HIPC, the important dimensions of concern, and the relationship between concern and adoption was developed. This framework leverages a number of theories and addresses several gaps in our understanding. Exploratory interviews were conducted to test and refine the framework. The second stage of the study involved testing the hypothesised relationships using a survey of citizens in the U.S. and Ireland. For the final stage, interviews were conducted with citizens in both countries. The research had four core objectives, which are outlined below.

### **7.2.1 *Examining the Antecedents***

The first objective was to explore the antecedents to individuals' HIPC. The literature review revealed a dearth of research exploring the factors which drive HIPC. However, in the broader information privacy research, prior studies have examined a myriad of potential antecedents (Li, 2011; Smith *et al.*, 2011). All of these antecedents were reviewed to determine their relevance to the health context. Based upon this literature review and the exploratory interviews, several antecedents were added to the research framework across three categories; individuals' characteristics, perceptions, and experiences. As citizens form the focus of the study, it was important to ascertain what individual characteristics influence HIPC. Gender, age, healthcare need, and health status were included as individual characteristics. Perception based factors included individuals' perceived trust in health professionals and technology vendors, perceived

risk of loss associated with disclosing health data to health professionals and technology vendors, and perceived sensitivity. Experience-related factors included privacy media coverage awareness, health information seeking experience, and mHealth experience. Together, these antecedents leverage two theories, the Information Boundary theory (perceived sensitivity) and Protection Motivation theory (perceived trust, perceived risk, and media coverage awareness). The quantitative survey involved testing the hypothesised influence of each factor on HIPC. Interviews aimed to develop a deeper understanding of the relationship between each factor and HIPC. Figure 7.2 below outlines the proposed antecedents.

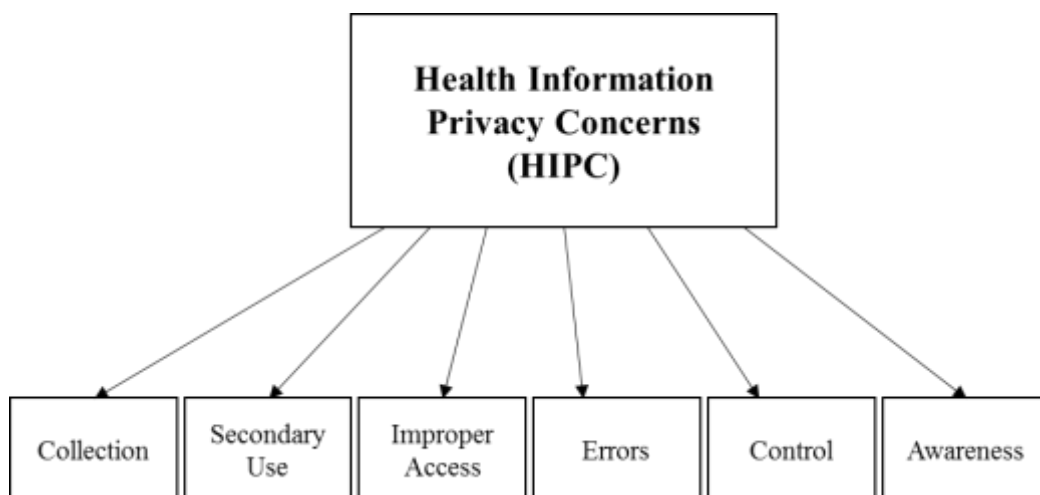
**Figure 7.2 Proposed Antecedents**



### 7.2.2 Measuring HIPC

The second objective of the study aimed to comprehensively examine citizens' HIPC. Many existing privacy studies in the Health Informatics discipline measured privacy concern as a one dimensional construct (e.g. Guo *et al.*, 2015), often using one item, without clearly defining privacy (Shaw *et al.*, 2011). This approach is useful for determining if concern is relevant, but does not provide an in-depth understanding of the different concerns in the health context. The broader information privacy literature in the MIS discipline provides a host of validated scales for measuring concern. For example, a number of recent health studies (Angst & Agarwal, 2009; Hwang *et al.*, 2012; Li *et al.*, 2014) utilised the four dimensional Concern for Information Privacy measure (CFIP). More recently, Hong and Thong (2013) developed the Internet Privacy Concerns measure (IPC), which consists of six dimensions of concern. As all six dimensions are arguably pertinent to the health context, IPC was viewed as the most comprehensive measure of concern. Thus the study adapted IPC to health context. The survey tested this newly adapted HIPC measure among Irish and U.S. samples to evaluate its reliability and validity. The qualitative study explored these dimensions in greater detail to improve understanding. The second order HIPC factor and its six first order factors are depicted in Figure 7.3 below.

**Figure 7.3 HIPC Dimensions**



### 7.2.3 Investigating the HIPC-Intention Relationship

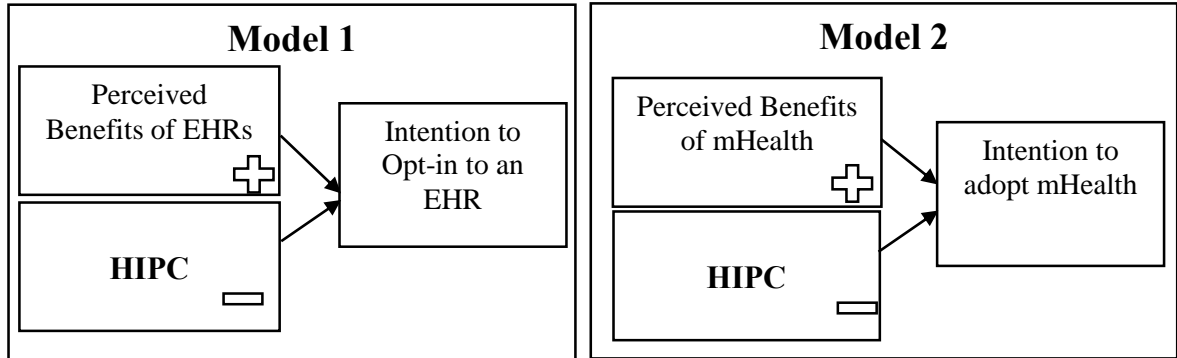
The third objective aimed to develop an understanding of the relationship between HIPC and individuals' adoption of Health Information and Communication Technologies (ICTs). Information privacy concerns have been found to reduce individuals' intentions to use ICTs in other contexts, and increase intentions to withhold or falsify data (Li, 2011). Health ICTs are relatively nascent and thus the relationship between HIPC and adoption of health ICTs remains relatively unexplored. The few existing studies have found support for the negative influence of concern on adoption (e.g. Angst and Agarwal, 2009; Li *et al.*, 2014). This study explored the relationship between HIPC and adoption of two types of health technology. Firstly, the relationship between HIPC and acceptance of an Electronic Health Record system (EHR) was examined. EHRs are implemented by healthcare providers and require citizens' consent prior to the digitisation of their data. Secondly, the relationship between HIPC and intention to personally adopt mHealth solutions was investigated. Intention to adopt mHealth was explored in the broad sense, followed by intention to use mHealth applications, wearable devices, and personal health records. These technologies are different as individuals choose to personally adopt mHealth and thus choose what data to disclose, whereas EHRs are implemented by healthcare organisations. The role of the citizen is different in both situations, and the relationship the citizen has with health professionals varies greatly from their relationship with health technology vendors.

Based on previous findings, it was hypothesised that HIPC would negatively influence citizens' (1) acceptance of EHRs and (2) intentions to adopt mHealth. The health technology adoption literature provides support for the relationship between intentions to adopt health technologies and actual adoption behaviour (Or *et al.*, 2011; Li *et al.*, 2016). However, the privacy paradox, a contradiction between citizens' intentions and their actual behaviour has been evidenced in other contexts. Thus, in the interest of rigour, the Privacy Calculus theory was leveraged to explore the privacy paradox. The Privacy Calculus theory proposes that individuals consider both their concerns and the benefits of adoption prior to adopting. If they perceive the benefits outweigh their concerns, they will adopt. The examination of the HIPC-intention relationship in both



models based on the Privacy Calculus is outlined below. The qualitative study also explored the relationships between HIPC, perceived benefits, and intentions, to develop deeper insights.

**Figure 7.4 Proposed HIPC-Intention Relationship**



#### **7.2.4 Exploring Moderating Influences**

The fourth and final objective of the study explored the possible moderating influences of health conditions and privacy invasion experiences on the relationships between HIPC, benefits, and intentions. This study proposed that individuals with chronic and sensitive illnesses would be influenced by different factors than healthy individuals. The survey compared the HIPC-intention and benefits-intention relationships across individuals with chronic conditions, and individuals with no chronic conditions to determine if chronic illness can influence this relationship. The HIPC-intention and benefits-intention relationships were also compared across individuals with sensitive illnesses and individuals with no illnesses they view as sensitive. It was argued that individuals' experience of privacy invasion would moderate how HIPC and benefits impact intention. In other words, if individuals believe their privacy has been frequently breached, the HIPC-intention relationship will strengthen and the benefits-intention relationship will weaken.

In summary, the study had four objectives pertinent to examining information privacy in the health context. These objectives included understanding the antecedents to HIPC, developing a comprehensive means of measuring HIPC, investigating the relationship between HIPC and adoption intentions, and exploring factors that moderate this relationship.

## 7.3 Reviewing the Findings

This section briefly reviews the key findings of the study in line with the research objectives.

### 7.3.1 *Antecedents to HIPC*

The results provide support for the influence of individuals' characteristics, perceptions, and experience on HIPC. Individual characteristics including age, gender, and healthcare need were tested as antecedents. The study provides quantitative support for the positive influence of age on HIPC. This supports the findings of Laric *et al.*, (2009), who found that older individuals expressed higher concerns for the privacy of various health data types, extends the partial supported offered by studies in Australia and the U.S. (King *et al.*, 2012; Kordzadeh *et al.*, 2016), and refutes the insignificant finding in a recent Taiwanese study (Hwang *et al.*, 2012). This study extends support for the positive influence of age on HIPC to the Irish context, whilst using a comprehensive measure of HIPC, as opposed to the one-item measures adopted by Laric *et al.*, (2009), King *et al.*, (2012), and Kordzadeh *et al.*, (2016). The interviews also offer a potential explanation for studies with mixed and insignificant results on the role of age. Many older interviewees expressed a strong desire for privacy, which was coupled with an assumption that this privacy is guaranteed, leading to reduced concern. Many of these interviewees were not cognizant of possible uses for this data or risks to its privacy, and thus expressed lower current concerns. This supports the assertions of Dinev (2014) who noted that many individuals desire privacy but lack an understanding of the volume of data collection and how this impacts their privacy. In summary, it is argued that HIPC does increase with age, but some older citizens may express lower concerns due to an assumption of privacy.

In terms of gender, males expressed higher HIPC than females. This conflicts with the findings of prior studies which found that females expressed higher concerns regarding the privacy of their health data (Laric *et al.*, 2009; Vodicka *et al.*, 2013). The interviews also offer a potential explanation for this surprising finding. While expressing a strong desire for privacy, many female interviewees assumed their health data was private, and as a result expressed lower levels of

HIPC. In contrast, many males were cognizant of the possible uses for health data, discussing potential unauthorised access to this data or secondary uses, and thus males often expressed higher HIPC. This echoes the results of an Internet based study, which found that women desired high levels of privacy, but often assumed they had a greater level of privacy (Joinson *et al.*, 2010). In addition, this study examined HIPC across six dimensions related to potential uses of health data, compared to the broad one dimensional measures used in previous studies (Laric *et al.*, 2009; Vodicka *et al.*, 2013). As males discussed the potential risks to their health data in interviews and many females assumed their data remained private, it is understandable that males in this study expressed higher concerns.

As expected, healthcare need had a positive influence on HIPC with individuals with greater need for healthcare services expressing higher concerns. The interviews provide a deeper understanding. Individuals with greater healthcare needs frequent doctors and hospitals more often. This results in an extensive health record for the individual, across a range of parties, thereby reducing control and as a result increasing individuals' perception of the risks associated with dispersed access to this data. Many of these interviewees were aware of the risks for secondary use, the potential for accidental or malicious unauthorised access, and expressed concern regarding their lack of control over how this information travels. These findings advance understanding of the role of health variables, as this relationship has not been explored in the existing literature.

In terms of individual perceptions, the study found a positive relationship between perceived sensitivity and HIPC. This echoes the results of Bansal *et al.*, (2010), and extends support for the sensitivity-HIPC relationship to an Irish sample. Interviewees expressed strong concerns regarding the privacy of health data they viewed as sensitive particularly in terms of unauthorised secondary use. Interviewees also expressed a stronger desire to control their sensitive data, to limit secondary usage, and access to their data. This provides empirical support for the assertions made by other researchers that individuals create boundaries to determine what personal health information can be disclosed and how it can be used (Anderson and Agarwal, 2011).

As hypothesised, the survey found that perceived risk associated with disclosing health data to technology vendors and health professionals positively influenced HIPC. Previous studies shown that risk perceptions increase individuals' privacy concerns towards health information websites (Xu *et al.*, 2011). This study extends the risk-privacy concern relationship to the context of HIPC in a general sense. The interviews further develop our understanding of this relationship. When interviewees believed disclosure of health data to health professionals or technology vendors may lead to negative outcomes, they expressed high concerns regarding unauthorised secondary use by technology vendors, and accidental or malicious access in the health setting.

The survey found that perceived trust in health professionals increased HIPC. While this relationship had not been previously examined in the health context, this finding conflicts with previous assumptions. For example, Rahim *et al.*, (2013) posited that trust in health professionals would reduce HIPC. This study provides empirical evidence that points to a contrary interpretation of this relationship. The interviews provide two possible explanations for this finding. Firstly, the survey examined two dimensions of trust, integrity and benevolence with regards to the individual's health data, as it is widely argued that high trust in an organisation's benevolence and integrity will reduce concerns (McKnight *et al.*, 2002). However, while interviewees expressed high trust in health professionals' integrity and benevolence, they expressed concerns regarding their ability to protect the privacy of their health data. Secondly, interviewees expressed low trust in the intentions of large health organisations, other employees in the health organisations, technology companies, third parties, and government departments who may be interested in accessing their health data. As a result, individuals expressed high HIPC, especially regarding secondary use, access, and control, irrespective of their personal trust in health professionals.

The study found that the relationship between trust in technology vendors and HIPC was negative as expected, but insignificant. This contrasts with Dinev *et al.*, (2016), who found that trust in EHR vendors significantly reduced HIPC. The interviews provide insights into the insignificant relationship. Unlike health professionals, interviewees had no pre-existing relationship with

technology vendors, and expressed low to no trust in the motivations of technology vendors with their health data. Interviewees had strong concerns about unauthorised secondary use, access, and lack of control over health data disclosed to technology vendors. As a result, interviewees either did not use mHealth solutions, or only disclosed data they viewed as non-sensitive. The absence of pre-existing trust can result in refusal to adopt or disclose data, in a bid to preserve privacy. Interviewees also noted if technology vendors could prove they were trustworthy, they may be more willing to disclose data, as their privacy concerns would be reduced. In conclusion, the study elucidates the relationship between trust in different parties and HIPC. Trust can reduce HIPC, if individuals trust in both the party's intentions, and capabilities to protect their data.

The study provides an important insight into the influence of privacy media coverage on HIPC. Previous studies have shown that greater awareness of privacy media coverage leads to higher concerns for the privacy of one's personal data stored by organisations (Smith *et al.*, 1996), and online entities (Malhotra *et al.*, 2004). The survey extends these findings to the health context, offering strong empirical support for the positive relationship between privacy media coverage and HIPC. The interviews offer two main insights which further develop our understanding of this relationship. Firstly, the influence of privacy media coverage on HIPC was strongest when interviewees: were familiar with an injured party from a privacy breach, were aware of specific stories, were cognizant of the risks to their own data, and paid attention to privacy media coverage. Secondly, privacy media coverage influences the majority of dimensions of HIPC, especially the awareness, control, and improper access dimensions. These privacy news stories remind individuals that (1) they are unaware of how their health data is protected and used, and (2) they have no control over the use and dissemination of this data.

### ***7.3.2 Towards a comprehensive measure of HIPC***

The six dimensional measure IPC measure was adapted to ensure applicability to the health context and titled HIPC. The survey data in both countries provided strong support for the reliability and validity of this new measure. In addition, the interviews provide four important

insights which advance our understanding of citizens' privacy concerns regarding their health data. Firstly, the widely discussed importance of privacy in the health context (e.g. Dinev *et al.*, 2016) was confirmed by interviewees. Ensuring the privacy of health data was paramount in the opinion of interviewees of all ages in both countries. Secondly, many interviewees had a blind assumption that health data was private, and only ever used to treat them. Similarly, with regards to mHealth, individuals believed this data remained on their own device and was not shared or subsequently used by technology vendors. This view sharply contrasts with the reality, as studies have shown that many States in the U.S. sell citizen data, and mHealth solutions share user data with a myriad of third parties (FTC, 2014). Thirdly, irrespective of privacy assumptions, all interviewees expressed strong opposition to unauthorised secondary use, and improper access to health data. Individuals who assumed health data was private, discussed these concerns in the hypothetical sense, expressing disagreement with these uses, and noting that if they did occur they would be very upset. Individuals who did not assume privacy was a guarantee, had high concerns regarding possible ongoing secondary uses or previous improper access.

Fourthly, the control and awareness dimensions of HIPC represent possible means of appeasing concern. When individuals felt they could not exercise control over their health data, they were extremely concerned. In addition, a lack of awareness of how health data is protected and used caused concern. Interviewees expressed the view that greater efforts to improve their awareness through education on how their data is secured, and transparency, coupled with an ability to exercise control over how their data is used and accessed, could appease concern. The mixed methods approach followed in this study provided a deeper understanding of privacy in the context of health data, reaffirming the importance of privacy, illustrating individuals' desire for privacy, highlighting the dominant concerns, and identifying the elements of concern which could be harnessed to reduce overall concerns.

### 7.3.3 *Understanding the HIPC-Intention Relationship*

The study examined the relationship between HIPC and citizens' intentions to (1) opt-in to an EHR, and (2) adopt mHealth solutions. The study found support for the negative relationship between HIPC and individuals' intention to allow their health data to be included in an EHR. This supports the findings of Angst and Agarwal (2009), and extends this relationship to a more comprehensive six dimensional measure of HIPC, tested among an Irish and U.S. sample. Interviews also revealed that strong concerns regarding unauthorised secondary use, malicious access, and lack of control, led to strong opposition to the digitisation of one's health record in a centralised system. In addition, individuals stated they might withhold certain data to protect their privacy in this context.

HIPC did not have a significant influence on intention to personally adopt mHealth in a general sense. However, HIPC reduced the intended frequency of mHealth application usage. In other words, if individuals had high HIPC, they might still use mHealth, but this use would be infrequent. The interviews revealed that HIPC does influence adoption of mHealth, but in a different way than expected. If individuals perceive that an mHealth solution requires the disclosure of sensitive data, they will not use this specific solution, but they may try other solutions. Individuals also place many conditions upon this use to protect their privacy including: utilising information-based mHealth applications which individuals perceive to be safe and generic, using mHealth solutions which require the disclosure of non-sensitive data only, limiting the volume of data disclosed, and falsifying the data disclosed. These revelations echo assertions and findings of researchers in the Internet context, who noted that in the presence of information privacy concerns, individuals will disclose minimal data, and may falsify data disclosed (Stutzman *et al.*, 2011; Keith *et al.*, 2013). In summary, the findings show that HIPC influences not only intentions but adoption behaviours and *how* individuals use these technologies.

The study also found that perceived benefits of EHRs and mHealth positively influenced adoption intentions. This supports previous studies which found that perceived benefits increased intentions to adopt personal health records (Li *et al.*, 2014), and wearable health devices (Li *et*

*al.*, 2016). The study extends support for the positive influence of perceived benefits to the context of EHR adoption, and mHealth adoption on a broader level. The study explored the Privacy Calculus theory, which posits that individuals compare the benefits and privacy concerns associated with a technology prior to adopting (Culnan, 1993; Culnan and Armstrong, 1999). The interviews provide support for the Privacy Calculus in influencing individuals' intentions to accept EHRs and adopt mHealth. Benefits could outweigh the influence of HIPC when the benefits were either (1) potentially lifesaving or (2) of great importance and relevance to the individual. This supports the views of Dinesen *et al.*, (2016) who asserted that health technologies must offer meaningful benefits for individuals to accept the privacy invasions they present. The study also showed that benefits had a stronger influence on the initial adoption decisions. This is unsurprising as the benefits are often more apparent at the outset. Privacy concerns in contrast, may not be considered when deciding whether or not to adopt. This study suggests that privacy concerns influence *how* individuals adopt these technologies. For instance, individuals may opt-in to an EHR, and afterwards may become concerned for their privacy. This may lead to them deciding to withhold data due to concern. In the context of mHealth, HIPC may influence the type of solution individuals adopt. Furthermore, post-adoption privacy concerns may cause the individual to cease using the solution, to falsify data, delete data, or withhold data going forward. In addition, the influence of perceived benefits seems to diminish following adoption, particularly for hedonic benefits. Individuals need to believe not only that they are achieving benefits, but that these benefits are relevant and important. Thus, the Privacy Calculus is important in this context, but the comparison of benefits and concerns is not straightforward. This comparison may be staggered, and influence not only adoption decisions, but decisions regarding what technology to use, how to use it, and whether or not to continue use.

#### **7.3.4 Examining Moderating Influences**

This study extends our understanding of health information privacy by providing evidence of moderating influences. Firstly, the moderating influence of chronic illness and sensitive illness on the HIPC-intentions and benefits-intentions relationships was investigated. The survey



revealed that among individuals with a chronic illness, the negative influence of HIPC on intention to accept EHRs was stronger, and the positive influence of benefits on intention was weaker. However, HIPC positively influenced mHealth adoption intentions. As both technologies can benefit individuals with chronic conditions through improving the healthcare they receive (EHRs), and empowering them to manage their chronic conditions (mHealth), benefits may have a greater influence on adoption decisions. However, HIPC may influence subsequent usage. For individuals with sensitive conditions, HIPC did not have a significant influence on intention to adopt EHRs or mHealth. However, the positive influence of benefits on intention to adopt both technologies was significantly weaker among this group. These individuals may use non-sensitive solutions or disclose non-sensitive data, but they are strongly opposed to maintaining a personal health record detailing their sensitive conditions or using any solutions which specifically focus on their sensitive illnesses. These findings provide insights on the influence of different conditions and show that individuals with health conditions may disclose insensitive data but express strong concerns regarding sensitive data in health technologies. It is evident that if the benefits are relevant to the individual's health but they don't believe their condition is sensitive, HIPC will not strongly influence initial adoption intentions. HIPC influences intentions when the data is sensitive and influences the volume and type of data disclosed.

Secondly, the study found that the frequency of personal and health data privacy invasion experience strengthened the negative influence of HIPC and weakened the positive influence of benefits on intention to opt-in to an EHR. For individuals who believed their privacy had been frequently breached, HIPC had a stronger negative influence on intention, as they believed future breaches may occur and feared the potential repercussions of such a breach. In contrast, personal and health privacy invasion experience did not moderate the HIPC-intention, and benefits-intentions to adopt mHealth relationships, but higher privacy invasion experience was associated with lower intentions towards mHealth applications. The interviews show that privacy invasion experience can strengthen the link between HIPC and intention when the invasion was severe,

occurred frequently, caused shock, pertained to sensitive data, and the individual still feels vulnerable. If, in contrast, the data was not sensitive or the individual no longer feels vulnerable, the HIPC-intention relationship is not strengthened.

## **7.4 Research Contributions**

The research makes four key contributions to the literature on the relationship between Health Information Privacy Concern and technology adoption. These contributions are now discussed in detail.

Firstly, the study developed our understanding of the predictors of health information privacy concern. The study showed that HIPC is influenced by individuals' characteristics, perceptions, and experiences. In the existing information privacy literature, a myriad of studies explored the antecedents to concern across various contexts leading to a disjointed body of knowledge. Recent efforts to categorise these antecedents have highlighted the importance of the context of the study in determining the influential antecedents (Li, 2011; Smith *et al.*, 2011). In the health context, a small number of studies have examined antecedents. For example, Dinev *et al.*, (2016) found trust in EHRs reduced HIPC, and Bansal *et al.*, (2010) found that perceived sensitivity increased concern. This study re-examined perceived trust and sensitivity, in addition to extending a number of antecedents from the information privacy literature to the health context. The study provides empirical support and in-depth insights into several antecedents. HIPC are shaped by individual characteristics including age, gender, and healthcare need, perceptions related to trust, risk, and sensitivity, and experience of privacy media coverage.

Prior to this study, our understanding of the antecedents to HIPC was limited, as only a small number of studies examined the antecedents and these studies focused on one or two antecedents. The study makes a substantial contribution to our understanding of the antecedents, and represents an initial step towards developing a comprehensive set of antecedents to privacy concerns in the health context. This is an important step for the literature, as understanding the drivers of privacy concern is imperative to develop approaches for addressing and appeasing concern.

Secondly, the study provides an understanding of the *privacy paradox* in the context of HIPC and intentions to accept an EHR and adopt mHealth. The privacy paradox occurs when individuals' behaviours contradict the concerns they express for privacy (Tsai *et al.*, 2011). In other words, individuals often express high concerns for the privacy of their information, but disclose this information in return for seemingly minor benefits. As a result, there has been much debate regarding the predictive power of behavioural intentions, with some arguing that privacy researchers should not assume intentions will result in actual behaviour (Belanger and Crossler, 2011). However, Li (2011) has argued there is sufficient empirical evidence to support the link between privacy concern, intention, and actual behaviour. In addition, the extant health technology adoption literature, supports the link between intention and behaviour. Researchers also argue that in other contexts, intentions are passive, and thus may not lead to behaviours, but intentions to adopt health technologies are active intentions, and thus more likely to be matched by behaviours (Or *et al.*, 2011; Li *et al.*, 2016). In order to explore the privacy paradox in the health context, this study leveraged the Privacy Calculus theory.

This study showed that both perceived benefits and HIPC can influence intention, but benefits often have a stronger influence on adoption intentions, and even initial adoption decisions. However, HIPC influence the type of data disclosed, with individuals withholding data they view as sensitive, and only adopting mHealth solutions which are deemed non-sensitive and require minimal data disclosure. The results obtained in this study support the assumptions underlying the Privacy Calculus theory that both benefits and privacy concerns can influence adoption. However, it further advances this understanding in a health-specific context, by illustrating that individuals in many cases, may not actively consider the benefits and concerns simultaneously. The study supports assertions that privacy concerns represent a barrier to health technology adoption, but if the benefits are significant, i.e. if health technologies can improve individuals' health, benefits are likely to outweigh concerns (Fischer *et al.*, 2014). Furthermore, whilst benefits may drive the decision to adopt mHealth in the broad sense, it is HIPC that influences the type of solution adopted, and subsequent use in terms of the volume and type of data disclosed.

Aside from the Privacy Calculus, individuals may also adopt if they perceive they have some level of control over the privacy of their health data. These insights break new ground by providing an explanation of the privacy paradox in the context of HIPC and technology adoption. On a prime facie level, there may be evidence of a privacy paradox as intentions may contradict individuals' privacy concerns, but on a deeper level, it is now clear that individuals' privacy concerns influence the volume and type of data disclosed. These important insights advance our understanding on the paradoxical relationship between privacy concern and behaviour.

The third contribution relates to the specific context and focus of this study. The focus of the study is unique as the majority of existing privacy research focuses on personal information (e.g. Hong and Thong, 2013). Only in recent years has health information received attention in privacy research. These studies have confirmed the importance of privacy concern on citizens' acceptance of EHRs (e.g. Angst and Agarwal, 2009; Dinev *et al.*, 2016), and adoption of personal health records (Li *et al.*, 2014). This study answers calls for studies to explore the predictors and inhibitors of health information technology adoption (Dinev *et al.*, 2016). The study extends the few previous studies by exploring the role of HIPC in a comprehensive manner, focusing on the predictive influence of specific antecedents, measuring concern via six dimensions, and investigating the inhibiting influence of HIPC and positive impact of benefits on intentions. In doing so, it provides a greater degree of granularity as to the factors that exert the greatest influence on information privacy concern, as well as elucidating the relationships between HIPC, benefits, and adoption intentions.

The context of the study in terms of the chosen samples also contributes to the literature. The study collected data from the Republic of Ireland and the United States. To date, the majority of previous health information privacy studies have utilised U.S. samples (e.g. Angst and Agarwal, 2009), with a small number focusing on other countries including New Zealand (Chhanabhai and Holt, 2007), Canada (Laric *et al.*, 2009), Australia (King *et al.*, 2012), and Taiwan (Hwang *et al.*, 2012). This study is the first to focus on information privacy in Ireland, thus answering previous calls to explore the role of information privacy and health information privacy concerns in

European countries (Anderson and Agarwal, 2011; Belanger and Crossler, 2011; Li *et al.*, 2016), as well as calls for studies which compare health privacy among different cultures (Dinesen *et al.*, 2016). The inclusion of the U.S. sample was important as many constructs were adapted to the health context for the first time in this study. Testing these constructs in both the U.S., where a host of privacy studies have been conducted, and Ireland, a country where no previous privacy studies have been conducted was important for validation purposes. In addition, the inclusion of both countries enabled interesting comparisons between citizens in countries with different health systems and different levels of exposure to health ICTs. This contributes to the literature in terms of developing and testing several constructs which can be applied in future research, and in terms of the highlighting differences in the views of citizens in both countries. Lastly, the sample characteristics make a contribution to the broader privacy literature, which has focused largely on student samples. The study includes individuals of all ages, and occupations (student, employed, retired), answering calls to investigate health privacy among older populations (Li *et al.*, 2014), and calls for privacy studies which include student and non-student populations (Belanger and Crossler, 2011).

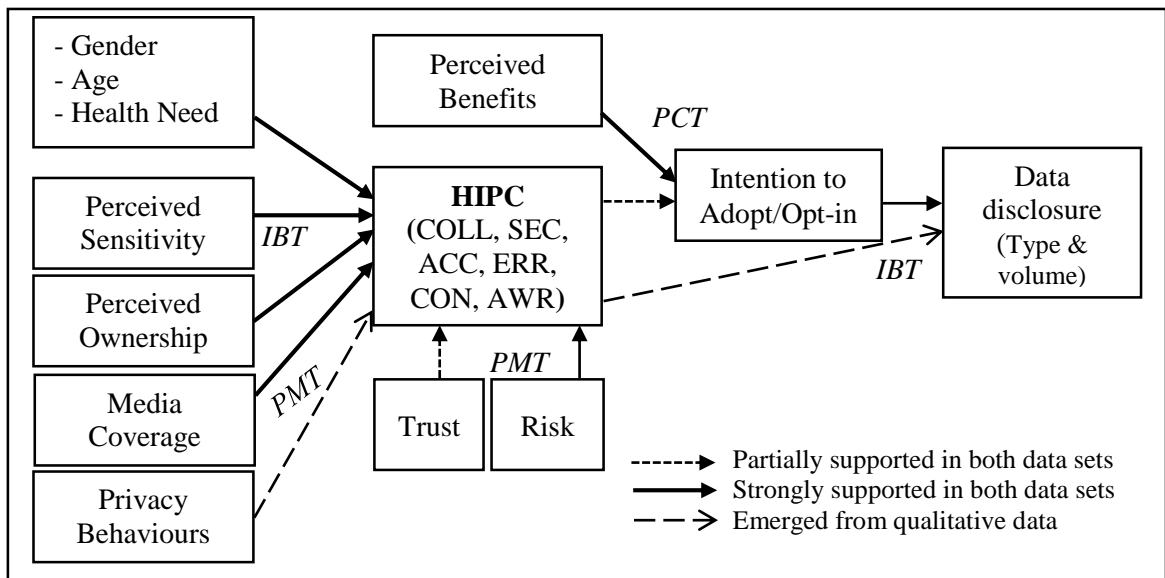
The fourth contribution of this study relates to the research methodology employed. The study applied a three-stage sequential mixed methods research design. The large majority of existing research utilises a quantitative survey (Angst and Agarwal, 2009; Li *et al.*, 2014; Li and Slee, 2014; Dinev *et al.*, 2016). While survey research provides valuable insights into the influence of HIPC on adoption, examining the labyrinthine privacy construct in the complex health context, calls for a more comprehensive approach to fully understand its role. Mixed methods are viewed as superior than single method studies when the phenomenon of interest is complex (Teddlie and Tashakkori, 2009). Furthermore, mixed methods studies can be applied to develop a more comprehensive understanding of a phenomenon (Venkatesh *et al.*, 2013). However, there is a paucity of mixed methods studies in the information privacy literature and indeed the broader information systems literature, resulting in many calls for mixed methods studies in this discipline (Venkatesh, Brown and Bala, 2013). This is the first study to apply a mixed methods research

design in the context of health information privacy. The sequential research design involved three stages of data collection, commencing with a preliminary exploratory study to test and refine the research framework developed from the literature. The second stage quantitatively tested this framework using a survey. The final stage consisted of semi-structured interviews to gain deep insights into the relationships between the various antecedents and HIPC, and the link between HIPC and adoption. The quantitative and qualitative findings were integrated to provide a more comprehensive picture of the role of information privacy in the health context.

## 7.5 Towards a Revised HIPC Framework

This section provides an overview of the final HIPC framework for examining citizens' HIPC and health technology acceptance and adoption. The framework is based on the integrated quantitative and qualitative findings, the overarching Theory of Reasoned Action and the supporting theories including Information Boundary theory (IBT), Privacy Calculus theory (PCT) and Protection Motivation theory (PMT). The revised framework is depicted below in Figure 7.5.

**Figure 7.5 Final HIPC Framework**



The HIPC framework above, represents the most comprehensive effort to date to understand the influence of citizens' Health Information Privacy Concerns on their acceptance and adoption of health technologies. Each construct in the framework is briefly reviewed at this point. Firstly, in

terms of individual characteristics, gender has an influence on HIPC. Males tend to be more cognizant of the possible risks to their health data and thus express higher concerns. Females express a strong desire for privacy, but often assume privacy is guaranteed and thus often express lower concerns. Secondly, age has a positive influence on privacy concern, as older individuals have a more extensive health record and are more likely to have health problems. This influence is strongest among individuals who are still employed, as they see possible repercussions to the misuse of this data. Older, retired individuals may express lower concerns due to an assumption of privacy and a lack of comprehension of the breadth of risks and uses enabled by technology. Individuals with greater healthcare needs express higher HIPC, as they have more extensive health records, and could be drastically impacted if their data was not private. In terms of specific health conditions, individuals with chronic conditions view health technologies more favourably as they can benefit from their implementation in health organisations and personal adoption. In contrast, individuals with sensitive conditions express higher concerns about the use of sensitive data, and are unwilling to use health technologies which require this data

The influence of perceived sensitivity on HIPC was strongly supported in the quantitative and qualitative data. This relates to Information Boundary theory, which posits that individuals create self-defined boundaries to determine what data can and cannot be disclosed (Petronio, 1991). This theory has been used in information privacy research to explore the boundaries individuals develop for different information types (Li, 2012). This study extends Information Boundary theory to the context of Health Information Privacy Concern and health technology adoption. The study provides support for this theory, as individuals with higher perceptions of sensitivity, express higher HIPC, particularly in terms of unauthorised secondary use, and improper access. Furthermore, even if individuals adopt mHealth technologies, they will not disclose sensitive health data, and may cease use if this data was requested. In summary, the study shows that individuals do create different boundaries for different types of health data. These boundaries influence HIPC, and the relationship between HIPC and adoption. Individuals will limit the disclosure of this data in mHealth solutions, and desire granular control of sensitive data collected

by health organisations. Perceived ownership of health data ties into the boundaries created by individuals. If individuals believe health data belongs to them, they develop stricter boundaries for the use of this data, are more concerned for the privacy of this data, and express a strong desire for control over this data.

A number of constructs in the framework pertain to Protection Motivation theory or PMT, which was originally developed by Rogers (1975). The theory is comprised of two broad elements; threat and coping appraisals. Threat appraisal encompasses the perceived severity of threats facing the individual, and the likelihood of these threats occurring. Coping appraisal relates to individuals' perceived ability to take action to reduce the threat (Rogers, 1975). This study extends PMT to the context of health information privacy. Threat appraisal is first represented by privacy media coverage awareness, which captures individuals' cognizance of the severity of threats to their health data. The study provides strong support for the influence of privacy media coverage. Greater awareness of privacy media coverage is associated with stronger concerns for the privacy of one's own health data. Perception of risk represents individuals' perception of likelihood of a given threat occurring. The individual considers the different risks they are aware of (media coverage), and the risks to their own data stored by healthcare provider or technology vendors. For example, if an individual recalls media coverage pertaining to a breach of health data in a hospital, and believes their data in a hospital is at risk, they will express high privacy concerns specifically regarding improper access to this data, potential secondary uses, and perhaps their lack of awareness of how their data is protected.

Coping appraisal is represented firstly by trust. If the individual trusts in the integrity, benevolence, and competence of the health professional or technology vendor to protect their data, their view of the threats will be diminished to a degree, and as a result their privacy concerns may weaken. However, the absence of trust in any of these dimensions can exacerbate individuals' perceptions of risk and HIPC. For instance, if an individual has high trust in the benevolence and integrity of health professionals, but low trust in their competence to protect their data, they will express higher HIPC. Secondly, privacy-protective behaviours were



discussed frequently in the interviews as a means to reduce the risks to one's data. These behaviours included withholding data and falsifying data. If individuals feel the privacy of their health data is at risk, they engage in these behaviours as a coping mechanism. These behaviours provide individuals with a sense of control and can reduce HIPC. This shows that the privacy-protective behaviours examined in the Internet context (Son and Kim, 2008) apply to health context. The study shows that threat appraisal and coping appraisals can both influence HIPC, and individuals' behaviours in the presence of concern.

Lastly, the Privacy Calculus theory (PCT) is included in the HIPC framework. Privacy Calculus theory assumes that individuals compare the benefits and privacy concerns prior to making an adoption decision (Culnan, 1993; Culnan and Armstrong, 1999). This study shows that both perceived benefits and HIPC can influence adoption intention, but benefits have a stronger influence on the decision to adopt. However, in order for benefits to influence continued use, they must be both important and relevant to the individual. HIPC influences the type of technology adopted, and subsequent behaviours such as the volume and type of data disclosed, with individuals often withholding sensitive data. This study extends the Privacy Calculus theory to explain the privacy paradox in the context of HIPC and mHealth adoption and illustrates that the relevance of benefits (Lwin *et al.*, 2007) also impacts HIPC.

Calls have been made for theorising to understand citizens' adoption of health technologies (Agarwal *et al.*, 2010). This study focuses on the influence of citizens' HIPC on this adoption. The study makes a large contribution to the literature on Health Information Privacy Concerns and health technology adoption, by developing the HIPC framework and leveraging several theories to explain the relationships within the framework. In summary, individuals' perceptions of sensitivity and ownership (IBT), appraisal of the severity and volume of risks to their data (media coverage), and the likelihood of these risks occurring (risk perception), can increase their HIPC. Trust and privacy-protective behaviours provide mechanisms for reducing privacy concerns. Individuals' adoption decisions are influenced by perceived benefits and HIPC, with perception of sensitivity, risk, and coping appraisals influencing how individuals behave to

protect their privacy. This framework has been supported in terms of two adoption scenarios (1) citizens' intentions to opt-in to an EHR introduced by healthcare providers, and (2) citizens' intentions to adopt mHealth technologies including (mHealth applications, wearable monitoring devices, and personal health records). The HIPC framework represents a strong starting point for identifying the important predictors of HIPC, and developing in-depth explanations for the complex relationship between HIPC and adoption.

## 7.6 Implications for Practice

This study provides a number of actionable insights for practice. These insights can be leveraged by health organisations, technology vendors, and government bodies involved in developing and delivering health solutions including electronic health records (EHRs) and mHealth solutions. Recommendations are discussed across five areas: improving citizen awareness, increasing citizens' level of control, educating citizens, involving citizens in ICT design, and fostering trust.

The first area relates to citizens' awareness. Individuals in the study expressed strong concerns regarding their lack of awareness of how their health data was used or protected. Increased awareness of how data is used could potentially appease citizens' privacy concerns and increase their acceptance and adoption of health technologies. The following recommendations for improving awareness are presented:

**Health Professionals:** Individuals' lack of awareness regarding how their health data is used by health professionals can cause concern. In line with the assertions of Jensen *et al.*, (2005), it is argued that upon collection of data, individuals should be fully informed of the need for their data, how it will be used, who will have access, how it will be protected, and the implications of this usage on their privacy. This reduces the potential for shock if individuals became aware of secondary usage at a later date (Agaku *et al.*, 2014). Many interviewees highlighted the importance of awareness, viewing it as a sign of respect. Awareness and transparency can reduce HIPC and enable individuals to make informed decisions to warrant or revoke consent.

***Awareness and EHRs:*** Upon introducing new systems such as EHRs, awareness should be a central focus to ensure acceptance among citizens. Prior to adoption, citizens should be informed of secondary uses and informed of what parties can access this data. Awareness efforts should be undertaken by all invested parties. This can include health professionals informing patients in person during patient visits and providing information leaflets and details on further information sources. In addition, health organisations should promote awareness via leaflets and information sessions (Hwang *et al.*, 2012). Following implementation of the EHR, individuals should have the ability to access information on the patient portal. Again when seeking consent for secondary uses or sharing of data, ensuring citizens fully understand the request should be paramount. Individuals should be fully informed of the control they have to: limit access to data, limit usage of data, request their data, and correct errors in data.

***Awareness and mHealth:*** Health technology vendors should ensure users are aware of how their data is used. While many applications use privacy policies, these policies often do not list all of the parties that user data is shared with (FTC, 2014). Privacy policies are also often viewed as an ineffective means of informing users, as the majority of users do not read these policies (Bélanger, Hiller, and Smith, 2002). Thus, technology vendors should strive to be transparent using notifications, or even gamification to ensure users are fully cognizant of how their data is used and what parties can access this data. This may reduce concerns and increase data disclosure.

The second area relates to individuals' perceived lack of control over their health data. Increasing individuals' control over their health data can reduce their privacy concerns (Awad and Krishan, 2006). Improving the control afforded to citizens represents a possible avenue for appeasing privacy concerns and increasing adoption of health technologies. The practical implications related to improving control are as follows:

***Improving Control of Data disclosed to health professionals:*** Perceived lack of control over how health professionals use patients' health data is a significant cause of concern and a key barrier to data disclosure. Health professionals should inform citizens of any potential secondary usage upon the collection of data, and seek their consent to use the data. This should occur in person

where possible, due to individuals' pre-existing trust in health professionals. Should a secondary purpose for the data emerge at a later stage, consent should be sought at this time. Again, efforts should be made to do this in person. Individuals should also be informed that the decision to consent rests solely with them, and should not feel pressure to consent. Blanket consent for a number of subsequent uses should not be sought.

***Control and EHRs:*** When implementing a new EHR system, patient control should be a priority and built into the system. Firstly, consent should be sought to include the individuals' data. In line with the position expressed by Dinev *et al.*, (2016), it is argued that individuals should be able to control their privacy preferences in EHRs. This control could be achieved using a patient portal page that citizens can log on to. Citizens could exercise granular control over the different uses of their health data and determine the level of access granted to different parties. Individuals should be able to review these controls periodically, put a blanket ban on commercial uses or access by external organisations, and should receive a consent request if a subsequent use emerges. This level of control could appease citizens' concerns, and improve their acceptance.

***Control and mHealth:*** In terms of mHealth technologies, when individuals sign up for the service, they should have control over subsequent uses of their data. Again this consent should be explicit, and reviewed when new uses arise, or whenever the individual decides to update their controls. These controls could be incorporated into the settings of the application or health platform. Again this could appease concern and improve adoption.

The third area relates to education, which is an important issue in the context of health privacy and technology adoption. When individuals don't understand the risks of health data disclosure, or the benefits of health technologies, they cannot make informed decisions. The interviews illustrated that citizens currently lack an understanding of how their health data is used by health professionals and health technology vendors. This highlights the need to educate citizens and improve their privacy literacy especially in the context of their health data. Recommendations for improving literacy include:

***Educating Citizens regarding EHRs:*** The introduction of EHRs can benefit many parties, but citizens' acceptance represents a barrier to adoption. In order to improve attitudes, citizens should be educated on the benefits of the EHR system for them as an individual and on a broader level (Dinev *et al.*, 2016). Citizens should also be educated on the technical aspects of the EHR (Hwang *et al.*, 2012). These education efforts should also inform citizens of how their privacy is protected and how their data might be used and shared. Prior to implementation, large scale educational campaigns should be launched by all invested stakeholders. The government should utilise various media and online outlets to neutrally educate citizens (Hwang *et al.*, 2012). In addition, educational campaigns should be launched within health organisations and doctors' offices to ensure individuals have an information source, should they have queries. To ensure individuals can access their own patient portal, information sessions should be offered along with practical tutorials delivered in conjunction with health and educational institutions. These educational efforts could address privacy concerns from the outset, inform citizens of their control, and ensure they are aware of the available information sources.

***Education and mHealth:*** Adoption of mHealth solutions, especially by citizens with chronic conditions and older citizens, can reduce the financial burden on health services (PWC, 2013). Thus improving adoption by these groups is crucial. In order to ensure individuals of all ages and conditions are capable of adoption, educational efforts should be launched by technology companies in collaboration with governments and health bodies. These campaigns can ensure all citizens are aware of the technologies available to improve their lifestyle. In addition, for individuals who are not technically competent, resources should be available to empower these individuals to utilise mHealth solutions. Health organisations should provide information resources and recommend validated, respected solutions to patients, which may aid in their health management, while protecting their privacy.

The fourth recommendation pertains to the design of EHRs and mHealth technologies. The following recommendations are offered:

***Involve patients prior to implementation of EHRs:*** Patients and patient interest groups should be engaged prior to the implementation of an EHR. This communication can identify the specific concerns of patients regarding privacy and security. These concerns can then be addressed prior to implementation. In addition, the level of control desired by patients can be ascertained and incorporated in the system design. The inclusion of patients also signifies respect and acknowledges the importance of patient acceptance.

***Involve Older Citizens in the design of mHealth:*** As the incidence of chronic illness increases with age, it is widely argued that older citizens can benefit from the use of mHealth, but they are likely to abstain due to issues related to privacy and lack of trust (Or *et al.*, 2011; Fischer *et al.*, 2014). In addition, the interviewees in this study expressed the view that these technologies were not user-friendly. It is thus proposed that older individuals should be included in the design process by technology vendors, in conjunction with health professionals. Research via focus groups can aid in identifying the barriers to adoption and unravelling the specific privacy and trust concerns of these users. Target users should also be included in the design testing phase to ensure these solutions are easy to use and understand.

The final area relates to trust, which has played a fundamental role in healthcare delivery for centuries. The implications for practice pertaining to trust are as follows:

***Building Trust in Health Professionals' competence:*** Individuals have high trust in health professionals' integrity and intentions (benevolence), but low trust in their competence to protect data. This leads to concerns regarding unauthorised access to the data, both in the physical and electronic sense. In order to address these concerns, health professionals need to build trust in their competence to physically protect patient data, by ensuring cabinets and doors are secured. In addition, health professionals could briefly inform patients of the measures they use to protect their data physically and electronically. This could reduce concerns regarding unauthorised access (physical and electronic), and lack of awareness regarding how their data is protected. In addition, when introducing an EHR, trust can be fostered by informing citizens of the technical measures in place to maintain their privacy such as audit trails which track access to data.

Building trust in health professionals' competence and the privacy of EHRs can reduce concerns (Dinev *et al.*, 2016).

***Building trust in Health technology vendors:*** In terms of technology vendors, individuals trust their ability to protect their data (competence), but have low trust in their integrity and benevolence. The strong mistrust in technology vendors, increases citizens' privacy concerns, and reduces their willingness to disclose health data to these companies. In order to reduce these concerns and increase adoption, technology vendors should engage in efforts to build trust, as no pre-existing trust exists. Trust in their integrity could be fostered through an allegiance with a reputable health body or renowned health organisation. In addition, technology vendors could seek health professionals' endorsement on a local level. Trust in their benevolence could be developed through transparency efforts (Son and Kim, 2008), and informing citizens of any uses for their data, and seeking their permission prior to subsequent use.

In summary, this study provides a number of insights pertinent to health professionals, health organisations, technology vendors, and other parties interested in citizens' acceptance and adoption of health technologies. The study illustrates the potentially inhibiting influence of citizens' HIPC on acceptance, adoption, and information disclosure. Individuals may be willing to consent to secondary use and additional access if they are educated, aware, and have control.

## **7.7 Conclusion and Summary of the Contributions**

This study set out to examine the influence of citizens' HIPC on their acceptance of EHRs, and their adoption of mHealth solutions. The findings highlight the importance of individuals' characteristics, perceptions, and experiences in shaping their HIPC. The study also represents an initial attempt towards untangling the privacy paradox in the health context, by illustrating the influence of HIPC on adoption intentions, and willingness to disclose health data. The HIPC framework which was tested quantitatively and qualitatively, and refined based on the integrated findings harnesses several theories to understand citizens' HIPC. The findings of this study make a number of empirical and theoretical contributions to the information privacy, technology

adoption, and health informatics literature. The study also provides actionable insights for health and technology organisations interested in understanding the factors that influence citizens' HIPC and maximising their acceptance and adoption of health technologies. The following chapter reviews these contributions along with the limitations of the study and directions for future research. The key contributions of the study are summarised in table 7.1 below.

**Table 7.1 Summary of Study Contributions**

<b>Area</b>	<b>Call for Research</b>	<b>This Study</b>
<i>Empirical</i>	Future studies should include technology adoption constructs such as perceived usefulness (Angst and Agarwal, 2009). Future studies exploring individuals' privacy, risk, and trust perceptions regarding their personal health data are needed (Chhanabhai and Holt, 2007). Future health studies should focus on the Privacy Calculus and technology adoption (Li <i>et al.</i> , 2016).	The study tests and supports a number of antecedents to HIPC, adapts the six dimensional measure of privacy concern to the health context, and explores the relationship between HIPC, perceived benefits, and adoption intentions.
<i>Theoretical</i>	The majority of studies exploring citizens' adoption of health ICTs lack theoretical foundations (Or and Karsh, 2009). There is a need for future privacy studies to utilise a comprehensive approach examining antecedents, dimensions of privacy concern and outcomes (Smith <i>et al.</i> , 2011).	The study develops the HIPC framework which extends Information Boundary, Privacy Calculus, and Protection Motivation theory to the health privacy context. The HIPC framework provides a strong starting point for understanding the role of privacy in the health context.
<i>Method</i>	Mixed Methods can aid researchers in developing novel theoretical perspectives that can advance the IS field, thus we urge researchers to consider mixed methods approaches (Venkatesh, Brown and Bala, 2013)	This study utilised a mixed methods design to gain a deep insight into the HIPC construct. The survey confirmed/disconfirmed the relationship between several constructs and HIPC, and interviews developed in-depth insights into these relationships.
<i>Context</i>	There is a need to compare privacy concerns between student and non-student populations, and for studies in Northern Europe (Bélanger and Crossler, 2011). Future studies should explore the HIPC of broader populations including older individuals (Li <i>et al.</i> , 2014).	To answer these calls, the study collected data from individuals aged 18 – 65+ in Ireland and the United States.
<i>Practice</i>	Privacy concerns must be understood and addressed to ensure health ICTs are trusted upon implementation (Chhanabhai & Holt, 2007; Dinev <i>et al.</i> , 2016).	The findings provide health and technology organisations with actionable insights to educate individuals regarding health technologies in ways which appease concerns and increase adoption.



## **CHAPTER EIGHT: CONCLUSION**

### **8.1 Introduction**

The primary objective of this study was to conduct an in-depth investigation of the influence citizens' Health Information Privacy Concerns (HIPC) have on their acceptance of health technologies introduced by healthcare providers, and their personal adoption of mobile health (mHealth) solutions. The study followed a sequential mixed methods approach to gain a comprehensive picture of citizens' information privacy concerns in the health context.

The structure of the dissertation was as follows: Chapter One justified the need for this study and provided an overview of the research objectives, research framework, and key hypotheses. Chapter Two consisted of a review of the extant information privacy and technology adoption literature to identify gaps in understanding and determine the appropriate theories and constructs for this study. Chapter Three presented the proposed research framework for addressing these gaps and detailed the hypothesised relationships in the study. Chapter Four detailed the methodological steps involved in testing and refining the proposed research framework, and the epistemological assumptions underpinning the study. Chapter Five presented the results of the quantitative testing of the research framework. Chapter Six provided an overview of the primary findings from the interviews. The quantitative and qualitative findings were integrated to develop a deeper understanding of HIPC. Chapter Seven discussed the research contributions of the study and presented the revised HIPC framework along with a number of theoretical assumptions and the practical implications. This final Chapter draws conclusions on the contributions of this study to our understanding of Health Information Privacy Concerns. The limitations and directions for future research are also presented.

### **8.2 Contributions to Theory**

This section details the empirical and theoretical contributions of the research. While the previous chapter (Section 7.4) detailed how the study met the four research objectives, this section reviews

how the study addresses the gaps in the existing literature identified in Chapter Two and adds to our understanding of the information privacy construct in the health context.

### ***8.2.1 Addressing Gaps in the Literature***

The primary gaps in the literature addressed by the study are reviewed below.

#### **(i) Gap in understanding the predictors of HIPC**

One of the major deficiencies in the existing literature pertained to the dearth of research focused on understanding the drivers of individuals' Health Information Privacy Concerns. Many studies failed to explore the role of predictive factors, while others included a small number of antecedents such as trust in EHRs (Dinev *et al.*, 2016), perceived sensitivity and privacy invasion (Bansal *et al.*, 2010). The proposed HIPC framework posited that individuals' HIPC would be influenced by several factors including individuals' characteristics, perceptions, and experiences. The study supports the influence of individual characteristics such as age, perceptions such as sensitivity, and experience factors such as privacy media coverage awareness. Thus, this study provides a comprehensive picture of how individuals' HIPC are shaped. This is a crucial contribution to the literature as understanding the factors driving HIPC is imperative to developing approaches to address and appease citizens' concerns.

#### **(ii) Confusion regarding the conceptualisation of Information Privacy**

Conflicting conceptualisations of the information privacy construct dominate discussion in a number of academic disciplines. In the health context, many studies fail to offer an unambiguous definition of privacy, with many failing to distinguish privacy from similar but distinct concepts such as confidentiality (Shaw *et al.*, 2011). This approach limits our ability to draw conclusions on the role of privacy in these studies, as it has not been adequately defined. In order to resolve some of this confusion, this study reviewed the prevailing privacy definitions across a number of academic disciplines, and presented a balanced definition for health information privacy, which can be leveraged in future studies.

### **(iii) The proliferation of unidimensional measures**

The large majority of prior health information privacy studies utilised a unidimensional measure for examining HIPC, a number of which used one item (e.g. Chhanabhai and Holt, 2007). While these studies are useful for illustrating the importance of concern, they fail to provide in-depth insights into the prominent concerns in the health context. A small number of studies utilised the four dimensional Concern for Information Privacy (CFIP) measure (e.g. Angst and Agarwal, 2009; Dinev *et al.*, 2016). These studies illustrate the relevance of measures from the Internet context, and provide important insights into four dimensions of concern in the health context. However, this study proposed that the six dimensional Internet Privacy Concerns (IPC) measure provides a more comprehensive understanding of the facets of concern in the health context. This study adapted and tested the IPC measure among samples in two countries, and provided support for its use in the examination of citizens' HIPC. By doing so, the study provides insights into citizens' HIPC across six dimensions.

### **(iv) Understanding the influence of HIPC on Adoption Intentions**

To date, a small number of studies have examined the relationship between citizens' Health Information Privacy Concerns and their health technology adoption. These studies show that citizens' HIPC can have an inhibiting influence on their acceptance of Electronic Health Records (EHRs) (Angst and Agarwal, 2009; Li and Slee, 2014), and adoption of PHRS (Li *et al.*, 2014). It is imperative to build upon these studies to understand how HIPC inhibits individuals' adoption of health technologies (Dinev *et al.*, 2016). This study quantitatively and qualitatively explored the influence of citizens' HIPC on (1) their acceptance of EHRs, and (2) their adoption of mHealth solutions. The mixed methods approach provided an in-depth understanding of the relationship between HIPC and intentions, illustrating that concerns can not only reduce citizens' adoption intentions but can also reduce individuals' willingness to disclose health data, and cause individuals to engage in privacy-protective behaviours such as falsifying data disclosed. These insights are imperative for illustrating the negative impacts citizens' HIPC can have. This study is the first to untangle the HIPC-intention relationship in the health context.

**(v) Failure to leverage existing theory**

A large number of prior health information privacy studies lack theoretical foundations. In addition, many studies utilise one theory to explain the factors driving health technology adoption, or the trade-offs facing individuals' adoption decisions. These theories provide interesting insights but are limited as they fail to address the privacy construct in a holistic manner. This study and the proposed HIPC framework leverage a number of relevant theories to explain the factors driving citizens' HIPC, the influence of HIPC on intentions, and the trade-offs between HIPC and other constructs such as perceived benefits. The study harnessed the Information Boundary theory, Protection Motivation theory, and Privacy Calculus theory to develop, test, and refine the HIPC framework. This theoretically founded, empirically supported framework advances our understanding of citizens' HIPC based on the 'Antecedents-Concerns-Intentions-Behaviour' approach.

**(vi) Dearth of Mixed Methods Studies**

There is a paucity of studies which utilise a mixed methods approach to examine the role of information privacy in the health context. Due to the nascence of health technologies and this research area, mixed methods studies can provide a comprehensive picture of the privacy construct in this context (Venkatesh *et al.*, 2013). This study utilised a three-stage sequential mixed methods research design to conduct a comprehensive examination of citizens' HIPC. The proposed HIPC framework developed from the Literature Review, was tested and refined based on exploratory interviews. The hypothesised relationships in the framework were quantitatively tested using survey data collected from 447 citizens in Ireland and the United States. In the final stage of data collection, in-depth interviews were conducted with 50 citizens in both countries. These interviews provided explanations for the relationships in the framework. The quantitative and qualitative findings were integrated to further refine the HIPC framework and provide detailed insights into the drivers of HIPC, the dimensions of concern, and the relationship between HIPC and adoption intentions. This framework provides a strong starting point for future research

to build upon and gain a deeper understanding of citizens' concerns, and develop and test approaches for appeasing these concerns.

**(vii) Limitations inherent in study samples**

Many of the existing studies utilise samples which cannot be generalised to the wider population. For instance, some studies focus exclusively on student (Bansal *et al.*, 2010; Li *et al.*, 2014) or elderly samples (Fischer *et al.*, 2014). While both groups are interesting, the findings of these studies cannot be generalised due to the specificity of the samples. The samples in this study are diverse in terms of age, educational background, technical competence, and health condition, which is imperative to fully understand the role of different antecedents and the HIPC-intention relationship, and to explore the influence of age. This study adds to the small number of existing health information privacy studies that have utilised a diverse age sample and answers calls for studies which compare student and non-student populations (Bélanger and Crossler, 2011), and studies with older populations (Li *et al.*, 2014).

**8.2.2 Additional Contributions**

The study also makes additional contributions that were not identified as gaps in the existing literature. Firstly, the study identified constructs which may be relevant to examining privacy in the health context, but not other contexts. In the exploratory interviews, the issue of perceived ownership emerged as an important determinant of individuals' level of privacy concern. Based on these interviews, the perceived ownership construct was adapted from the organisational psychology literature and tested in the survey and subsequent interviews. The study shows that perceived ownership of health data increases individuals' HIPC. In addition to identifying this previously ignored construct, the study provides the grounds for future research to further explore ownership perceptions. Secondly, the interviews highlighted the prevalence of privacy-protective behaviours, which have not been previously examined in the health context. The interviews show that individuals engage in many behaviours which they believe protect the privacy of their health data including withholding and falsifying data. This is an important finding for directing future

research and also on a practical level as withholding data from health professionals could adversely impact the health of citizens. This further highlights the importance of negating citizens' HIPC to reduce the prominence of privacy-protective behaviours.

Thirdly, this study provided a deeper understanding of privacy in the health context. The study provides undisputed support for the importance of preserving health data privacy with all interviewees expressing a strong desire for their health data to remain private. The study also supports previous studies that show individuals often express high concerns regarding the privacy of their health data. The majority of interviewees were concerned for their health data privacy. In addition, those that expressed lower concerns did so due to their belief that their data was private, and an assumption that there was no need for concern.

### **8.3 Overview of the HIPC Framework**

The key contribution of this study is the culmination of the contributions outlined in the previous section leading to the development of a comprehensive framework for examining the drivers of HIPC, examining the dimensions of concern, and exploring the influence of HIPC on technology adoption. The primary constructs and underlying theoretical assumptions in the final HIPC framework are briefly reiterated here to demonstrate how this study creates a strong foundation for future research to build upon and advance understanding even further.

The HIPC framework proposes that individuals' HIPC are shaped by their characteristics, perceptions, and experiences. In line with the Information Boundary theory, the study shows that individuals create boundaries to determine what data they are willing to disclose and what data they wish to protect (Petronio, 1991). Perceived sensitivity increases citizens' HIPC and reduces willingness to disclose this data. In line with Protection Motivation theory (Rogers, 1975), the study shows that individuals appraise the threats to the privacy of their health data, and their ability to cope with these threats. Individuals reflect on the breadth and severity of the threats facing their data based on their knowledge of privacy media coverage, and compare these threats with their perception of the risk these threats will occur upon disclosure of their health data to

health technology vendors and health professionals. Individuals' coping appraisal is comprised of their trust in health technology vendors and health professionals to protect their data, and their intentions to engage in privacy-protective behaviours. When individuals believe the threats are severe and likely to occur, they express high HIPC. Trust can partially mitigate these threats and reduce HIPC. In line with the Privacy Calculus theory, both individuals' HIPC and perception of benefits can influence their adoption decisions. If individuals believe the benefits are achievable and relevant to them, they will express high adoption intentions. On the other hand, high HIPC can reduce intentions. In addition, citizens' HIPC can influence their subsequent adoption behaviours by determining the volume and type of data they are willing to disclose.

## **8.4 Limitations and Directions for Future Research**

Despite the contributions this study makes to research and practice, there are a number of limitations that should be noted. Firstly, the main objective of this study was to measure individuals' adoption intentions as opposed to their actual behaviour. Therefore, the study's findings should be considered in that context, as whilst it is critical to understand the factors that influence formation of intention, those intentions do not always evolve into actual practice. However, behavioural intention is viewed as a desirable dependent variable in this study, due to the nascence of health technologies (Hsieh, 2015), and the support provided by previous studies for the link between intentions and health technology adoption (Li *et al.*, 2016). In addition, actual adoption could not be examined, as Electronic Health Records have not yet been implemented on a national scale in Ireland and many of the U.S. respondents stated that their healthcare professional does not currently use EHRs. The study was undertaken with full understanding of this situation and thus provides predictive insights for health organisations interested in ensuring maximal patient adoption. With regards to mobile health, the study provides insights into citizens' intentions to adopt different mHealth solutions. This study shows that HIPC can reduce both individuals' adoption intentions, and their willingness to disclose different types of health data. To further advance our understanding of the relationship between citizens' HIPC and health technology adoption, future research should explore individuals' actual

adoption of mHealth technologies, and their actual disclosure of health data, focusing on the disclosure of sensitive data and the falsification of data disclosed (Keith *et al.*, 2013). This will further extend our understanding of the Information Boundary theory in this context. In addition, future research could utilise predictive analytics to further test the HIPC framework and explore the ability of such models to predict citizens' intentions to adopt health ICTs such as EHRs and mHealth solutions.

The second limitation relates to the study's samples. Although a concerted effort was made to ensure the views of citizens of varying ages, background, and health condition were included, there are some limitations inherent in the existing sample characteristics. Firstly, only a small number of individuals aged over 50 were included in the U.S. sample (n=28), and none of these individuals were retired. As a result, it was not possible on this occasion to make comparisons between retirees in the U.S. and Ireland. Secondly, based on self-selection and the voluntariness of information provision, it was only possible to include a small number of individuals with sensitive illnesses in this study. Whilst their inclusion provided valuable insights in relation to the influence of sensitive illness on privacy concern and adoption intentions, due to the limited size of this sub sample, it was not possible to quantitatively explore the influence of past stigmatisation on the privacy concerns and adoption intentions of individuals with sensitive illness. In addition, the sample did not include individuals with no Internet experience. While this is a shrinking group, these individuals may have different privacy concerns. Although these issues did not hinder analysis of the proposed models and the dominant constructs, it would be interesting for future research to focus on specific samples such as retirees, or those who have experience of stigmatisation in order to explore their views towards HIPC, EHRs, and mHealth solutions.

The third and final limitation relates to the comprehensiveness of the framework presented for understanding the role of information privacy concerns in the health context. The study leveraged a number of theories and examined several variables quantitatively and qualitatively. This study and the HIPC framework represent a great starting point for understanding the role of Health



Information Privacy Concerns in influencing health technology adoption. However, the framework may not include all factors which influence citizens' HIPC, and their adoption as a result. This framework can be retested and further advanced to develop a comprehensive understanding of HIPC and health technology adoption. A number of factors which emerged in the qualitative data could be tested quantitatively including health locus of control, which may influence HIPC and adoption decisions. As noted throughout the previous chapter, privacy-protective behaviours can play an important role in reducing concerns. Privacy-protective behaviours should be tested quantitatively by adopting the measure developed by Son and Kim (2008) to the health context. In addition, negative experiences such as past privacy invasion or exposure to negative media coverage may manifest in heightened privacy concerns for a limited time. The temporal influence of these effects represent another avenue for future research to deepen our understanding of how these factors influence individuals' HIPC, their attitudes towards health ICTs, and their subsequent adoption and use behaviours. This relates to the limited cognitive abilities of individuals in terms of processing all relevant information when making privacy and adoption decisions which has recently been highlighted (Dinev *et al.*, 2015). It would be interesting for future research into health technology adoption and information disclosure to explore the role of factors such as cognitive processing ability, and issue involvement which was investigated by Angst and Agarwal (2009).

This study provides deep insights in the relationship between HIPC and two diverse health ICTs, EHRs and mobile health solutions. Future research can explore the influence of privacy concerns on citizens' acceptance of other health ICTs such as home monitoring systems which connect health organisations to patients, but could be described as more pervasive and as a result may foster concerns for privacy. Furthermore, as health ICTs mature, it is likely we will see a shift towards the vision of 'Connected Health', where citizens' health data is collected by several devices and simultaneously shared among parties engaged in delivering health services to the individual. It is proposed that these new health ICTs will foster high privacy concerns regarding individuals' physical and informational privacy. These systems present many privacy challenges

and opportunities for future research to understand the changing role of privacy in the health context where emerging technologies are transcending physical and informational boundaries and becoming more pervasive and connected.

Lastly, as noted in section 7.6 and shown throughout the interviews, individuals currently lack privacy literacy particularly in the context of their health data. This illustrates the need to improve citizens' health privacy literacy. Further research is needed to understand the extent of this literacy issue, and to test different means for educating citizens of all ages to improve their health privacy literacy. This represents an important avenue for future research as individuals must be educated in order to make informed decisions which impact the privacy of their health data.

## **8.5 Summary**

Despite the limitations outlined in the previous section, the study makes several valuable contributions to the information privacy, technology adoption, and health informatics literature. These contributions include strong empirical support for the extension of a number of constructs to the health context including the adapted IPC measure of concern. Several relationships are empirically supported either in the quantitative or qualitative data including antecedents to HIPC, the HIPC-intention relationship, and moderating factors. The study extends Information Boundary theory, Protection Motivation theory, and the Privacy Calculus theory to provide a more comprehensive understanding of the impact of citizens' HIPC on their acceptance of EHRs and adoption of mHealth technologies. The final HIPC framework shows that individuals' boundary controls, threat and coping appraisals influence their HIPC, which together with perceived benefits influence technology adoption intentions. The HIPC framework represents a strong starting point for untangling the labyrinthine information privacy construct in the health context. This framework can be retested and developed further in future research. The insights from this study can be leveraged by health organisations, technology vendors, and government bodies charged with implementing new health technologies, in order to address citizens' HIPC and consequently increase their adoption.

## REFERENCES

- Ackerman, K. 2010. *Survey Finds Benefits of PHR Use, But Adoption Remains Low* [Online]. Available from: <http://www.ihealthbeat.org/insight/2010/survey-finds-benefits-of-phr-use-but-adoption-remains-low> [Accessed 10th January 2015].
- Acquisti, A. 2009. Nudging Privacy: The behavioural economics of personal information. *IEEE Security & Privacy Economics*, 7(6), pp. 82–85.
- Agaku, I.T., Adisa, A.O., Ayo-Yusuf, O.A. and Connolly, G. N. 2014. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association*, 21(2), pp. 374-378.
- Agarwal, R., Gao, G., DesRoches, C. and Jha, A.K. 2010. The Digital Transformation of Healthcare: Current Status and the Road Ahead. *Information Systems Research*, 21(4), pp. 796–809.
- Aggelidis, V.P. and Chatzoglou, P.D. 2009. Using a modified technology acceptance model in hospitals. *International Journal of Medical Informatics*, 78(2), pp. 115-126.
- Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 59(2), pp. 179–211.
- Ajzen, I. and Fishbein, M. 1977. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*, 84(5), pp. 888–918.
- Alavi, M., Kayworth, T.R. and Leidner, D.E. 2006. An Empirical Examination of the Influence of Organizational Culture on Knowledge Management Practices. *Journal of Management Information Systems* 22(3), pp. 191-224.
- Altman, I. 1975. *The environment and social behavior: privacy, personal space, territory, crowding*, Monterey, CA: Brooks/Cole.
- Altman, I. 1977. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33(3), pp. 66–84.
- Anderson, C.L. and Agarwal, R. 2011. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), pp. 469-490.
- Andrade, E.B., Kalthcheva, V. and Weitz, B. 2002. Self-Disclosure on the Web: The impact of Privacy Policy, Reward, and Company Reputation. *Advances in Consumer Research*, 29, pp. 350–354.
- Angst, C.M. 2006. Protect My Privacy or Support the Common-Good? Ethical Questions about Electronic Health Information Exchanges, *Journal of Business Ethics*, 90(2), pp. 169–178.
- Angst, C.M. and Agarwal, R. 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), pp. 339-370.
- Arizona State University 2015. *Employee trends by Campus* [Online]. Available from: <https://facts.asu.edu/Pages/Employees/Employee-Trends-by-Campus.aspx> [Accessed on 1<sup>st</sup> July 2015].

- Association for Information Systems 2011. *Senior Scholars' Basket of Journals* [Online]. Available from: <https://aisnet.org/?SeniorScholarBasket> [Accessed on 10<sup>th</sup> October 2014].
- Austin, L. 2003. Privacy and the Question of Technology. *Law and Philosophy*, 22(2), pp. 119–166.
- Avey, J.B., Avolio, B.J., Crossley, C.D. and Luthans, F. 2009. Psychological ownership: theoretical extensions, measurement and relation to work outcomes. *Journal of Organizational Behavior*, 30(2), pp. 173–191.
- Awad, N.F. and Krishnan, M.S. 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, pp. 13–28.
- Bandura, A. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2), pp. 191–215.
- Bandura, A. 1986. *Social foundations of thought and action: A social cognitive theory*, Englewood Cliffs, NJ: Prentice-Hall, Inc.
- Bansal, G., Zahedi, F.M. and Gefen, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), pp. 138–150.
- Baron, R. M. and Kenny, D. A. 1986. Moderator-Mediator Variables Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology*, 51(6), pp. 1173–82.
- Bélanger, F. and Crossler, R.E. 2011. Privacy in the Digital Age: A review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), pp. 1017–41.
- Bélanger, F., Hiller, J. S. and Smith, W. J. 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3), pp. 245–270.
- Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5), pp. 313–324.
- Bennani, A.E. and Oumlil, R. 2014. IT Acceptance by Nurses in Morocco: Application of a Modified Unified Theory of Acceptance and Use of Technology. *IBIMA Business Review*, pp.1–10.
- Bidmon, S., Terlutter, R. and Röttl, J. 2014. What explains usage of mobile physician-rating apps? Results from a web-based questionnaire. *Journal of Medical Internet Research*, 16(6), pp. e148.
- Björnberg, A. 2013. *Euro Health Consumer Index 2013* [Online]. Available from: <http://www.healthpowerhouse.com/files/ehci-2013/ehci-2013-report.pdf> [Accessed on 20<sup>th</sup> February 2014].
- Brown, M. and Muchira, R. 2004. Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research*, 5(1), pp. 62–70.
- Bryman, A. and Bell, E. 2007. *Business Research Methods*, Oxford, UK: Oxford University Press.

- Buchanan, T., Paine, C. and Joinson, A.N. 2007. Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), pp. 157–165.
- Caine, K. and Hanania, R. 2013. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association: JAMIA*, 20, pp. 7–15.
- Campos-Castillo, C. and Anthony, D.L. 2014. The double-edged sword of electronic health records: implications for patient disclosure. *Journal of the American Medical Informatics Association*, 22(e1), pp. e130-e140.
- Chang, I.C., Hwang, H.-G., Hung, W.F. and Li, Y.C. 2007. Physicians' acceptance of pharmacokinetics-based clinical decision support systems. *Expert Systems with Applications*, 33(2), pp. 296–303.
- Chau, P.Y. and Hu, P.J.H. 2002. Investigating healthcare professionals' decisions to accept telemedicine technology: an empirical test of competing theories. *Information & Management*, 39(4), pp. 297-311.
- Chellappa, R.K. and Sin, R.G. 2005. Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, 6(2-3), pp. 181–202.
- Chen, J., Zhang, Y. and Heath, R. 2001. An Exploratory Investigation of the Relationships Between Consumer Characteristics and Information Privacy, *Marketing Management Journal*, (11)1, pp. 73–81.
- Chen, K. and Rea, A.L. 2004. Protecting Personal Information Online: a survey of User privacy concerns and control techniques, *Journal of Computer Information Systems*, 44(4), pp. 85-92.
- Chen, R.F. and Hsiao, J.L. 2012. An investigation on physicians' acceptance of hospital information systems: a case study. *International Journal of Medical Informatics*, 81(12), pp. 810–20.
- Chhanabhai, P. and Holt, A. 2007. Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape general medicine*, 9(1), pp. 8.
- Cho, J. 2016. The impact of post-adoption beliefs on the continued use of health apps. *International Journal of Medical Informatics*, 87, pp. 75-83.
- Clarke, I., Flaherty, T.B., Hollis, S.M. and Tomallo, M. 2009. Consumer privacy issues associated with the use of electronic health records. *Academy of Health Care Management Journal*, 5(2), pp. 63–77.
- Clarke, R. 1999. Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*, 42(2), pp. 60–67.
- Compeau, D. and Higgins, C.A. 1995. Application of social cognitive theory to training for computer skills. *Information Systems Research*, 6(2), pp. 118–143.
- Compeau, D., Higgins, C.A. and Huff, S. 1999. Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study. *MIS Quarterly*, 23(2), pp. 145–158.

- Conboy, K., Fitzgerald, G. and Mathiassen, L. 2012. Qualitative Methods Research in Information Systems: Motivations, Themes, and Contributions. *European Journal of Information Systems*, 21(2), pp. 113-118.
- Conger, S., Pratt, J.H. and Loch, K.D. 2013. Personal information privacy and emerging technologies. *Information Systems Journal*, 23(5), pp. 401-417.
- Cook, T.D. and Campbell, D.T. 1979. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*, Boston: Houghton Mifflin Company.
- Corbin, J. and Strauss, A. 2008. *Basics of Qualitative Research: techniques and procedures for developing grounded theory*. 3rd ed. Thousand Oaks, CA: Sage Publications.
- Creswell, J.W. and Plano Clark, V. 2007. *Designing and Conducting Mixed Methods Research*, Thousand Oaks, CA: Sage.
- Creswell, J.W. 2003. *Research Design, Quantitative, Qualitative and Mixed Methods Approaches*. 2nd ed. Thousand Oaks, CA: Sage Publications.
- Culnan, B.M.J. 1993. 'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly*, pp. 341-364.
- Culnan, M.J. and Armstrong, P.K. 1999. Information Fairness, and Concerns, Trust: An Procedural Empirical Impersonal Investigation. *Organisational Science*, 10(1), pp. 104-115.
- Cunningham, S.M. 1967. The major dimensions of perceived risk. *Risk taking and information handling in consumer behaviour*, 1, pp. 82-108.
- Datta, L. 1994. Paradigm wars: A basis for peaceful coexistence and beyond. IN: Reichardt, C.S. and Rallis, S.F. (eds.) *The qualitative-quantitative debate: New perspectives*. San Francisco, CA: Jossey-Bass, pp. 53-70
- Davis, F.D. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, pp. 319-340.
- Davis, F.D. 1993. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, 38(3), pp. 475-487.
- Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. 1989. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 35(8), pp. 982-1003.
- Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. 1992. Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology*, 22(14), pp. 1111-1132.
- DeCew, J. 2002. *Privacy*. [Online]. Available from: <http://plato.stanford.edu/entries/privacy/> [Accessed on 13<sup>th</sup> October 2013].
- Department of Health 2013. *eHealth Strategy for Ireland*. [Online]. Available from: [http://health.gov.ie/wpcontent/uploads/2014/03/Ireland\\_eHealth\\_Strategy.pdf](http://health.gov.ie/wpcontent/uploads/2014/03/Ireland_eHealth_Strategy.pdf) [Accessed on 3<sup>rd</sup> January 2014].
- Djamasbi, S., Fruhling, A.L. and Loiacono, E.T. 2009. The influence of affect, attitude and usefulness in the acceptance of telemedicine systems. *Journal of Information Technology Theory and Application*, 10(1), pp. 41.

- Dillman, D.A. 2007. *Mail and internet surveys: the tailored design method*. 2nd ed, Hoboken, NJ: Wiley and Co.
- Dinesen, B., Nonnecke, B., Lindeman, D., Toft, E., Kidholm, K., Jethwani, K., Young, H.M., Spindler, H., Oestergaard, C.U., Southard, J.A. and Gutierrez, M. 2016. Personalized Telehealth in the Future: A Global Research Agenda. *Journal of medical Internet research*, 18(3), pp. e53.
- Dinev, T. and Hart, P. 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), pp. 413–422.
- Dinev, T., McConnell, A.R. and Smith, H.J. 2015. Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4), pp. 639-655.
- Dinev, T. 2014. Why would we care about privacy? *European Journal of Information Systems*, 23(2), pp. 97–102.
- Dinev, T. and Hart, P. 2006. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10(2), pp. 7–29.
- Dinev, T., Albano, V., Xu, H., D’Atroi, A. and Hart, P. 2016. Individuals’ Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective. IN: Gupta et al. (eds.) *Advances in Healthcare Informatics and Analytics, Annals of Information Systems 19*, Switzerland: Springer Publishing pp. 19-50.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. 2006. Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), pp. 389–402.
- Dinev, T., Xu, H., Smith, J.H. and Hart, P. 2012. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), pp. 295–316.
- Donaldson, T. and Dunfee, T. 1994. Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *Academy of Management Review*, 19(2), pp. 252–284.
- Earp, J.B., Antón, A.I., Member, S., Aiman-Smith, L. and Stufflebeam, W.H. 2005. Examining Internet Privacy Policies Within the Context of User Privacy Values. *IEEE Transactions on Engineering Management*, 52(2), pp. 227–237.
- Eastlick, M.A., Lotz, S.L. and Warrington, P. 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), pp. 877–886.
- Edney, J.J. and Buda, M.A. 1976. Distinguishing territoriality and privacy: Two studies. *Human Ecology*, 4(4), pp. 283–296.
- E-Estonia. 2014. *Electronic Health Record* [Online]. Available from: <http://e-estonia.com/component/electronic-health-record/> [Accessed on 12<sup>th</sup> February 2015].
- Eisenhardt, K.M. 1989. Agency theory: an assessment and review. *The Academy of Management Review*, 14(1), pp. 57–74.
- Eng, D.S. and Lee, J.M. 2013. The promise and peril of mobile health applications for diabetes and endocrinology. *Pediatric diabetes*, 14(4), pp. 231–8.

- Escobar-Rodríguez, T., Monge-Lozano, P. and Romero-Alonso, M.M. 2012. Acceptance of E-Prescriptions and Automated Medication-Management Systems in Hospitals: An Extension of the Technology Acceptance Model. *Journal of Information Systems*, 26(1), pp. 77–96.
- Eurobarometer 2011. *Attitudes on Data Protection and Electronic Identity in the European Union*, [Online]. Available from: [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf) [Accessed on 17<sup>th</sup> November 2013].
- European Commission. 2012. *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century* [Online]. Available from: [http://ec.europa.eu/health/ehealth/docs/com\\_2012\\_736\\_en.pdf](http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf) [Accessed on 1<sup>st</sup> December 2013].
- Evans, D., Nichol, P. and Perlin, J. 2006. Effect of the implementation of an enterprise-wide Electronic Health Record on productivity in the Veterans Health Administration. *Health Economics, Policy and Law*, 1(2), pp. 163–169.
- Featherman, M.S. and Pavlou, P.A. 2003. Predicting e-services adoption: a perceived risk Facets perspective. *International Journal of Human-Computer Studies*, 59, pp. 451–474.
- Fetter, M. 2009. Electronic health Records and Privacy. *Issues in Mental Health Nursing*, 30, pp. 408–409.
- Fichman, R.G., Kohli, R. and Krishnan, R. 2011. The role of information systems in healthcare: Current research and future trends. *Information Systems Research*, 22(3), pp. 419-428.
- Fischer, S.H., David, D., Crotty, B.H., Dierks, M. and Safran, C. 2014. Acceptance and use of health information technology by community-dwelling elders. *International Journal of Medical Informatics*, 83(9), pp. 624-635.
- Fishbein, M. and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research*, Reading, MA: Addison-Wesley.
- Flynn, H.A., Marcus, S.M., Kerber, K. and Alessi, N. 2003. Patients' concerns about and perceptions of electronic psychiatric records. *Psychiatric Services*, 54(11), pp. 1539–1541.
- Fornell, C. and Larcker, D. F. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, pp. 39-50.
- Fox, S. and Duggan, M. 2012. *Mobile Health* [Online]. Available from: [http://www.pewinternet.org/files/oldmedia//Files/Reports/2012/PIP\\_MobileHealth2012\\_FIN\\_AL.pdf](http://www.pewinternet.org/files/oldmedia//Files/Reports/2012/PIP_MobileHealth2012_FIN_AL.pdf) [Accessed on 13<sup>th</sup> March 2014].
- FTC. 2014. *Consumer Generated and Controlled Health Data* [Online]. Available from: [https://www.ftc.gov/system/files/documents/public\\_events/195411/privacyseries-healthdataagenda.pdf](https://www.ftc.gov/system/files/documents/public_events/195411/privacyseries-healthdataagenda.pdf). [Accessed on 15<sup>th</sup> May 2015].
- Gaskin, J. 2012a. *Data Screening* [Online]. Available from: [http://statwiki.kolobkreations.com/index.php?title=Data\\_screening](http://statwiki.kolobkreations.com/index.php?title=Data_screening) [Accessed on 10<sup>th</sup> July 2015].
- Gaskin, J. 2012b. *Confirmatory Factor Analysis* [Online]. Available from: [http://statwiki.kolobkreations.com/index.php?title=Confirmatory\\_Factor\\_Analysis](http://statwiki.kolobkreations.com/index.php?title=Confirmatory_Factor_Analysis) [Accessed on 11<sup>th</sup> July 2015].



- Gay, V. and Leijdekkers, P. 2015. Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability. *Journal of Medical Internet Research*, 17(11), pp. e260.
- George, D. and Mallery, M. 2010. *SPSS for Windows Step by Step: A Simple Guide and Reference*, Boston: Pearson.
- Gerety, T. 1977. Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review*, 12, pp. 233–296.
- Goodwin, C. 1991. Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing*, 10(1), pp. 149–166.
- Goodwin, L., Courtney, K., Kirby, D. and Iannacchione, M.A. 2002. A pilot study: Patients' perceptions about the privacy of their medical records. *Online Journal of Nursing Informatics*, 6(3).
- Greene, J.C. and Caracelli, V.J. 2003. Making Paradigmatic Sense of Mixed Methods Practice. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 91–110.
- Greenhalgh, T., Morris, L., Wyatt, J.C., Thomas, G. and Gunning, K. 2013. Introducing a nationally shared electronic patient record: Case study comparison of Scotland, England, Wales, and Northern Ireland. *International Journal of Medical Informatics*, 82, pp. 125–13
- Guo, X., Sun, Y., Wang, N., Peng, Z. and Yan, Z. 2013. The dark side of elderly acceptance of preventive mobile health services in China. *Electronic Markets*, 23(1), pp. 49–61.
- Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. 2010. *Multivariate Data Analysis, A Global Perspective*, New Jersey: Pearson Education.
- Han, S., Mustonen, P., Seppanen, M. and Kallio, M. 2006. Physicians' acceptance of mobile communication technology: an exploratory study. *International Journal of Mobile Communications*, 4(2), pp. 210–230.
- Harris Interactive and Westin, A.F. 2001. *The Harris Poll: #49*, Harris Interactive, Rochester, NY.
- Hennington, A.H. and Janz, B.D. 2007. Physician Adoption of Electronic Medical Records: Applying the UTAUT Model in a Healthcare Context. *Communications of the Association for Information Systems*, 19, pp. 60–80.
- Ho, S.Y. and Chau, P.Y. 2013. The effects of location personalization on integrity trust and integrity distrust in mobile merchants. *International Journal of Electronic Commerce*, 17(4), pp. 39–72.
- Hofstede, G. 2016. *Ireland in Comparison with United States* [Online]. Available from: <https://geert-hofstede.com/ireland.html> [Accessed on 14<sup>th</sup> May 2016].
- Holden, R.J. and Karsh, B.T. 2010. The technology acceptance model: its past and its future in health care. *Journal of Biomedical Informatics*, 43(1), pp. 159–72.
- Hong, W. and Thong, J. 2013. Internet Privacy Concerns: An Integrated Conceptualisation and four empirical studies. *MIS Quarterly*, 37(1), pp. 275–298.
- Hoy, M.G. and Milne, G. 2010. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, 10(2), pp. 28–45.

- Hsiao, C.-J. and Hing, E. 2014. *Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices: United States, 2001–2013*. NCHS Data Brief, (No. 124)1–8.
- Hsieh, P.J. 2015. Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk. *International Journal of Medical Informatics*, 84(1), pp.1-14.
- Hsu, C. 2006. Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. *Online Information Review*, 30(5), pp. 569–586.
- Hsu, C.L., Lee, M.R. and Su, C.H. 2013. The role of privacy protection in healthcare information systems adoption. *Journal of Medical Systems*, 37(5), pp. 1-12.
- Hu, P., Chau, P., Sheng, O. and Tam, K. 1999. Examining the technology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems*, 16(2), pp. 91–113.
- Hughes, K. 2012. A Behavioural Understanding of Privacy and its Implications for Privacy Law. *The Modern Law Review*, 75(5), pp. 806–836.
- Hung, S.Y., Tsai, J.C.A. and Chuang, C.C. 2014. Investigating primary health care nurses' intention to use information technology: An empirical study in Taiwan. *Decision Support Systems*, 57, pp. 331-342.
- Hwang, H.G., Han, H.E., Kuo, K.M. and Liu, C.F. 2012. The differing privacy concerns regarding exchanging electronic medical records of internet users in Taiwan. *Journal of medical systems*, 36(6), pp. 3783-3793.
- Ifinedo, P. 2012. Technology acceptance by health professionals in Canada: An analysis with a modified UTAUT model. *IN: System Science (HICSS), 45th Hawaii International Conference 4<sup>th</sup> January 2012 Hawaii*. IEEE, pp. 2937-2946.
- Janda, S. and Fair, L.L. 2004. Exploring Consumer Concerns Related to the Internet. *Journal of Internet Commerce*, 3(1), pp. 1–21.
- Järvinen, O.P. 2009. Privacy Management of Patient-Centered E-Health. *IN: Wilson, E.V. (ed.) Patient-Centered E-Health*, Hershey, PA: IGI Global, pp. 81–97.
- Jeng, D.J.F. and Tzeng, G.H. 2012. Social influence on the use of clinical decision support systems: revisiting the unified theory of acceptance and use of technology by the fuzzy DEMATEL technique. *Computers & Industrial Engineering*, 62(3), pp. 819-828.
- Jensen, C., Potts, C. and Jensen, C. 2005. Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2), pp. 203–227.
- Ji, P. and Lieber, P.S. 2010. Am I Safe? Exploring Relationships Between Primary Territories and Online Privacy. *Journal of Internet Commerce*, 9(1), pp. 3–22.
- Johnson, B. and Turner, L.A. 2003. Data Collection Strategies in Mixed Methods Research. *IN: Tashakkori, A. and Teddlie, C. (eds.) Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 297–319.
- Johnson, M.P., Zheng, K. and Padman, R. 2014. Modeling the longitudinality of user acceptance of technology with an evidence-adaptive clinical decision support system. *Decision Support Systems*, 57, pp. 444-453.

- Joinson, A., Reips, U.D., Buchanan, T. and Schofield, C.B.P. 2010. Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction*, 25(1), pp. 1–24.
- Jourard, S. 1964. Some Psychological Aspects of Privacy. *Law and Contemporary Problems*, 31, pp. 307–318.
- Junglas, I.A., Johnson, N.A. and Spitzmüller, C. 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), pp. 387–402.
- Karahanna, E., Straub, D.W. and Chervany, N.L. 1999. Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), pp. 183–213.
- Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B. and Greer, C. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, 71(12), pp. 1163–1173.
- Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C.P. and Abdullat, A. 2015. The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, 25(6), pp. 637–667.
- Kemper, E.A., Stringfield, S. and Teddlie, C. 2003. Mixed Methods Sampling Strategies in Social Science Research. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 273–319.
- Kerai, P., Wood, P. and Martin, M. 2014. A pilot study on the views of elderly regional Australians of personally controlled electronic health records. *International Journal of Medical Informatics*, 83, pp. 201–209.
- Kijsanayotin, B., Pannarunothai, S. and Speedie, S.M. 2009. Factors influencing health information technology adoption in Thailand's community health centers: applying the UTAUT model. *International Journal of Medical Informatics*, 78(6), pp. 404–16.
- Kim, D. and Chang, H. 2006. Key functional characteristics in designing and operating health information websites for user satisfaction: an application of the extended technology acceptance model. *International Journal of Medical Informatics*, 76(11-12), pp. 790–800.
- Kim, J. and Park, H.A. 2012. Development of a health information technology acceptance model using consumers' health behavior intention. *Journal of Medical Internet Research*, 14(5), pp. e133.
- King, T., Brankovic L. and Gillard, P. 2012. Perspectives of Australian adults about protecting the privacy of their health Information in statistical databases. *International Journal of Medical Informatics*, 81(4), pp. 279–89.
- Kitchenham, B. 2004. *Procedures for Performing Systematic Reviews*, Keele, UK, Keele University, 33, pp. 1-26.
- Klein, R. 2007. Internet-Based Patient-Physician Electronic Communication Applications: Patient Acceptance and Trust. *e-Service Journal*, 5(2), pp. 27–52.
- Kordzadeh, N., Warren, J. and Seifi, A. 2016. Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management*, 36, pp. 724-734.

- Korzaan, M.L. and Boswell, K.T. 2008. The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions. *Journal of Computer Information Systems*, 48(4), pp. 15–24.
- Kvale, S. 1996. The interview situation. IN Kvale, S. (ed.) *Interviews. An Introduction to Qualitative Research Interviewing*, London: Sage, pp. 124-143.
- Lafky, D.B. and Horan, T.A. 2011. Personal health records: Consumer attitudes toward privacy and security of their personal health information. *Health Informatics Journal*, 17(1), pp. 63–71.
- Lance, C.E., Dawson, B., Birkelbach, D. and Hoffman, B.J. 2010. Method effects, measurement error, and substantive conclusions. *Organizational Research Methods*, 13(3), pp. 435-455.
- Lanseng, E. and Andreassen, T. 2007. Electronic Healthcare: a study of people's readiness and attitude toward performing self-diagnosis. *International Journal of Service Industry Management*, 18(4), pp. 394–417.
- Laric, M.V., Pitta, D.A. and Katsanis, L. P. 2009. Consumer Concerns for Healthcare Information Privacy: A comparison of US and Canadian Perspectives. *Research in Healthcare Financial Management*, 12(1), pp. 93–111.
- Lasagna, L. 1964. *Hippocratic Oath, Modern version*. John Hopkins Sheridan Libraries [Online] Available from: <http://guides.library.jhu.edu/content.php?pid=23699&sid=190964> [Accessed on 22<sup>nd</sup> September 2014]
- Laufer, R. and Wolfe, M. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Development Theory. *Journal of Social Issues*, 33(3), pp. 22–42.
- Legris, P., Ingham, J. and Colletette, P. 2003. Why do people use information technology? A critical review of the technology acceptance model. *Information & Management*, 40(3), pp. 191–204.
- Li, H., Gupta, A. Zhang, J. and Sarathy, R. 2014. Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision Support Systems*, 57, pp. 376–386.
- Li, H., Sarathy, R. and Xu, H. 2010. Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), pp. 62–71.
- Li, H., Wu, J., Gao, Y. and Shi, Y. 2016. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, 88, pp. 8-17
- Li, J., Talaei-Khoei, A., Seale, H., Ray, P. and Macintyre, C.R. 2013. Health Care Provider Adoption of eHealth: Systematic Literature Review. *Interactive Journal of Medical Research*, 2(1), pp. e7.
- Li, T. and Slee, T. 2014. The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology*, 65(8), pp. 1541–1554.
- Li, Y. 2011. Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28(28), pp. 453– 496.
- Li, Y. 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), pp. 471–481.

- Lim, S., Xue, L., Yen, C.C., Chang, L., Chan, H.C., Tai, B.C. and Choolani, M. 2011. A study on Singaporean women's acceptance of using mobile phones to seek health information. *International Journal of Medical Informatics*, 80(12), pp. e189–202.
- Lincoln, Y.S. and Guba, E.G. 1986. But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, (30), pp. 73–84.
- Lincoln, Y.S. and Guba, E.G. 1985. *Naturalistic Inquiry*, Newbury Park, CA: Sage.
- Liu, C., Marchewka, J.T., Lu, J. and Yu, C.S. 2005. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, 42(2), pp. 289–304.
- Lwin, M., Wirtz, J. and Williams, J.D. 2007. Consumer Online Privacy Concerns and Responses: A Power– Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science*, 35(4), pp. 572–585.
- MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. 2011. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, 35(2), pp. 293–334.
- Malhotra, N.K., Kim, S.S. and Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale and a Causal Model. *Information Systems Research*, 15(4), pp. 336–355.
- Mandl, K.D., Szolovits, P. and Kohane, I.S. 2001. Public standards and patients' control: how to keep electronic medical records accessible but private. *British Medical Journal: BMJ*, 322(7281), pp. 283–287.
- Mason, R.O. 1986. Four Ethical Issues of the Information Age. *MIS Quarterly*, 10(1), pp. 5–12.
- Maxey, S.J. 2003. Pragmatic Threads in Mixed Methods Research in the Social Sciences: The search for Multiple models of inquiry and the end of the Philosophy of Formalism. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 51–90.
- Maxwell, J.A. 1992. Understanding and Validity in Qualitative Research. *Harvard Educational Review*, 62(3), pp. 279–300.
- Mays, N. and Pope, C. 2000. Assessing quality in qualitative research. *British Medical Journal: BMJ*, 320(7226), pp. 50–52.
- McKnight, D.H., Choudhury, V. and Kacmar, C. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), pp. 334–359.
- Metzger, M.J. 2007. Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, 12(2), pp. 1–27.
- Metzger, M.J. and Docter, S. 2003. Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting & Electronic Media*, 47(3), pp. 350–374.
- Milberg, S.J., Smith, H.J. and Burke, S.J. 2000. Information Privacy: Corporate Management and National Regulation. *Organization Science*, (11)1, pp. 35–57.
- Milne, G.R. and Gordon, M.E. 1993. Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework. *Journal of Public Policy & Marketing*, 12(2), pp. 206–215.

- Moore, A.D. 2003. Privacy: Its Meaning. *American Philosophical Quarterly*, 40(3), pp. 215–227.
- Moore, B. 1984. *Privacy: Studies in Social and Cultural history*. London: M.E. Sharpe.
- Moore, G.C. and Benbasat, I. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2(3), pp. 192–222.
- Moores, T.T. 2012. Towards an integrated model of IT acceptance in healthcare. *Decision Support Systems*, 53(3), pp. 507–516.
- Morris, M.G. and Venkatesh, V. 2000. Age differences in technology adoption decisions: Implications for a changing work force. *Personnel Psychology*, 53(2), pp. 375–403.
- Morse, J.M. 2003. Principles of Mixed Methods and MultiMethod Research Design. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 189–208.
- Morton, M.E. and Wiedenbeck, S. 2009. A framework for predicting EHR adoption attitudes: a physician survey. *Perspectives in Health Information Management*, 6, pp. 1a.
- Mosa, A.S.M., Yoo, I. and Sheets, L. 2012. A systematic review of healthcare applications for smartphones. *BMC Medical Informatics and Decision Making*, 12(67), pp. 1–31.
- Mottl, J. 2015. *Wearables primed for big growth, with Apple Watch driving adoption*, FierceMobile Healthcare [Online]. Available from: <http://www.fiercemobilehealthcare.com/story/reports-wearables-primed-big-growth-applewatch-driving-adoption/2015-02-22> [Accessed on 2<sup>nd</sup> February 2016].
- Nam, C., Song, C., Lee, E. and Park, C.I. 2006. Consumers' privacy concerns and willingness to provide marketing-related personal information online. IN: Pechman, C. and Price, L. (eds) *Advances in Consumer Research*, 33, pp. 212–217.
- Nehmad, E. and Fogel, J. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), pp. 153–160.
- Newell, P. 1995. Perspectives on Privacy. *Journal of Environmental Psychology*, 15(2), pp. 87–104.
- Newell, P. 1998. A Cross-Cultural Comparison of Privacy definitions and functions: A systems approach. *Journal of Environmental Psychology*, 18(4), pp. 357–371.
- Newman, I., Ridenour, C. S., Newman, C. and DeMarco, G.P J. 2003. A Typology of Research Purposes and Its Relationship to Mixed Methods. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 167–188.
- Nolan, A. and Kenny, A. 2014. *The Over 50s in a Changing Ireland: Economic Circumstances, Health and Well-Being. TILDA Wave Two Key Findings* [Online]. Available from: <http://tilda.tcd.ie/assets/pdf/Wave2-Key-Findings-Report.pdf> [Accessed on 1<sup>st</sup> March 2015].
- Norberg, P.A., Horne, D.R. and Horne, D.A. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1), pp. 100–126.

- O'Cathain A., Knowles, E., Turner, J., Maheswaran, R., Goodacre, S., Hirst, E. and Nicholl, J. 2014. Explaining variation in emergency admissions: a mixed methods study of emergency and urgent care systems. *Health Research and Services Delivery*, 2(48).
- O'Cathain, A., Murphy, E. and Nicholl, J., 2008. The quality of mixed methods studies in health services research. *Journal of Health Services Research & Policy*, 13(2), pp. 92-98.
- O'Cathain, A., Murphy, E. and Nicholl, J., 2010. Three techniques for integrating data in mixed methods studies. *British Medical Journal: BMJ*, 341, pp. 4587.
- OECD. 2015. *Health Expenditure and Financing* [Online]. Available from: [http://stats.oecd.org/index.aspx?DataSetCode=HEALTH\\_STAT](http://stats.oecd.org/index.aspx?DataSetCode=HEALTH_STAT) [Accessed on 12<sup>th</sup> March 2015].
- Okazaki, S., Li, H. and Hirose, M. 2009. Consumer Privacy Concerns and Preference for Degree of Regulatory Control. *Journal of Advertising*, 38(4), pp. 63–77.
- Or, C.K.L. and Karsh, B.T. 2009. A systematic review of patient acceptance of consumer health information technology. *Journal of the American Medical Informatics Association: JAMIA* 16(4), pp. 550–60.
- Or, C.K.L., Karsh, B.T. Severtson, D.J., Burke, L.J., Brown, R.L. and Brennan, P.F. 2011. Factors affecting home care patients' acceptance of a web-based interactive self-management technology. *Journal of the American Medical Informatics Association: JAMIA*, 18(1), pp. 51–9.
- Oxford English Dictionary. 2016. *Privacy* [Online]. Available from: <http://www.oxforddictionaries.com/definition/english/privacy> [Accessed on 2<sup>nd</sup> May 2016].
- Rust, R.T., Kannan, P.K. and Peng, N. 2002. The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30(4), pp. 455–464.
- Pai, F.Y. and Huang, K.I. 2011. Applying the technology acceptance model to the introduction of healthcare information systems. *Technological Forecasting and Social Change*, 78(4), pp. 650-660.
- Pavlou, P. 2011. State of the Information Privacy Literature: Where Are We Now and Where should we go? *MIS Quarterly*, 35(4), pp. 977–989.
- Pavlou, P.A., Liang, H. and Xue, Y. 2007. Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS Quarterly*, 31(1), pp. 105–136.
- Payton, F.C., Pare, G., Le Rouge, C.M. and Reddy, M. 2011. Health care IT: Process, people, patients and interdisciplinary considerations. *Journal of the Association for Information Systems*, 12(2), pp. 3.
- Perera, G., Holbrook, A., Thabane, L., Foster, G. and Willison, D. 2011. Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics*, 80(2), pp. 94–101.
- Petronio, S.S. 1991. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1(4), pp. 311–335.
- Pew Research Center. 2013. *Health Fact Sheet* [Online]. Available from: <http://www.pewinternet.org/fact-sheets/health-fact-sheet/> [Accessed on 11<sup>th</sup> August 2015].

- Phelps, J., D'Souza, G. and Nowak, G. 2001. Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), pp. 2–17.
- Phelps, J., Nowak, G. and Ferrell, E. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *American Marketing Association*, 19(1), pp. 27–41.
- Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, 88(5), pp. 879–903.
- Podsakoff, P.M. and Organ, D.W. 1986. Self-reports in organizational research: Problems and prospects. *Journal of Management*, 12(4), pp. 531–544.
- Podsakoff, P.M., MacKenzie, S.B. and Podsakoff, N.P. 2012. Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63, pp. 539–569.
- Poland, B.D. 1999. Transcription Quality as an Aspect of Rigour in Qualitative Research. *IN: Bryman, A. and Burgess R.G. (eds.) Qualitative Research: Volume III*, London: Sage, pp. 13–33.
- Posner, R. 1981. The Economics of Privacy. *Law and Economics with Imperfect Information*, 71(2), pp. 405–409.
- Powell, J., Fitton, R. and Fitton, C. 2006. Sharing electronic health records: the patient view. *Informatics in Primary Care*, 14(1), pp. 55–7.
- Preacher, K.J. and Hayes, A.F. 2004. SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, & Computers*, 36(4), pp. 717–731.
- Privacy Rights Clearinghouse 2013. *Mobile Health and Fitness Apps: What Are the Privacy Risks?* [Online]. Available from: <https://www.privacyrights.org/mobile-medical-apps-privacy-alert> [ Accessed on 2<sup>nd</sup> February 2014].
- Prosser, W. 1960. Privacy. *California Law Review*, 48(3), pp. 383–423.
- PWC 2013. *Socio-economic impact of mHealth. An assessment report for the European Union*, [Online]. Available from: [http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic\\_impactof-mHealth\\_EU\\_14062013V2.pdf](http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic_impactof-mHealth_EU_14062013V2.pdf) [Accessed on 1<sup>st</sup> February 2014].
- Pyper, C., Amery, J., Watson, M. and Crook, C. 2004. Patients' experiences when accessing their on-line electronic patient records in primary care. *British Journal of General Practice*, 54(498), pp. 38–43.
- Rahim, A., Ismail, Z. and Samy, G. N. 2013. Information Privacy Concerns in Electronic Healthcare Records: A Systematic Literature Review. *IN: Proceedings of the 3rd International Conference on Research and Innovation in Information Systems – 2013 (ICRIIS'13)*, 27<sup>th</sup> November Kuala Lumpur, IEEE, pp. 504–509.
- Rai, A., Chen, L., Pye, J. and Baird, A. 2013. Understanding determinants of consumer mobile health usage intentions, assimilation, and channel preferences. *Journal of Medical Internet Research*, 15(8), pp. e149.
- Raykov, T. 1997. Estimation of composite reliability for congeneric measures. *Applied Psychological Measurement*, 21(2), pp. 173–184.



- Regan, P.M., FitzGerald, G. and Balint, P. 2013. Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, 26(1-2), pp. 81–99.
- Ritchie, J. and Spencer, L. 1994. Qualitative data analysis for applied policy research. *IN: Bryman, A. and Burgess, R.G. (eds.) Analysing Qualitative Data*, London: Routledge, pp. 173–194.
- Robey, S. 2014. *10 Problems Electronic Health Records Can Help Solve* [Online]. Available from: <http://www.fool.com/investing/general/2014/07/19/10-problems-electronic-health-records-can-help-sol.aspx> [Accessed on 11<sup>th</sup> January 2015].
- Rogers, E. 1995. *Diffusion of Innovations*, New York: Free Press.
- Rogers, R.W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), pp. 93–114.
- Rogith, D., Yusuf, R.A., Hovick, S.R., Peterson, S.K., Burton-Chase, A.M., Li, Y., Meric-Bernstam, F. and Bernstam, E.V. 2014. Attitudes regarding privacy of genomic information in personalized cancer therapy. *Journal of the American Medical Informatics Association*, 21(e2), pp. e320-e325.
- Rohm, A.J. and Milne, G.R. 2004. Just what the doctor ordered The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, 57(9), pp. 1000–1011.
- Rongen, A., Robroek, S.J. and Burdorf, A. 2014. The importance of internal health beliefs for employees' participation in health promotion programs. *Preventive Medicine*, 67, pp. 330-334.
- Rust, R.T., Kannan, P.K. and Peng, N., 2002. The customer economics of Internet privacy. *Journal of the Academy of Marketing Science*, 30(4), pp. 455-464.
- Saigí-Rubió, F., Torrent-Sellens, J. and Jiménez-Zarco, A. 2014. Drivers of telemedicine use: comparative evidence from samples of Spanish, Colombian and Bolivian physicians. *Implementation Science: IS*, 9(1), pp. 128.
- Sarker, S., Xiao, X. and Beaulieu, T. 2013. Qualitative studies in information systems: a critical review and some guiding principles. *MIS Quarterly*, 37(4), pp. iii-xviii.
- Schaper, L.K. and Pervan, G.P. 2007. ICT and OTs: A model of information and communication technology acceptance and utilisation by occupational therapists. *International Journal of Medical Informatics*, 76, pp. S212-S221.
- SCIMago. 2011. *Journal Rankings: Health Informatics* [Online]. Available from: <http://www.scimagojr.com/journalrank.php?category=2718> [Accessed on 10<sup>th</sup> October 2014].
- Shadish, W.R., Cook, T.D. and Campbell, D.T. 2002. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Houghton, Mifflin and Company.
- Shaw, N.T., Kulkarni, A. and Mador, R.L. 2011. Patients and Health Care Providers' Concerns about the Privacy of Electronic Health Records: A Review of the Literature. *Electronic Journal of Health Informatics*, 6(1), pp. 1–5.
- Sheehan, K.B. and Hoy, M.G. 1998. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28(3), pp. 37–51.
- Sheehan, K.B. 1999. An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors. *Journal of Interactive Marketing*, (13)4, pp. 24–38.

- Sheehan, K.B. 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society*, 18(1), pp. 21-32.
- Shin, D.H. 2010. The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5), pp. 428-438.
- Simon, S.R., Evans, J.S., Benjamin, A., Delano, D. and Bates, D.W. 2009. Patients' attitudes toward electronic health information exchange: qualitative study. *Journal of Medical Internet Research*, 11(3), pp. e30.
- Sipior, J.C., Ward, B.T. and Connolly, R. 2013. Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, 26(6), pp. 661-678.
- Smith, H.J., Dinev, T. and Xu, H. 2011. Information privacy research: An Interdisciplinary review. *MIS Quarterly*, 35(4), pp. 989-1015.
- Smith, H.J., Milberg, S.J. and Burke, S.J. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, (20), pp. 167-196.
- Solove, D. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), pp. 477-564.
- Son, J. and Kim, S.S. 2008. Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, 32(3), pp. 503-529.
- Stewart, K. and Segars, A.H. 2002. An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), pp. 36-49.
- Stigler, G. 1980. An Introduction to Privacy in Economics and Politics. *The Journal of Legal Studies*, 9(4), pp. 623-644.
- Straub, D., Boudreau, M.C. and Gefen, D. 2004. Validation Guidelines for IS Positivist Research. *Communications of the AIS*, 13(24), pp. 380-427.
- Stutzman, F., Capra, R. and Thompson, J. 2011. Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27, pp. 590-598.
- Sun, Y., Wang, N., Guo, X. and Peng, Z. 2013. Understanding the acceptance of mobile health services: a comparison and integration of alternative models. *Journal of Electronic Commerce Research*, 14(2), pp. 183.
- Tashakkori, A. and Teddlie, C. 1998. *Mixed Methodology: Combining Qualitative and Quantitative Approaches*, Thousand Oaks, CA: Sage Publications.
- Tashakkori, A. and Teddlie, C. 2003. The Past and the Future of Mixed Methods Research: From 'Methodological Triangulation' to 'Mixed Methods Designs. *Handbook of Mixed Methods in Social and Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp.671-701.
- Tashakkori, A. and Teddlie, C. 2008. Quality of Inferences in Mixed Methods Research: Calling for an Integrative Framework. *IN: Bergman, M. (ed.) Advances in Mixed Methods Research: Theories and Applications*, London: Sage Publications, pp. 101-119.
- Tavares, J. and Oliveria, T. 2016. Electronic Health Record Patient Portal Adoption by Health Care Consumers: An Acceptance Model and Survey. *Journal of Medical Internet Research*, 18(3), pp. e49.

- Taylor, H. 2003. Most People Are “Privacy Pragmatists” Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. *The Harris poll*, pp. 1–6.
- Taylor, S. and Todd, P.A. 1995. Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), pp. 144-176.
- Teddlie, C. and Tashakkori, A. 2009. *Foundation of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. Thousand Oaks, CA: Sage Publications.
- Thompson, R.L., Higgins, C.A. and Howell, J.M. 1991. Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly*, 15(1), pp. 125–143.
- Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 22(2), pp. 254–268.
- Tsarenko, Y. and Tojib, D.R. 2009. Examining customer privacy concerns in dealings with financial institutions. *Journal of Consumer Marketing*, 26(7), pp. 468–476.
- Tung, F.C., Chang, S.C. and Chou, C.M. 2008. An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Informatics*, 77(5), pp. 324-335.
- U.S. Department of Health and Human Services. 2014. *More physicians and hospitals are using EHRs than before* [Online]. Available from: <http://www.hhs.gov/news/press/2014pres/08/20140807a.html> [Accessed on 10<sup>th</sup> March 2015].
- van Heerden, A., Norris, S., Tollman, S., Richter, L. and Rotheram-Borus, M.J. 2013. Collecting maternal health information from HIV-positive pregnant women using mobile phone-assisted face-to-face interviews in Southern Africa. *Journal of Medical Internet Research*, 15(6), pp. e116.
- Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), pp. 425–478.
- Venkatesh, V. and Davis, F.D. 2000. Theoretical Acceptance Extension Model: Field Four Studies of the Technology Longitudinal. *Management Science*, 46(2), pp. 186–204.
- Venkatesh, V. and Speier, C. 1999. Computer Technology Training in the Workplace: A Longitudinal Investigation of the Effect of Mood. *Organizational Behavior and Human Decision Processes*, 79(1), pp. 1–28.
- Venkatesh, V., Brown, S.A. and Bala, H. 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37, pp. 21-54.
- Venkatesh, V., Sykes, T. and Zhang, X. 2011. Just what the doctor Ordered: A Revised UTAUT for EMR System Adoption and Use by Doctors. IN: *Proceedings of the 44th Hawaii International Conference on System Sciences*, 4<sup>th</sup> January 2011 Hawaii, IEEE, pp.1–10.
- Vodicka, E., Mejilla, R., Leveille, S.G., Ralston, J.D., Darer, J.D., Delbanco, T., Walker, J. and Elmore, J.G. 2013. Online access to doctors' notes: patient concerns about privacy. *Journal of Medical Internet research*, 15(9), pp. e208.
- Walsham, G. 1995. Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems*, 4(2), pp. 74-81.

- Walter, Z. and Lopez, M.S. 2008. Physician acceptance of information technologies: Role of perceived threat to professional autonomy. *Decision Support Systems*, 46(1), pp. 206-215.
- Ward, S., Bridges, K. and Chitty, B. 2005. Do Incentives Matter? An Examination of OnLine Privacy Concerns and Willingness to Provide Personal and Financial Information. *Journal of Marketing Communications*, 11(1), pp. 21-40.
- Warren, S. and Brandeis, L. 1890. The Right to Privacy. *Harvard Law Review*, pp. 193-220.
- Westin, A. 1967. *Privacy and Freedom*, New York: Athenbaum.
- Westin, A. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), pp. 431-453.
- Westin, A. 2005. Public Attitudes Toward Electronic Health Records. *Privacy and American Business*, 12(2), pp. 2-6.
- White, T.B. 2004. Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, 14(1), pp. 41-51.
- Whittaker, R. 2012. Key Issues in Mobile Health and Implications for New Zealand. *Healthcare and Informatics Review Online*, 16(2), pp. 2-7.
- WHO 2015. *Definition of an older or elderly person* [Online]. Available from: <http://www.who.int/healthinfo/survey/ageingdefnolder/en/> [Accessed 1<sup>st</sup> June 2015].
- Williams, L.J., Cote, J.A. and Buckley, M.R. 1989. Lack of method variance in self-reported affect and perceptions at work: reality or artifact? *Journal of Applied Psychology*, 74(3), pp. 462.
- Wilson, V.E. and Lankton, N.L. 2004. Modeling Patients' Acceptance of Provider-delivered E-health. *Journal of the American Medical Informatics Association*, 11(4), pp. 241-249.
- Wirtz, J., Lwin, M.O. and Williams, J.D. 2007. Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4), pp. 326-348.
- Wu, I. L., Li, J.-Y. and Fu, C.Y. 2011. The adoption of mobile healthcare by hospital's professionals: An integrative perspective. *Decision Support Systems*, 51(3), pp. 587-596.
- Wu, J. H., Wang, S.C. and Lin, L. M. 2007. Mobile computing acceptance factors in the healthcare industry: a structural equation model. *International Journal of Medical Informatics*, 76(1), pp. 66-77.
- Xu, H., Dinev, T., Smith, J. and Hart, P. 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12), pp. 798-824.
- Xu, H., Teo, H.H. and Tan, B. 2005. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *IN: International Conference for Information Systems*, pp. 71.
- Yang, H. L. and Miao, X.M. 2008. Concern for Information Privacy and Intention to Transact Online. *IN: Proceedings of the 4<sup>th</sup> International Conference on Wireless Communications, Networking and Mobile Computing*: 1-4, Dalian, China, October, pp. 12-14.
- Yao, M.Z., Rice, R.E. and Wallis, K. 2007. Predicting User Concerns About Online Privacy. *Journal of the American Society for Information Science and Technology*, 58(5), pp. 710-722.

- Yao, M.Z. and Zhang, J. 2008. Predicting User Concerns About Online Privacy in Hong Kong. *CyberPsychology and Behavior* (11)6, pp. 779–781.
- Yarbrough, A.K. and Smith, T.B. 2007. Technology acceptance among physicians: a new take on TAM. *Medical Care Research and Review*, 64(6), pp. 650–72.
- Youn, S. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, (43)3, pp. 389– 418.
- Younger, K., 1972. Report of the Committee on Privacy to the UK Parliament, chaired by K. Younger, Cmnd 5012.
- Zhang, Y., Chen, J.Q. and Wen, K.W. 2002. Characteristics of Internet Users and Their Privacy Concerns—A Comparative Study Between China and the United States. *Journal of Internet Commerce*, (1)2, pp. 1–16.
- Zhao, X., Lynch, J.G. and Chen, Q. 2010. Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. *The Journal of Consumer Research*, 37(2), pp. 197-206.
- Zheng, S., Shi, K., Zeng, Z. and Lu, Q. 2010. The exploration of instrument of users' privacy concerns of Social Network Service. *IN: International Conference on Industrial Engineering and Engineering Management*, 7<sup>th</sup> December 2010, IEEE, pp. 1538–1542.

## APPENDIX A: HEALTH TECHNOLOGY ADOPTION STUDIES

Author	Type	Focus	Model	Variance	Findings
Kijsanayotin, Pannarunothai and Speedie (2009)	HIT acceptance health centres in Thailand	Healthcare employees	UTAUT + previous IT experience	50%: intentions 27%: actual use	Performance Expectancy (PE), Effort Expectancy (EE), Voluntariness and Social Influence (SI) Intention, previous IT experience & social influence
Schaper and Pervan (2007)	Quantitative - Australia	Occupational therapists	UTAUT + computer anxiety, self-efficacy, attitude, compatibility	Intention	Compatibility & EE influencing PE, SI & computer attitude not significant
Venkatesh, Sykes, and Zhang (2011)	US EHR adoption	Physicians	Modified UTAUT	44% intention 47% in use	Age – key moderator EE remained significant over time
Chang <i>et al.</i> , (2007)	Clinical Decision Support Systems (CDSS) adoption in Taiwan	Physicians	UTAUT	43% intention 28% in usage	PE, EE, social influence and facilitating conditions Intention influenced use
Bennani and Oumlil (2014)	HIT acceptance in Morocco	Nurses	UTAUT + trust	Intention	PE nor EE significant Social influence and trust significant
Willis <i>et al.</i> , (2008)	EHR	Nurses	UTAUT	51%: Intention 28% use	Social influence had greatest impact, then PE, facilitating conditions and EE
Aggelidis and Chatzoglou (2009)	HIT acceptance in Greek hospital	Healthcare professionals	UTAUT	Intention	EE, PE, social influence and facilitating conditions all significant
Jeng and Tzeng (2012)	CDSS	Healthcare professionals	UTAUT	Intention	PE significant Social influence insignificant
Ifinedo (2012)	HIT acceptance in Canada	Healthcare professionals	UTAUT + compatibility	Intention	EE, social influence and facilitating conditions significant PE insignificant
Han <i>et al.</i> , (2006)	Mobile HIT in Finland	Physicians	TAM + Social influence, compatibility, personal innovativeness in terms of IT (PIIT)	74%: Intentions	Perceived Usefulness (PU) strongest influence on intention. Perceived Ease of Use (PEOU) and SI also significant on intention. Compatibility did not significantly influence intention
Chen and Hsiao (2012)	HIT in Taiwan	Physicians	TAM + self-efficacy, compatibility, support from top-management	PU and PEOU explained 81.4% of Intention	PU & PEOU significant on influence – PEOU greater influence, PU influenced most by top management support, PEOU influenced by competency of the project team and system quality

Author	Type	Focus	Model	Variance	Findings
Escobar-Rodriguez <i>et al.</i> , (2012)	E-prescription acceptance in a Spanish hospital	91 physicians 118 nurses	TAM + perceived compatibility, perceived usefulness to reduce errors, training perceived risk	Intention	PU significantly influenced intention PEOU significantly influence PU but not intention PU to prevent errors influenced intention
Morton and Wiedenback (2009)	EHR adoption in a Mississippi academic health centre	Physicians	TAM	73%: Attitude	Att influenced most by PU and physician involvement, PEOU and doctor-patient relationship PU influenced by PEOU and negatively by doctor-patient relationship
Chau and Hu (2002)	Telemedicine use in 41 departments in 8 hospitals	Healthcare professionals	TAM, TPB, and Combined	TAM: 42% TPB: 37% Combined: 40%	TAM: intention influenced by ATT and PU TPB: attitude and PBC influence intention
Johnson <i>et al.</i> , (2014).	CDSS acceptance in Pennsylvania hospital	44 Medical residents	TAM, optimism towards the technology, computer experience	N/A	PEOU strongly predicated self-reported use & satisfaction Neither PU nor PEOU influenced initial use PU did not influence self-reported or actual use
Walter and Lopez (2008)	EHRs and CDSS	Physicians	TAM + perceived threat to professional autonomy	N/A	Perceived threat to professional autonomy negatively influenced PU and intention in both technologies but was stronger for intention in EHRs. PU and PEOU much less positively influenced intention PEOU positively influenced PU
Moore (2012)	HIT acceptance in Greek hospital	Nurses and physicians	TAM + depth and breadth of use, attitude towards use, compatibility	N/A	Use was not significantly influenced by attitude, PU, PEOU or compatibility Argued that acceptance is influenced by information quality and personal enabling factors
Pai and Huang (2011)	HIT acceptance	Healthcare professionals	TAM + system quality, service quality and information quality variables	N/A	PEOU influenced intention most then PU Service and information quality influence PU and PEOU PEOU also influences PU
Hu <i>et al.</i> , (1999)	Telemedicine in Hong Kong	Physicians	TAM	44%: Intention	PU & PEOU influenced attitude Att & PU influenced intention

Author	Type	Focus	Model	Variance	Findings
Saigí-Rubió <i>et al.</i> , (2014)	Telemedicine in Columbia, Bolivia and Spain	Physicians	TAM + individual and environmental factors, technology readiness, ICT implementation in the country	Spain: 72.9% Columbia: 62.6% Bolivia: 57.6%	Use in Spain: propensity to innovate and PEOU of ICT Columbia and Bolivia: ICT use in personal life, optimism about ICTs, but not by PEOU of ICTs nor propensity to innovate
Djamasbi and Fruhling (2009)	Telemedicine	Healthcare professionals (39 lab assistants)	TAM + affect	61%: Intention	PEOU influenced PU PU was significant predictor of attitude but PEOU was not. Positive or negative affect influence attitude. PU & attitude influence intention
Tung <i>et al.</i> (2008)	Electronic logistics system in Taiwan	Nurses	TAM + compatibility and trust	70%: Intention	PU, PEOU, compatibility, trust and perceived financial costs influence intention PEOU and trust influenced PU
Wu <i>et al.</i> , (2007)	MHS acceptance in healthcare (Taiwan)	Healthcare professionals (physicians, nurses and technicians)	TAM + compatibility, MHS self-efficacy, training	70%: Intention	PU, PEOU & compatibility significantly influence intention, PEOU & compatibility influence PU. Compatibility also influences PEOU & self-efficacy Training influenced self-efficacy
Wu <i>et al.</i> , (2011)	Mobile healthcare in Taiwan	Healthcare professionals	TAM + TPB + personal innovativeness in IT (PIIT), perceived service availability	63%: Intention	PU influenced attitude but PEOU did not PU & ATT, SN & PBC influenced intention PIIT significantly influenced PBC but not attitude. Perceived service availability significantly influenced PU but not PEOU
Hsieh (2015)	EHRs in Taiwan	Physicians	TPB+ trust, financial, performance, psychological and privacy risk	49%: Intention	Intention predicted by attitude, SN & PBC most Trust influenced risk perception & intention Privacy risk related to trust
Hung <i>et al.</i> , (2014)	Taiwan	Nurses	TRA + three-layer framework by Chau and Hu	57%: Intention	Intention influenced by attitude & social influence Attitude influenced by PU, perceived trust & SI
Malliet <i>et al.</i> , (2014)	EHR use in 4 acute care academic settings	Nurses	UTAUT + actual usage, satisfaction	54.9% of variance in acceptance and use	PE to attitude was strongest self-efficacy was not significant EE influence PE but not attitude Facilitating conditions significantly influenced EE SI significantly influenced intention.



## APPENDIX B: SYSTEMATIC LITERATURE REVIEW

### SEARCH TERMS

#	Model	Context	Focus	Privacy
1	Technology Adoption	& Health	& Patient OR Citizen	-
2	Theory of Reasoned Action	& Health	& Patient OR Citizen	-
3	Technology Acceptance Model	& Health	& Patient OR Citizen	-
4	Theory of Planned Behaviour	& Health	& Patient OR Citizen	-
5	Motivation Model	& Health	& Patient OR Citizen	-
6	Innovation Diffusion Model	& Health	& Patient OR Citizen	-
7	Social Cognitive Theory	& Health	& Patient OR Citizen	-
8	Model of Personal Computer Utilisation	& Health	& Patient OR Citizen	-
9	Unified Theory of Technology Acceptance and Adoption	& Health	& Patient OR Citizen	-
10	Privacy Calculus Theory	& Health	& Patient OR Citizen	-
11	TRA	& Health	& Patient OR Citizen	-
12	TAM	& Health	& Patient OR Citizen	-
13	TAM	& Health	& Patient OR Citizen	-
14	TPB	& Health	& Patient OR Citizen	-
15	MM	& Health	& Patient OR Citizen	-
16	IDT	& Health	& Patient OR Citizen	-
17	SCT	& Health	& Patient OR Citizen	-
18	UTAUT	& Health	& Patient OR Citizen	-
19	Technology Adoption	& Health	& Patient OR Citizen	& Privacy
20	Theory of Reasoned Action	& Health	& Patient OR Citizen	& Privacy
21	Technology Acceptance Model	& Health	& Patient OR Citizen	& Privacy
22	Theory of Planned Behaviour	& Health	& Patient OR Citizen	& Privacy
23	Motivation Model	& Health	& Patient OR Citizen	& Privacy
24	Innovation Diffusion Model	& Health	& Patient OR Citizen	& Privacy
25	Social Cognitive Theory	& Health	& Patient OR Citizen	& Privacy
26	Model of Personal Computer Utilisation	& Health	& Patient OR Citizen	& Privacy
27	Unified Theory of Technology Acceptance and Adoption	& Health	& Patient OR Citizen	& Privacy
28	Privacy Calculus Theory	& Health	& Patient OR Citizen	& Privacy
29	TRA	& Health	& Patient OR Citizen	& Privacy
30	TAM	& Health	& Patient OR Citizen	& Privacy
31	TAM	& Health	& Patient OR Citizen	& Privacy
32	TPB	& Health	& Patient OR Citizen	& Privacy
33	MM	& Health	& Patient OR Citizen	& Privacy
34	IDT	& Health	& Patient OR Citizen	& Privacy
35	SCT	& Health	& Patient OR Citizen	& Privacy
36	UTAUT	& Health	& Patient OR Citizen	& Privacy

## **APPENDIX C: SYSTEMATIC LITERATURE REVIEW: JOURNALS**

### **MIS Journals**

- European Journal of Information Systems
- Information Systems Journal
- Information Systems Research
- Journal of AIS
- Journal of Information Technology
- Journal of MIS
- Journal of Strategic Information Systems
- MIS Quarterly

Source: Association for Information Systems, 2011

### **Health Informatics Journals**

1. Implementation Science
2. Medical Image Analysis
3. Journal of the American Medical Informatics Association: JAMIA
4. BMC Medical Research Methodology
5. Journal of Medical Internet Research
6. Journal of Biomedical Informatics
7. Journal of NeuroEngineering and Rehabilitation
8. Computer Methods and Programs in Biomedicine
9. International Journal of Medical Informatics
10. Journal of Medical Systems
11. Journal of Telemedicine and Telecare
12. Journal of the Medical Library Association: JMLA
13. Journal of Clinical Bioinformatics

(SCImago, 2011)

## APPENDIX D: ETHICAL APPROVAL LETTER

Ollscoil Chathair Bhaile Átha Cliath  
Dublin City University



9<sup>th</sup> April 2015

**Dr Regina Connolly**  
**DCU Business School**

**REC Reference:** DCUREC/2015/045

**Proposal Title:** An Examination of the Influence of Citizens' Health Information Privacy Concerns on their Acceptance and Adoption of Health ICTs

**Applicant(s):** Dr Regina Connolly ; Ms Grace Kenny ;

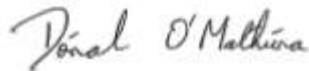
Dear Regina,

Further to Expedited Review, the DCU Research Ethics Committee approves this research proposal.

Materials used to recruit participants should note that ethical approval for this project has been obtained from the Dublin City University Research Ethics Committee.

Should substantial modifications to the research protocol be required at a later stage, a further submission should be made to the REC.

Yours sincerely,

A handwritten signature in dark ink, reading 'Dónal O'Mathúna'.

**Dr Dónal O'Mathúna**  
Chairperson  
DCU Research Ethics Committee



## APPENDIX E: SURVEY INVITATION EXAMPLE

### Health Information Privacy Concerns Survey

Dear Participant,

You are invited to participate in a PhD Study conducted by Grace Kenny from Dublin City University in Ireland. This study explores individuals' concerns related to the collection, storage, and use of their physical and mental health information using technology. The research has received IRB approval from Dublin City University and is supported by the ASU-DCU Transatlantic Partnership.

Participation in this research involves completing a survey which will take approximately 10 to 15 minutes of your time. The questions relate to your experience using the Internet and health technologies, your privacy experiences and your health information privacy concerns. The survey can be accessed through the link at the bottom of this email. Participation is extremely appreciated and completely voluntary. All information you provide will be anonymous. Data will be stored securely and disposed of in 18 months.

Survey Link:

[https://qtrial2015az1.az1.qualtrics.com/SE/?SID=SV\\_0HTnQGtsmBjb4eF](https://qtrial2015az1.az1.qualtrics.com/SE/?SID=SV_0HTnQGtsmBjb4eF)

If you are interested in the findings of the study or have any questions, please email the researcher at: [grace.kenny@asu.edu](mailto:grace.kenny@asu.edu)

Thank you in advance for your participation!



Ollscoil Chathair Bhaile Átha Cliath  
Dublin City University



## APPENDIX F: SURVEY INSTRUMENT

### Citizen Health Information Privacy Concern Survey: Irish Sample

You are invited to participate in a PhD Study conducted by Grace Kenny from Dublin City University's Business School. This research is supported by the ASU-DCU Transatlantic Partnership and has been approved by the DCU Research Ethics Committee. This study examines individual's concerns regarding the collection, storage, and use of their personal health information via technology.

**What are we asking you to do?** Participation in this research involves completing a survey. The survey consists of 6 sections and will take approximately 15 minutes to complete.

**How is your information protected?** The responses and information you provide will be anonymous. Data will only be seen by the researcher and will be stored **securely**. However, if anything comes to light that shows you are in danger, we are legally obliged to report it. Participation in the survey is voluntary and you can choose not to participate or to withdraw your participation at any time. All responses will be securely disposed of in 18 months.

**Additional Information:** If you are interested in the findings of the study or have questions, you can email the researcher [grace.kenny2@mail.dcu.ie](mailto:grace.kenny2@mail.dcu.ie). For more information on the ASU-DCU Transatlantic Partnership, please visit: <https://dcu.asu.edu/>

**If participants have concerns about this study and wish to contact an independent person, please contact:**

The Secretary,  
Dublin City University Research Ethics Committee,  
c/o Research and Innovation Support,  
Dublin City University, Dublin 9. Tel 01-7008000

**Project supported by:**

**DCU O'Hare Research Scholarship**

**ASU-DCU Catalyst Fund**

## I: TECHNOLOGY EXPERIENCE

1. Approximately how long have you been using the Internet?

<i>Less than 1 year</i>	<i>1 - 5 years</i>	<i>5-10 years</i>	<i>10-15 years</i>	<i>&gt;15 years</i>

2. Which of the following technologies do you use to access the Internet? (Please tick all that apply)

Personal Computer (PC) ☐

Laptop ☐

Smartphone/ mobile phone ☐

Tablet ☐

Other, please specify: \_\_\_\_\_

***Please circle the number that indicates how often you engage in each of the following Internet activities.***

		<i>Never</i>	<i>Once a month or less</i>	<i>2-3 times a month</i>	<i>1-3 times a week</i>	<i>4 times a week - Every day</i>
<b>3</b>	I use the Internet for personal purposes (e.g. email, social networking)	1	2	3	4	5
<b>4</b>	I use the Internet for work or study purposes	1	2	3	4	5
<b>5</b>	I search online for information related to disease diagnosis and treatment	1	2	3	4	5
<b>6</b>	I search online for information related to health management (exercise, diet, mental health, etc.)	1	2	3	4	5
<b>7</b>	I search online for health information for education, research or learning purposes	1	2	3	4	5
<b>8</b>	I purchase health products such as health food and medical equipment online	1	2	3	4	5
<b>9</b>	I use social media (e.g. Facebook, Twitter) as a source of health information	1	2	3	4	5

**Please circle the number that indicates how often you use each type of mobile health application.**

		<i>Never</i>	<i>Once a month or less</i>	<i>2-3 times a month</i>	<i>1-3 times a week</i>	<i>4 times a week - Every day</i>
<b>10</b>	Exercise or fitness applications	1	2	3	4	5
<b>11</b>	Diet, food, or calorie tracking applications	1	2	3	4	5
<b>12</b>	Blood pressure monitoring applications	1	2	3	4	5
<b>13</b>	Applications related to pregnancy	1	2	3	4	5
<b>14</b>	Diabetes applications	1	2	3	4	5
<b>15</b>	Medication management applications	1	2	3	4	5
<b>16</b>	Sleep tracking applications	1	2	3	4	5
<b>17</b>	Mood monitoring applications	1	2	3	4	5
<b>18</b>	Health information applications (e.g. WebMD)	1	2	3	4	5

**Please circle the number that indicates how often you use each of the following health technologies.**

		<i>Never</i>	<i>Once a month or less</i>	<i>2-3 times a month</i>	<i>1-3 times a week</i>	<i>4 times a week - Every day</i>
<b>19</b>	Health Monitoring Devices (e.g. FitBit, Jawbone, Heart rate monitor)	1	2	3	4	5
<b>20</b>	Personal Health Record systems (e.g. Microsoft Healthvault)	1	2	3	4	5

## II: PRIVACY EXPERIENCE

**For each statement, please circle the number that best describes your experience.**

		<i>Never</i>	<i>Once</i>	<i>Rarely</i>	<i>Often</i>	<i>Very often</i>
<b>1</b>	In the past, the privacy of my personal information (e.g. demographical, financial) has been invaded	1	2	3	4	5
<b>2</b>	In the past, the privacy of my personal <b>health</b> information (e.g. medication, health history) has been invaded	1	2	3	4	5

Over the last year, how often have you heard or read about the <b>potential misuse</b> of:		<i>Never</i>	<i>Once</i>	<i>Rarely</i>	<i>Often</i>	<i>Very often</i>
<b>3</b>	Individuals' <b>personal</b> information (e.g. demographical, financial)	1	2	3	4	5
<b>4</b>	Individuals' <b>health</b> information (e.g. medication, health history)	1	2	3	4	5

***For each option, please circle the number that best describes your knowledge.***

How would you describe your knowledge of your <b>privacy rights</b> regarding:		<i>None</i>	<i>Very little</i>	<i>Average</i>	<i>Quite extensive</i>	<i>Very extensive</i>
<b>5</b>	Your personal information (e.g. Data Protection Acts, 1988, 2003)	1	2	3	4	5
<b>6</b>	Your health information	1	2	3	4	5

***Based on your experience with health professionals (doctors, nurses, pharmacists etc.), please circle the number that indicates your level of agreement with each statement.***

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>7</b>	I know health professionals are <b>always</b> honest when it comes to using my health information	1	2	3	4	5
<b>8</b>	I know health professionals care about patients	1	2	3	4	5
<b>9</b>	I know health professionals are <b>not</b> opportunistic when using my health information	1	2	3	4	5
<b>10</b>	I know health professionals are predictable and consistent with regards to using my health information	1	2	3	4	5
<b>11</b>	I know health professionals are competent and effective in providing their services	1	2	3	4	5
<b>12</b>	I trust that health professionals keep my best interests in mind when dealing with my health information	1	2	3	4	5



		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>13</b>	It would be risky to disclose my personal health information to health professionals	1	2	3	4	5
<b>14</b>	There would be high potential for loss associated with disclosing my personal health information to health professionals	1	2	3	4	5
<b>15</b>	There would be too much uncertainty associated with giving my personal health information to health professionals	1	2	3	4	5
<b>16</b>	Providing health professionals with my personal health information would involve many unexpected problems	1	2	3	4	5

***Based on your experience with technology vendors (e.g. websites, mobile applications) for all purposes (including but not limited to health), circle the number that indicates your level of agreement with each statement.***

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>17</b>	I know technology vendors are <b>always</b> honest when it comes to using my health information	1	2	3	4	5
<b>18</b>	I know technology vendors care about customers	1	2	3	4	5
<b>19</b>	I know technology vendors are <b>not</b> opportunistic when using my health information	1	2	3	4	5
<b>20</b>	I know technology vendors are predictable and consistent with regards to using my health information	1	2	3	4	5
<b>21</b>	I know technology vendors are competent and effective in providing their services	1	2	3	4	5
<b>22</b>	I trust that technology vendors keep my best interests in mind when dealing with my health information	1	2	3	4	5

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>23</b>	It would be risky to disclose my personal health information to technology vendors	1	2	3	4	5
<b>24</b>	There would be high potential for loss associated with disclosing my personal health information to technology vendors	1	2	3	4	5
<b>25</b>	There would be too much uncertainty associated with giving my personal health information to technology vendors	1	2	3	4	5
<b>26</b>	Providing technology vendors with my personal health information would involve many unexpected problems	1	2	3	4	5

### III: HEALTH EXPERIENCE

*The next questions relate to your personal health, and information related to your health.*

		<i>None</i>	<i>1 - 2</i>	<i>3-5</i>	<i>6-10</i>	<i>10 +</i>	<i>Rather not say</i>
<b>1</b>	How many face-to-face visits have you had with health professionals in the past 6 months? (including doctor's visits, hospital visits, physical therapy, lab tests)						
<b>2</b>	How many different healthcare providers (doctors, specialists etc.) have you seen in the last six months?						
<b>3</b>	How many prescription medications are you taking for chronic or long-term health problems?						

*Please circle the number that indicates your level of agreement with each statement.*

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly Agree</i>
<b>4</b>	I experience major pains and discomfort for extended periods of time	1	2	3	4	5
<b>5</b>	When it comes to chronic condition, I believe that my condition is severe	1	2	3	4	5

6. In general, how would you rate your **overall health**?

Excellent ☐      Very good ☐      Good ☐      Fair ☐      Poor ☐

7. Do you have any **chronic** illnesses (asthma, diabetes, coronary heart disease, inflammatory bowel disease etc.)?

Yes ☐      No ☐      I don't know ☐

*If yes, please circle the option below that best indicates your experience.*

		<i>Never</i>	<i>Once</i>	<i>Rarely</i>	<i>Often</i>	<i>Very often</i>
<b>8</b>	I have been <b>treated differently</b> or <b>discriminated</b> against by people who know about my chronic illness.	1	2	3	4	5

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>9</b>	I worry that I would be <b>treated differently</b> or be <b>discriminated</b> against if others knew about my chronic illness	1	2	3	4	5

10. Do you have any **sensitive** illnesses (any condition you **feel is private or embarrassing**)?

Yes ☐      No ☐

*If yes, please circle the option below that best indicates your experience.*

		<i>Never</i>	<i>Once</i>	<i>Rarely</i>	<i>Often</i>	<i>Very often</i>
<b>11</b>	I have been <b>treated differently</b> or <b>discriminated</b> against by people who know about my sensitive illness.	1	2	3	4	5

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>12</b>	I worry that I would be <b>treated differently</b> or be <b>discriminated</b> against if others knew about my sensitive illness	1	2	3	4	5

**13:** Do you have any **other conditions/illnesses** that periodically impact your life?

Yes

☐

No

☐

**For each type of health information, circle the number that indicates how sensitive you feel this information is.**

		<i>Not sensitive at all</i>	<i>Slightly sensitive</i>	<i>Neither</i>	<i>Very sensitive</i>	<i>Extremely Sensitive</i>
<b>14.</b>	Contact and demographic details (address, phone, age, gender, race)	1	2	3	4	5
<b>15.</b>	Information related to current health status (chronic and other illnesses, symptoms)	1	2	3	4	5
<b>16.</b>	Information related to your fitness at present	1	2	3	4	5
<b>17.</b>	Medications (including medications prescribed to you and over the counter medications)	1	2	3	4	5
<b>18.</b>	Recent test results (blood pressure, colonoscopy, cholesterol test, mammogram, prostate screening)	1	2	3	4	5
<b>19.</b>	Health history (previous illnesses and injuries)	1	2	3	4	5
<b>20.</b>	Mental health information (psychiatric diagnosis, suicide attempts, eating disorder, depression)	1	2	3	4	5
<b>21.</b>	Sexual health information (sexually transmitted diseases including HIV)	1	2	3	4	5
<b>22.</b>	Domestic abuse records (fear of partner, suspicious physical injury)	1	2	3	4	5
<b>23.</b>	Genetic information (paternity tests, genetic tests)	1	2	3	4	5
<b>24.</b>	Plastic surgery (rhinoplasty, liposuction, face lift etc.)	1	2	3	4	5
<b>25.</b>	Reproductive health information (infertility, miscarriages, abortion)	1	2	3	4	5
<b>26.</b>	Information pertaining to addiction	1	2	3	4	5

***Please circle the number that indicates your level of agreement with each statement.***

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>27.</b>	I feel that information related to my health should be kept between myself and my doctor	1	2	3	4	5
<b>28.</b>	I feel a very high degree of ownership over information related to my health	1	2	3	4	5
<b>29.</b>	Information related to my health should be shared with other health professionals	1	2	3	4	5
<b>30.</b>	I feel that information related to my health defines who I am	1	2	3	4	5
<b>31.</b>	Information related to my health should be shared with my family	1	2	3	4	5
<b>32.</b>	I feel that information related to my health belongs to me	1	2	3	4	5
<b>33.</b>	Information related to my health should be shared with other parties (e.g. my employer, government)	1	2	3	4	5

#### IV: HEALTH INFORMATION PRIVACY CONCERN

**This section includes questions related to your privacy concern regarding your health information. In this section, Health care entities include BOTH health professionals AND health technology vendors that may request/collect information related to your physical and mental health.** Please circle the number that indicates your level of agreement with each statement (1 = strongly disagree, 7= strongly agree).

	Information Collection and Use	<i>Strongly Disagree – Strongly Agree</i>						
1.	It usually bothers me when health care entities ask me for personal health information	1	2	3	4	5	6	7
2.	I am concerned that when I give personal health information to a healthcare entity for some reason, that they might use the information for other reasons	1	2	3	4	5	6	7
3.	It bothers me to give my personal health information to so many health care entities	1	2	3	4	5	6	7
4.	It usually bothers me when I am not aware or knowledgeable about how my personal health information will be used by health care entities	1	2	3	4	5	6	7
5.	It usually bothers me when I do not have control of personal health information that I provide to health care entities	1	2	3	4	5	6	7
6.	I am concerned when control is lost or unwillingly reduced as a result of providing health care entities with my personal health information	1	2	3	4	5	6	7
7.	When health care entities ask me for personal health information, I sometimes think twice before providing it	1	2	3	4	5	6	7
8.	I am concerned that health care entities would sell my health personal health information in their computer databases to other health care entities or non-health related organisations	1	2	3	4	5	6	7
9.	It is very important to me that I am aware and knowledgeable about how my personal health information will be used by health care entities	1	2	3	4	5	6	7
10.	It usually bothers me when I do not have control or autonomy over decisions about how my personal health information is used, and shared by health care entities	1	2	3	4	5	6	7
11.	I'm concerned that health care entities are collecting too much personal health information about me	1	2	3	4	5	6	7
12.	It usually bothers me when health care entities seeking my health information do not disclose the way the data are processed and used	1	2	3	4	5	6	7

	Protection and Accuracy	Strongly Disagree – Strongly Agree						
13	I am concerned that health care entities do not take enough steps to make sure that unauthorised people cannot access my personal health information in their computers	1	2	3	4	5	6	7
14	I am concerned that health care entities would share my personal health information with other health care entities without my authorisation	1	2	3	4	5	6	7
15	I am concerned that health care entities' databases that contain my personal health information are not protected from unauthorised access	1	2	3	4	5	6	7
16	I am concerned that health care entities do not take enough steps to make sure that my personal health information in their files is accurate	1	2	3	4	5	6	7
17	I am concerned that health care entities do not devote enough time and effort to preventing unauthorised access to my personal health information	1	2	3	4	5	6	7
18	I am concerned that health care entities do not devote enough time and effort to verifying the accuracy of my personal information in their databases	1	2	3	4	5	6	7
19	I am concerned that health care entities do not have adequate procedures to correct errors in my personal health information	1	2	3	4	5	6	7

**20.** If I knew that my **health information** was not being adequately protected, I would be **MOST concerned** about:

(Please rank options in order of importance by placing a number between 1 and 7 beside each option with 1 representing your biggest concern)

- Losing my job ☐
- Losing the respect of my colleagues ☐
- Losing the respect of my family and friends ☐
- Being treated differently by my colleagues ☐
- Being treated differently by my family and friends ☐
- Having my identity stolen ☐
- Having my financial information stolen ☐

## V: TECHNOLOGY ADOPTION

***This section includes brief descriptions of different health technologies. Please read each description and answer the related questions.***

**Electronic Health Records systems (EHRs)** are used by health professionals to maintain a digital record for each patient. These records include all of the patient's health information from illnesses, to test results, and medication details. Health professionals can **update and share** these health records. When EHRs are introduced, **patients' consent** to allow their health information to be digitised is sought. Patients can also access their health record using an online portal.

If an electronic health record (EHR) system was introduced in Ireland, to what extent would you **allow your health information** to be included?

<b>1</b>	<i>Extremely Unlikely</i>	<i>Unlikely</i>	<i>Neither likely or unlikely</i>	<i>Likely</i>	<i>Extremely Likely</i>
	1	2	3	4	5
<b>2</b>	<i>Highly Improbable</i>	<i>Improbable</i>	<i>Neither probable or improbable</i>	<i>Probable</i>	<i>Highly Probable</i>
	1	2	3	4	5
<b>3</b>	<i>Extremely Unwilling</i>	<i>Unwilling</i>	<i>Neither willing or unwilling</i>	<i>Willing</i>	<i>Definitely Willing</i>
	1	2	3	4	5

**4.** If an electronic health record system was introduced in Ireland, how often would you access your personal electronic health record using an online portal?

<i>Never</i>	<i>Once a month or less</i>	<i>2-3 times a month</i>	<i>1-3 times a week</i>	<i>4 times a week – Every day</i>
1	2	3	4	5



**For each statement, please circle the number that indicates your level of agreement**

	<b>I believe:</b>	<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>5</b>	Health professionals (GPs, nurses, other physicians) would encourage me to consent to an electronic health record	1	2	3	4	5
<b>6</b>	Electronic health records would increase my involvement in my healthcare	1	2	3	4	5
<b>7</b>	Important people in my life (friends, family, and colleagues) would encourage me to consent to an electronic health record	1	2	3	4	5
<b>8</b>	Electronic health records would increase my access to my own health information	1	2	3	4	5
<b>9</b>	Electronic health records would improve my communication with health professionals	1	2	3	4	5
<b>10</b>	People who influence my decisions would encourage me to consent to an electronic health record	1	2	3	4	5
<b>11</b>	Electronic health records would make managing my healthcare easier for health professionals	1	2	3	4	5
<b>12</b>	Electronic health records would improve the healthcare I receive	1	2	3	4	5

Individuals can use health technologies to monitor their personal health. These technologies include **Mobile Health Applications** which can be used to track exercise or manage an illness, **Health Monitoring Devices** such as a Fitbit or heart rate monitor, and **Personal Health Records (PHRs)** which allow individuals to maintain their own digital health record and share health information with health professionals.

**Based on the health technologies described above, indicate your agreement with each statement.**

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>13</b>	I intend to use/continue to use health technologies	1	2	3	4	5
<b>14</b>	I plan to use/ continue to use health technologies	1	2	3	4	5
<b>15</b>	I predict I will use/ continue to use health technologies	1	2	3	4	5

**Please indicate how often you feel you would use each of the following technologies.**

		<i>Never</i>	<i>Once a month or less</i>	<i>2-3 times a month</i>	<i>1-3 times a week</i>	<i>4 times a week –Every day</i>
<b>16</b>	Personal health records	1	2	3	4	5
<b>17</b>	Mobile Health Applications	1	2	3	4	5
<b>18</b>	Health Monitoring devices	1	2	3	4	5

**Based on the health technologies described above, please circle the number that indicates your agreement with each statement**

		<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither agree or disagree</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>19</b>	I am confident in my current ability to use health technologies to manage my health	1	2	3	4	5
<b>20</b>	When it comes to using health technologies to manage my health, I believe I am knowledgeable	1	2	3	4	5
<b>21</b>	I could use health technologies to manage my health, if I had used a similar technology before	1	2	3	4	5
<b>22</b>	I could use health technologies to manage my health, if someone showed me how to	1	2	3	4	5
<b>23</b>	I could use health technologies to manage my health, if I had time to try them out	1	2	3	4	5

**Based on the health technologies described above, please indicate your agreement with each statement.**

	<b>I believe:</b>	<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>24</b>	Using health technologies would improve my access to my health information	1	2	3	4	5
<b>25</b>	Health technologies would be easy to use	1	2	3	4	5
<b>26</b>	Health professionals (GPs, nurses, other physicians) would encourage me to use health technologies to manage my health	1	2	3	4	5
<b>27</b>	Using health technologies would improve my ability to manage my health	1	2	3	4	5
<b>28</b>	Important people in my life (friends, family, and colleagues) would encourage me to use health technologies to manage my health	1	2	3	4	5
<b>29</b>	Using health technologies would make managing my health easier	1	2	3	4	5
<b>30</b>	Using health technologies would make managing my health fun	1	2	3	4	5
<b>31</b>	People who influence my decisions would encourage me to use health technologies to manage my health	1	2	3	4	5
<b>32</b>	Using health technologies would help me to become more informed about my own health	1	2	3	4	5
<b>33</b>	Using health technologies would result in an improvement in my health management	1	2	3	4	5
<b>34</b>	I could use health technologies to compete with my friends to achieve health goals	1	2	3	4	5
<b>35</b>	Using health technologies would improve the quality of my health	1	2	3	4	5

	<b>I would use health technologies:</b>	<i>Strongly disagree</i>	<i>Disagree</i>	<i>Neither</i>	<i>Agree</i>	<i>Strongly agree</i>
<b>36</b>	If I had a chronic illness	1	2	3	4	5
<b>37</b>	If I was a caregiver (for a child, parent, grandparent)	1	2	3	4	5
<b>38</b>	If I had an incentive from my employer, insurance provider or the government	1	2	3	4	5
<b>39</b>	If I travelled often	1	2	3	4	5
<b>40</b>	If I moved or relocated often	1	2	3	4	5
<b>41</b>	If it helped connect information between my doctors and health providers	1	2	3	4	5
<b>42.</b>	If I wanted to track fitness goals	1	2	3	4	5

## VI: GENERAL CHARACTERISTICS

***Please tick the box that best describes you.***

**1. Gender:**

Male ☐

Female ☐

**2. Age:**

18-19 ☐      20-24 ☐      25-29 ☐      30-34 ☐      35-39 ☐      40-44 ☐

45-49 ☐      50-54 ☐      55-59 ☐      60-64 ☐      65-69 ☐      70+ ☐

**3. What is the highest level of education you have achieved to date?**

Some Secondary School or less ☐

Completed Secondary School ☐

Some college ☐

Undergrad/Bachelor's degree ☐

Master's degree ☐

Beyond Masters ☐

**4. Which option best describes your current employment status?**

- Student ☐
- Jobseeker ☐
- Employed ☐
- Self-employed ☐
- Retired ☐
- Homemaker ☐

**5. Which industry best describes the one you are currently employed in? (Employed only)**

- Retail trade ☐
- Finance, insurance, real estate ☐
- Professional, scientific, and management services ☐
- Education ☐
- Healthcare and/or social services ☐

Other, please specify: \_\_\_\_\_

**6. Which discipline best describes the one you study? (Students only)**

- Arts and Humanities (e.g. History, Philosophy) ☐
- Business (e.g. Accounting, HRM) ☐
- Education ☐
- Engineering (e.g. Mechanical, Electrical) ☐
- Law ☐
- Life, Physical, or Mathematical Sciences ☐
- Medicine and Health Sciences (e.g. Nursing) ☐
- Social and Behavioural Sciences (Psychology, Sociology) ☐
- Computer Science ☐

Other, please specify: \_\_\_\_\_

**7. Please use this space to make any additional comments regarding health technologies, the survey, or your health information privacy concerns.**

--

**Thank you for taking the time to participate**

## APPENDIX G: SURVEY ITEMS AND SUPPORT

	Variable to be measured	Items	Source	Items
Antecedents: Individual Characteristics	Gender	1	King <i>et al.</i> , (2012)	Female/Male
Antecedents: Individual Characteristics	Age	1	King <i>et al.</i> , (2012)	11 options
Antecedents: Individual Characteristics	Healthcare Need	3	Klein (2007) Wilson and Lankton (2004)	Number of visits to health professionals, number of different health professionals visited, number of prescriptions.
Antecedents: Individual Characteristics	Poor Health Status	3	Angst and Agarwal (2009) Bansal <i>et al.</i> , (2010)	Frequency of pain and discomfort, severity of condition, overall health status
Antecedents: Perceptions	Perceived Sensitivity	12	Caine and Hainana (2013), Laric <i>et al.</i> , (2009)	12 types of health data
Antecedents: Perceptions	Trust in Health Professionals	6	Li <i>et al.</i> , (2014) Hong and Thong (2014)	Three dimensions: benevolence, competence and integrity
Antecedents: Perceptions	Trust in Health Technology Vendors	6	Li <i>et al.</i> , (2014) Hong and Thong (2014)	Three dimensions: benevolence, competence and integrity
Antecedents: Perceptions	Risk Perceptions: Health Professionals	4	Li <i>et al.</i> , (2014) Hong and Thong (2014)	4 items related to perceived risks of disclosing health data to health professionals
Antecedents: Perceptions	Risk Perceptions: Health Technology Vendors	4	Li <i>et al.</i> , (2014) Hong and Thong (2014)	4 items related to perceived risks of disclosing health data to health technology vendors
Antecedents: Experience	Privacy Media Coverage Awareness	2	Smith <i>et al.</i> , (1996)	Awareness of privacy media coverage regarding personal data and health data

Antecedents: Experience	Privacy Invasion Experience	2	Li <i>et al.</i> , (2014)	Experience of privacy invasion of personal data, and health data
Antecedents: Experience	Health Information Seeking Experience	6	Kim and Park (2012)	4 items: Using Internet for disease diagnosis, for management, for education and learning, for buying health products
			Pilot Testing	1 item: Use Social media for health purposes
Antecedents: Experience	Mobile health application experience	8	Fox and Duggan (2012)	Categories of mobile health application
Health Information Privacy Concerns	HIPC	19	Hong and Thong (2013)	6 dimensions: Collection, Unauthorised Secondary Use, Improper Access, Errors, Control and Awareness
Intentions: EHRs	Intention to Opt-In to EHRs	3	Bansal <i>et al.</i> , (2010)	Likelihood, Probability, and Willingness
Perceived Benefits: EHRs	Perceived Benefits of EHRs	5	Wu <i>et al.</i> , (2007), Wilson and Lankton (2004), Or <i>et al.</i> , (2011)	Adopted to EHR Context
Intentions: mHealth	Intention to adopt mHealth in the broad sense	3	Venkatesh <i>et al.</i> , (2003)	Intention to use, plan to use, predict I will use
Intentions: mHealth	Intentions to adopt different mHealth solutions	3	N/A	Frequency of use of mHealth applications, wearable devices, and personal health records
Perceived Benefits: mHealth	Perceived Benefits of mHealth	8	Li <i>et al.</i> , (2014) Pilot Testing	
Controls: EHRs	Social Influence	3	Or <i>et al.</i> , (2011)	Opinions of health professionals, important people, and influential people
Controls: mHealth	Social Influence	3	Or <i>et al.</i> , (2011)	Opinions of health professionals, important people, and influential people

Controls: mHealth	MHealth self-efficacy	5	Kim and Park (2012)	2 items: current ability, 3 items: potential ability
Controls	Education	1	N/A	Several Options
Controls	Job Status	1	N/A	Options: Student, Employee, Unemployed, Homemaker, Self-employed, Retired
Controls	Industry	1	N/A	Several Options
Controls	Academic Discipline	1	N/A	Several Options
Antecedents: Experience	Mobile Health Experience	2	N/A	Experience using wearable health devices, and personal health records
Additional: Experience	Internet Experience	1	Malhotra <i>et al.</i> , (2004)	Approximately how long have you been using the Internet?
Additional: Experience	Devices Used	1	Kim and Park (2012)	Which of the following technologies do you use to access the Internet?
Additional: Experience	Frequency of Use	2	N/A	Use Internet for work purposes, for personal purposes
Additional: Perceptions	Perceived Ownership	3	Avey <i>et al.</i> , (2009)	Adopted to health context: degree of ownership, data belongs to me, data defines me
Antecedents: Extra	Legislation Awareness	2	Pilot Testing	Awareness of data legislation governing personal data, and health data
Intentions: Extra	Access to EHRs	1	N/A	Frequency of Access to EHR
Intentions: Extra	Conditional use of mHealth	1	Angst and Agarwal (2009)	Situations when I use mHealth: 6 options
Moderators	Chronic Illness	1	Angst and Agarwal (2009)	Do you have any chronic illnesses?
Additional	Stigma: Chronic	2	Pilot Testing	Frequency of past stigmatisation, fear of future stigmatisation



Moderators	Sensitive Illness	1	N/A	Do you have any illnesses or conditions you would describe as sensitive?
Additional	Stigma: Sensitive	2	Pilot Testing	Frequency of past stigmatisation, fear of stigmatisation
Additional	Repercussion	1	Pilot Testing	Biggest concern if health data was not private 7 options

## APPENDIX H: INTERVIEW CONSENT FORM

### Citizens' Health Information Privacy Concerns on their Adoption of Health ICTs

**Purpose of the study:** You are invited to participate in a PhD Study conducted by Grace Kenny, DCU Business School in Ireland. This study is funded by the DCU O'Hare Scholarship and the ASU-DCU catalyst fund. This study explores individuals' concerns related to the collection, storage, and use of information pertaining to their physical and mental health. Participants are invited to participate in a one to one interview with the researcher to discuss their experiences and perspectives regarding health information privacy. The interview will last approximately 30 minutes. The researcher will request to record (audio only) the interview.

Participant – please complete the following (Circle Yes or No for each question)

<i>I have read the Plain Language Statement (or had it read to me)</i>	Yes/No
<i>I understand the information provided</i>	Yes/No
<i>I have had an opportunity to ask questions and discuss this study</i>	Yes/No
<i>I have received satisfactory answers to all my questions</i>	Yes/No
<i>I agree to participate in an interview with the researcher</i>	Yes/No
<i>I am aware that my interview will be audiotaped</i>	Yes/No
<i>I am aware that may withdraw from the Research Study at any point</i>	Yes/No
<i>I understand that my participation will be anonymous</i>	Yes/No

The information you provide in the interview will be confidential and stored securely in the researcher's office. This information will be securely disposed of within two years of this interview. However, if any information comes to light which shows that you are in danger, we are legally obliged to report it.

I have read and understood the information in this form. My questions and concerns have been answered by the researchers, and I have a copy of this consent form. Therefore, I consent to take part in this research project

**Participants Signature:** \_\_\_\_\_

**Name in Block Capitals:** \_\_\_\_\_

**Witness:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Project supported by:**  
**DCU O'Hare Research Scholarship**  
**ASU-DCU Catalyst Fund**



Ollscoil Chathair Bhaile Átha Cliath  
Dublin City University



## **APPENDIX I: INTERVIEW GUIDE**

### **Introduction**

[Aim: Thank participant, explain interview process, and allow for questions]. Firstly, I want to say thank you for taking the time to meet with me today. Before we get started, I'll tell you a bit about what we're doing today. The interview will consist of broad questions and topics all related to your personal information, most of them will relate to your personal health information but some will be broader. There are no right or wrong answers, I'm just looking for your personal opinion and you don't have to divulge any personal health conditions, but again if you do they'll be confidential. If it is okay with you, I will audio record the interview on this device. The interview is completely confidential; your name or information will never be used. The interview will be transcribed by myself and locked in my office until completion of the research. If you would rather not answer a question or want to stop at any time that's completely fine. The interview should last between 30 and 45 minutes. Have you any questions before we start?

### **Participant Background**

[Employed/Self-employed] Q: To start, could you tell me about your job, what do you do for a living?

[Students] Q: Could you tell me about your studies? (Discipline, year, part-time jobs)

[Retirees] Q: Prior to retiring, what did you do for living? (How long are you retired?)

#### **Internet Experience**

Broad Introduction Question: Tell me about your Technology Use? (length of experience with computers, types of devices used, frequency of use, different purposes)

Internet Q: Tell me about your Internet Use (frequency of use, purposes, devices used, experience)

Additional Qs: [Employees] Would you use computers much in work? (types of uses, access to personal data?)

[Retirees] Q: Are there any things you can't/won't do online (ascertain limits in ability and desire)

### **Health Information Seeking Behaviours**

Broad Introduction Question: Do you search online for health information?

For what purposes (ascertain if fitness related, related to specific condition or generic searches)

How often would you search online for health information?

Are there any particular websites you use for health information? (Why?)

Additional Qs: What devices do you use?

Are there any risks associated with using the Internet as a source of health information?

Do you visit health forums? (Browse or post)

Social media activity (to determine frequency of information disclosure)

### **Health IT Experience**

Broad Introduction Question: Do you use any mobile health applications (List categories if necessary: health information, pregnancy, medication management, mental health, fitness, diet, sleep, chronic illness based applications)

Have you ever used a mobile health application? (If so, details on the application, reason for cessation of use)

Do you use any wearable tracking devices (Fitbit, Jawbone, smartwatch: explain if necessary)?

Additional Qs: (Retirees) Have you heard of these applications (Describe if possible)

Use/Awareness of Healthkit on iPhone

Would you use mobile health applications/wearable devices? (Reasons why/why not, what type of applications)

## **Antecedents**

### **Media Coverage**

Can you recall any privacy related new stories you have heard? (Level of awareness)

Do you hear these stories often? (Frequency)

Where have you heard these stories? [news or word of mouth]

Have you ever heard similar stories related to health information?

How do you react when you hear these stories?

### **Privacy Invasion Experience**

Has your data ever been used in a way which you deemed excessive?

How often does this occur? (Frequency)

How you feel/react?

Has your health information ever been used in a way which was excessive or surprising?

**Trust: Health Professionals**

Broad Introductory Question: How would you describe your trust in health professionals (Why?)

How would you describe your trust in them to protect your health data?

Additional Qs: Additional health professionals such as nurses, pharmacists, specialists etc.

Trust in ability to protect health data (Competence)

Trust to only use data for patient's benefit (Benevolence/Integrity)

Do you think trust is an important component in your relationship with health professionals?

**Trust: Technology vendors**

Broad Introductory Question: How would you describe your trust in technology companies you're your health data (Why?)

How would you describe your trust in them to protect your health data?

Additional Qs: Small vs. large technology organisations

Trust in ability to protect health data (Competence)

Trust to only use data for patient's benefit (Benevolence/Integrity)

**Risk: Health Professionals**

Broad Introductory Question: Do you think there are any risks associated with disclosing data to health professionals? (Why/What risks)

Do you think there are risks of negative outcomes when you disclose data to health professionals?

Do you think there are risks of loss when you disclose data to health professionals?

Additional Qs: Additional health professionals such as nurses, pharmacists, specialists etc.

**Risk: Technology Companies**

Broad Introductory Question: Do you think there are any risks associated with disclosing data to technology companies? (Why/What risks)

Do you think there are risks of negative outcomes when you disclose data to technology companies?

Do you think there are risks of loss when you disclose data to technology companies?

### **Perceived Sensitivity**

Broad Introductory Question: Would you describe health data as sensitive?

Why is health data sensitive/not sensitive to you?

What type of health data are you most sensitive about? Why?

Additional Qs: What types of health data do you think are most sensitive in general?

### **Stigma**

Have you ever been treated differently due to a health condition? (Explain occasion, frequency, feelings)

Do you fear that you will be treated differently due to a health condition? (Why, what parties etc.)

Do you think people with certain health conditions are treated differently? (Why? How?)

## **Health Information Privacy Concerns**

How would you describe your concern for the privacy of your health data? (Any current concerns, past concerns)

What are you currently concerned about? (health professionals and technology companies)

Collection: How do you feel about the collection and storage of large quantities of your health data? (what data types, health professionals and technology companies, present vs. future concern)

Secondary Use: Are you ever concerned that your health data might be used for secondary purposes without your permission? (health professionals and technology companies, present vs. future concern, what uses)

*Additional:* What purposes do you think your health data should be used for? (health professionals and technology companies, conditions on use)

Improper Access: Are you ever concerned that your health data might be accessed by unauthorised parties? (health professionals and technology companies, present vs. future concern, what parties, why)

*Additional:* What parties do you think should have access to your health data (health professionals, employers, legal and insurance companies, government etc., why)

Errors: Does the possibility of errors in your health data cause concern? (Why, health professionals and technology companies, present vs. future concern)

Control: Do you currently believe you have control over your health data (health professionals and technology companies, why, how do you feel, present vs. future concern)

*Additional:* What level of control over your health data do you think you should have? (health professionals and technology vendors)

Awareness: Are you currently aware of how your health data is protected? (health professionals and technology companies, present vs. future concern)

Are you aware of how your health data is used and shared? health professionals and technology companies, present vs. future concern)

*Additional:* Is awareness important for you? Should we be more aware? Should we ask more questions/should health professionals/technology companies be more transparent?

Additional Questions: Is privacy (health data) important to you? Why?

## **Health Information Technologies**

### **EHRs**

Describe EHRs:

If an EHR was introduced, would you give permission for your health data to be included? (Why/Why not? Conditions on acceptance)

What do you think the benefits of this system would be? (for health professionals and patients)

Would the opinion of your friends, family, health professionals influence your decision? (Social Influence)

### **Mobile Health**

Describe mHealth applications, wearables and PHRs:

Would you use these technologies? (Which ones, why, conditions)

What technologies would you not use? (Why)

What do you think the benefits of these technologies are?

If your friend, family member, or doctor recommended one of these technologies would you adopt? (Social Influence)

[Retirees] Do you think you could use these technologies? (self-efficacy)

## **Additional Questions**

### **Perceived Ownership**

Who owns data pertaining to your health? (you or health professional/technology company)

Why?

Additional Questions: When you disclose this data, do you retain ownership?

### **Legislation**

Are you aware of existing legislation which protects your personal data? (HIPAA in the U.S.)

Views on the need to regulate health data usage?

**Close**

Any additional comments? Any questions?

[Clarify any confusing comments at this point if necessary]

Thank you so much for taking the time to meet with me today.



## APPENDIX J: CODING PROTOCOL

	Themes	Codes	Sub-codes
Antecedents	Awareness of Media Coverage	1. Personal Data 2. Health Data	Awareness of frequency (High or low) Degree of Familiarity (High or low) Issue Involvement (High or low) Understanding of Risk (High or low) Discounting Techniques (Yes or No)
	Privacy Invasion	1. Personal Data invasions 2. Health data invasions	Surprise vs. Expectation Level of Severity (High or low) Discounting Techniques (Yes or No)
	Health Information Seeking Behaviour	1. Experienced or Inexperienced	Frequency of Searches (High or low) Breadth of Purpose Search Process (Broad vs. Focused) Views on Credibility Views on Risk
	Perceived Trust	1. Health Professionals 2. Technology Vendors	Competence Integrity Benevolence Individual vs. Organisational trust
	Perceived Risk	1. Health Professionals 2. Technology Vendors	Trust vs. Risk
	Perceived Sensitivity		Broad perception of sensitivity Personal nature of health data Possible repercussions
Dimensions of Concern	HIPC	1. Collection 2. Secondary Use 3. Improper Access 4. Errors 5. Control 6. Awareness	Broad concerns Current vs. Future concerns Health professionals vs. technology vendors Blind assumptions of privacy
Benefits	Perceived Benefits	1. EHRs 2. mHealth	Type of benefits (Lifesaving, hedonic, or utilitarian)

Intentions	Intentions	1. EHRs 2. mHealth	Broad intentions Conditions on adoption Influence of HIPC Influence of Benefits Sensitivity of Data Privacy Calculus
Additional Factors	Perceived Ownership	-	Type of ownership (full vs. shared) Current level of ownership Desire for Ownership
	Health Locus of Control	-	HLOC and privacy (Internal, external or shared) HLOC and personal health (Internal, external or shared)
	Privacy-Protective Behaviours	-	Information provisions Private actions Past vs. Expected Behaviours

## APPENDIX K: INTERVIEW ANALYSIS: MEDIA COVERAGE

Interview Participant	Answer	Extracted Meaning
1	“I don’t read much about celebrities or watch them on stupid television shows but no I don’t. If it’s misinformation out there, that’s a different thing. If its wrong information, but I think that’s serious and wrong information about anyone is very serious”	-Does not pay attention to media coverage in general -Concerned with misinformation
2	“There’s nothing that comes to mind but you read things in the paper that you know not talking about the net particularly but it would be talking about member all those people whose phones were tapped and the people that done the tapping eventually almost got away with it, I know the one from the news of the world whatever her name was she got away with and the guy that was with her. Nobody I know personally and so consequently I wouldn’t loosely talk about that.”	-No specific stories -Aware of misuse of data -Sees no redress for misuse -No personal stories
3	“Well Sony seem to be in the news every other week due to some form of data breach I know they had a huge one a few years ago, there’s actually loads of stories in the news. This stuff seems to happen all the time I find I don’t keep up with every story as there’s just so many and I also use a password manager for all my accounts so it informs me when to change my passwords for everything. <i>Health:</i> “I’m sure it happens all the time but there are no stories I can think of off the top of my head no. I’m sure some insurance companies are doing some dodgy stuff to get health information though. It makes me worry sometimes but if I had serious illnesses I’d be more concerned and as I get older too about my health information specifically.”	-Aware of frequency and large breaches -Uses passwords to protect self -No specific health stories but aware it is likely to occur -Worried at times -Conditions: More worried if had serious conditions and as he ages
4	“I’ve seen people create fake profiles on sites like Facebook to get revenge or they might add you and you don’t know them. They do concern me and I might change my passwords anytime I get freaked out but I don’t put too much stuff on Facebook anyways so if people seen it I wouldn’t be overly worried; I’d prefer them to not be able to see it though <i>Health:</i> “Yeah I’ve heard of a few from the HSE of people losing patients’ information or people who didn’t need to see the information seeing it or files being taken.”	-Aware of social media risks but limits personal risks by limiting information disclosed -Broad awareness of health breaches
5	“Like I see things going viral very quickly can kind of scare me like videos of a girl talking about her dad working in a major financial firm going viral overnight and having a major effect on her life. It’s scary to see how something someone says can be shared by so many people. I’ve heard so many stories about celebrities’ information or photos being leaked its kind of	-Broad awareness of stories in general and celebrities -Feels vulnerable, would be more concerned if happened to a friend

Interview Participant	Answer	Extracted Meaning
	<p>scary like it shows how vulnerable any of us are. If that was someone I knew it would scare me.”</p> <p>Health: “I’ve worked in a hospital for many years. I know pretty much anyone can walk in and take a patient’s chart and have a read and they could be someone you know. I’ve not heard lots of news stories but I’ve heard stories in general or seen it from working in this environment. I remember that woman in England, a nurse who revealed information to a journalist about the Duchess and because of the media storm it caused she committed suicide. That was a genuine error with a devastating outcome. It’s all like that you google something and then Facebook or google is reminding you to take your contraceptive pill or to exercise. I think it’s worse if they do it with your health data because that’s so personal they shouldn’t be using that to target advertising.”</p>	<ul style="list-style-type: none"> <li>-Aware of risks in health context due to working experience</li> <li>-Aware of health news stories and negative outcome</li> <li>-Aware of potential use of health data for advertising</li> <li>-Views health data as personal</li> </ul>
6	<p>“Well there was loads you know the whole Jennifer Lawrence thing where someone hacked into her iCloud and stole a bunch of photos and leaked them. And I think a week or two ago a card enquirer had their systems hacked and lost a bunch of card numbers. When I hear stuff like that I start to think where is that information I gave out before and is it still out there. I know I’ve been fairly conscious of it the last few years but there was a time before when I wouldn’t have really thought about it maybe cos I was inexperienced or didn’t understand.”</p> <p>Health: “I can’t think of any off the top of my head but I’ve definitely heard about clinics in the US being hacked or employees looking at things they shouldn’t but none specifically stick out in my head”</p>	<ul style="list-style-type: none"> <li>-Aware of celebrity stories</li> <li>-News stories make him think of his own information</li> <li>-Broad awareness of health stories and possible breaches but no specific stories</li> </ul>
7	<p>“There’s a lot. I suppose the Sony one will always stick out in my mind. I’m not talking about any recent ones but the one years ago when people’s financial information was breached and I don’t think it was encrypted either I remember thinking they handled it really poorly too. It’s something you’re hearing a lot of more and more lately. There’s even the Alan Shatter one recently.”</p> <p>Health: “I’ve not heard lots of news stories no. With my work though, I can appreciate the danger to that kind of information and the potential repercussions if it fell into the wrong hands. One thing I’ve come across is a lot of the time you’d be looking at existing claims and I’ve seen claimants’ names when I really shouldn’t just due to someone forgetting to remove the name or bad data controls. It’s particularly sensitive information and it shouldn’t be happening. It shows how so many people could have access to this information even if I didn’t necessarily</p>	<ul style="list-style-type: none"> <li>-Aware of frequency of breaches and large breaches</li> <li>-No specific health stories</li> <li>-Aware of health data travelling due to work</li> <li>-Hope his health data would only be accessed when necessary and respected.</li> </ul>

Interview Participant	Answer	Extracted Meaning
	work in a health based company. Even in my previous job which related to health and you'd get a list of names like all the employees of a certain company and you'd see this person has breast cancer. Regardless of your level at company you'd see that and maybe you need to but it makes you hope that if you were in that situation only people who needed your information could access it and those who had access had respect for the sensitivity of that kind of information."	
8	<p>"There was the leak of photos there of celebrities such as Jennifer Lawrence from the cloud. I think though a breach can happen to anyone like my parent's credit card was scammed twice within a month and they wouldn't use the card a lot because they would be careful and worried. There's a lot of largely publicised breaches then the Sony breach a few years back is one and more recent ones they've had.</p> <p>Health: "I've heard of breaches alright. Like laptops being stolen. I think there's been breaches in celebland about such a person got plastic surgery or whatever. I saw something online the mirror newspaper of X-ray images of someone who got a coffee jar stuck somewhere unfortunate – those films were shared worldwide isn't that scary. Quite horrific imagine that was you. I certainly wouldn't want my labour story shared with the world any graphic details definitely not. I wouldn't want any of my son's information going anywhere."</p>	<ul style="list-style-type: none"> <li>-Aware of frequency of breaches</li> <li>-Awareness of public breaches, celebrity breaches and family experiences</li> <li>-Aware of health breaches</li> <li>-Wouldn't want her health information shared</li> </ul>
9	<p>"A data breach there's a lot of those, obviously the Sony one from last year, and then there's a good few lizard squad they were going around and obviously there's wikileaks obviously Snowden was on the run, so many I can't think of them all but I think eh there was a big one, credit unions were going after people who couldn't pay their loans and they hired private investigators and got their PPS numbers that was a big fiasco and I think it was 3 credit unions in Kildare but em they got into serious trouble over that because of the PPS numbers basically the same scenario as peoples' PPS numbers in Irish waters people were going mad over that. Health breaches, no I can't really think oh the hospital records being found in a bin outside a hospital."</p>	<ul style="list-style-type: none"> <li>-Aware of high volume of breaches</li> <li>-Very aware of stories breaches internationally and nationally and data misuse</li> <li>- Vague recall of a health breach</li> <li>- Aware of potential for information to travel</li> </ul>
10	<p>No. Wait I have, I was just thinking of people I know but ye definitely with celebrities you'd always hear of you know people's accounts being hacked you know like last year peoples' private pictures were being shared you know so ye you definitely hear of it. And I know wikileaks back a few years ago lots of private government information was stolen and leaked especially with America and you know the Iraq war that was massive."</p>	<ul style="list-style-type: none"> <li>-Broadly aware of celebrities and big breaches like Wikileaks but no personal stories</li> <li>-Unaware of health breaches</li> </ul>

Interview Participant	Answer	Extracted Meaning
	“Eh no I can’t say I have [heard of health stories]”	
11	<p>“I have heard horror stories aplenty about youngsters, okay I know I won’t go to the extremes of sex texting or whatever they call it, but the danger when it goes on there is it can go viral and it can lead to all sorts of danger for them.”</p> <p>“I mean employers are just as capable of eavesdropping electronically as anyone else, not that they need to but if they wanted to do a quick check, is there anything there, and oh look at this guy maybe pass him over and on to the next candidate. So I’m just saying, I don’t think people seem to realise the potential, for good and for bad”</p>	<p>-Aware of ‘extreme stories’</p> <p>-Danger of photographs</p> <p>-Danger of information posted online being misconstrued and employer searching for information</p> <p>-Perceived risks focused on information disclosed not collected by organisation- doesn’t view risks to himself</p> <p>-Solution: doesn’t use social media views as an intrusion</p>
12	“I would have heard of stories alright, laptops being stolen from hospitals or other places like government ministers leaving a laptop in a taxi or something and the information being then leaked out or something getting it. I’ve only heard it a couple of times now, it possibly is you know but it may not get out to the general, the mainstream”	<p>-Aware of some stories of laptops but no specifics</p> <p>-Heard small number of stories but not in mainstream news</p>
13	I would be surprised that so many people would be looking at that poor woman’s story. I think it’s good she wants people to be aware but it’s such a personal thing I would not know if I would want to do that, I would want to get help yes, and I certainly wouldn’t condone that behaviour but I don’t know that I would be happy to put it for so many people.	<p>-Domestic abuse story surprised by attention</p> <p>-Unaware of health stories</p> <p>-Knowledgeable of risks to privacy in health setting due to work experience</p> <p>-Boundary control on information</p>
14	<p>“You hear a lot of complaints sometimes on radio and stuff like that and you hear people complaining about you know girls you know the post pictures on Facebook and they’re misconstrued or whatever, people have access to them</p> <p>. Now I know that there are probably filters than you can put on Facebook too, to a degree, but I think once it’s up there it’s up there, it’s difficult to get it back. I think it happens all the times with those companies. They use the information for things people might not be happy with. I can’t think of any specific but I’m sure they all do it.”</p>	<p>-Aware of danger to information disclosed on Facebook</p> <p>-Broadly aware of risk of information misuse</p> <p>-No specific stories</p>
15	“Not personally, my daughter who lives in Australia they’ve had problems with credit cards and things like that a few times, you know it hasn’t happened to me personally and I would be very	-Daughter had experience

Interview Participant	Answer	Extracted Meaning
	careful about it, I mean you keep getting these boxes popping up on the computer I won't open them at all, I don't, I just avoid them, and emails if I don't know who they are, or phone calls on my phone if I don't know who they are I won't answer them or anything like that, I'm a bit careful like that but you can understand somebody just not thinking and being caught out you know, it's very quick. I'm a bit reluctant of giving too much information online, because they always tell you 'oh it's perfectly safe' and everything like that, I just don't believe that, because when you hear of Wikileaks and all that, and you just hear of so many problems with sites going down and people being hacked you know. We had an example this week people in hospitals were getting holidays in exchange for information so they could get the contract. People have been suspended"	<ul style="list-style-type: none"> <li>-Views himself as more careful than others</li> <li>-Reluctant to disclose information</li> <li>-Broad awareness of risk of hacking and surveillance</li> <li>-Health information sharing example influenced view that health data is shared with external companies see trust</li> </ul>
16	"Well just as we speak, there's a very, story after breaking worldwide about domestic abuse, and that's gone worldwide" "My daughter bought Uggs for Christmas off a website that had 100% genuine and she ordered them 10 weeks for Christmas but up to Christmas week they still hadn't come and I got suspicious, I said that must not have been an official website, and it was an unofficial one and she never got the Uggs or the money back and it was on the news then that the police everybody not to go on those websites unless it was, there were like specific shops, because they were all con artists, and they were getting an awful lot of money from people, people didn't realise that it was a con. I wouldn't buy online. I'd be terrified that would happen to me."	<ul style="list-style-type: none"> <li>-Aware of current story</li> <li>-Experience of daughter and financial loss</li> <li>-Solution: Does not buy online or only use official websites</li> </ul>
17	"The stuff that comes up on Google or on the news and that you know, or things that would have happened in my daughter's job because she's in a job where they would have had to take what do they call it they take in personal information and their job is very secure and they all had to take this oath that they won't pass on any information and all that, and it has been passed because they've been broken in to and stuff has been robbed. It makes me more scared for my own information and I hate, I hate them putting all the stuff they're putting up on about their children on Facebook, I hate it."	<ul style="list-style-type: none"> <li>-Vague knowledge of data theft but physical sense not online</li> <li>-Fear for own information</li> <li>-Does not agree with information disclosure online</li> </ul>
18	"Well, you hear things like that all the time, but I've never known anybody that it happened to. I'd be afraid they'd [online companies] would run off with my money"	<ul style="list-style-type: none"> <li>-Aware that financial loss occurs frequently but no specific stories in news or someone they know</li> <li>-Fear of financial loss</li> <li>-No risks discussed other than financial</li> </ul>

Interview Participant	Answer	Extracted Meaning
		-Solution: doesn't shop online
19	<p>"Yeah I mean how many times this year did a file go missing? And I think, you see this on the television as well, on these crime programmes and you know files going haywire out the back of the filing cabinet but I do think now with most times unless the company sits down which banks do have to, but with the health system you often hear of files being robbed out of a car and I don't know whether they're all on backup somewhere because you know you don't have your own information."</p>	<p>-Broad awareness of risk of health files going missing -No awareness of other risks such as financial and non-physical</p>
20	<p>"Yeah you hear a lot of stories. The biggest was probably the one with celebrities' personal photos being leaked when their iCloud accounts were hacked. So you had people like Jennifer Lawrence's photos being leaked online for the world to see. I know some people were critical but she was sending private photos to someone she was in a committed relationship with. You can't fault her for that she doesn't deserve to have the world seeing something as intimate as that regardless of how famous she is. It just shows we are all vulnerable and really need to think before we send something that might get out. Technology is great and it makes communication so easy but it's nowhere near as safe as we assume it is. You can't be crippled by fear either but with things you really value I would be more careful."</p> <p>Not in terms of people I know or any famous people but I've heard stories of hospitals losing files and laptops being stolen here in Ireland and it's just ridiculous that these things still happen especially with something like health information."</p>	<p>-Aware of frequency -Highly aware of celebrity breaches -Shows vulnerability -Need to think before disclosing information -Importance of balancing – can't be in fear but should protect things you value -Aware of data loss in health context – frustrated that this can occur</p>
21	<p>"My understanding of the, of free internet services is that if you're paying for a service you're the customer and if you're not paying for the service you're the product. I haven't been surprised by privacy breaches because I'm fairly careful."</p>	<p>-View that all internet companies misuse data -Careful when online -Falsifies or withholds data -Not aware of health privacy stories</p>
22	<p>"I read in the paper about files in James' being found outside the hospital, yeah I read about that and it was a big kind of thing and there was a big crackdown in the hospital about like the patient file doesn't leave the ward and stuff like that. I don't think that anyone would kind of, I personally wouldn't be looking up peoples' information. I had a friend and her granny was my patient and she kept pressuring me like she wanted to know her results and I was like I can't tell you until the doctor tells your granny. I've only heard of the patient files in James' but that was it. I think</p>	<p>-Aware of health data loss and outcome of loss -View health professionals wouldn't access information for no reason based on exp. But sees potential for breaches -Low frequency in health</p>



Interview Participant	Answer	Extracted Meaning
	people are quite honest. You hear of money scams or breaking into your bank account and people hacking into your Facebook so you would be aware of that.”	-Aware of different risks online including financial, on social media -Need to be aware of risk online
23	<p>“I’ve read about them but I’ve never paid an awful lot of attention to them because I don’t know anybody personally who has suffered from it but I’m aware of the fact that it can happen and that information big time can be abused or misused.”</p> <p>“Where I’m working has a lot of personal information on the laptops about clients like very very personal information Now the laptops are encrypted but I still have eh I still have an alarm bell ringing here <i>what happens if?</i> I’m reassured all the time but it hasn’t happened but there’s huge potential I think for that to happen. I’ve heard of higher up in the HSE laptops being left in places. I’m working with it first hand at the moment and eh I am constantly saying to people you know is anybody aware, but I still think eh reminding people that the laptop is a very valuable piece of information that should be protected at all times. If somebody got that information that there could be third world war breakout. I can say it has never happened and the laptops are encrypted but there’s always the bell here ringing saying be very cautious.”</p>	<p>-Read stories but does not pay attention as does not know anyone who has experienced it.</p> <p>-Aware of potential misuse of data in general</p> <p>-Experience working with sensitive health data. Aware of risks and possible repercussions</p> <p>-Very concerned and cautious</p> <p>-Aware of laptop loss in health previously</p>
24	“Yeah you hear the kind of horror stories of people putting up pictures of their credit cards, you are sort of asking for that, I mean um I’ve come across a couple of um yeah so mainly things like peoples’ accounts being duplicated with a view towards cleaning the account, I know a couple of people that’s happened to. I guess I associate stuff like identity theft more with email even though I suspect it’s probably more prevalent with things like social media and things like that. But yeah I’ve heard stories of people I know and famous people.”	<p>-Aware of high frequency and different types of loss</p> <p>-Financial loss due to information disclosed and scams</p> <p>-Aware of celebrities and friends</p>
25	“Massive one going on over here with the IRS, well it wasn’t the IRS think it was State employees, whatever it was anyways the Chinese hacked in. There’s sort of uproar but I think there’s, there’s a tolerance here, for whatever reason, and because it’s been going on so long. They’re living under the illusion that, that is going to protect them forever from anything bad ever happening, again. Which is actually, I don’t know because I don’t have the stats at hand and I never will but I don’t know that storing everything and analysing it will eventually lead to any real solution”.	<p>-Awareness of specific case</p> <p>-Tolerance in the U.S.</p> <p>-View of others that data collection will help</p> <p>-He does not see how analyzing data can provide a solution</p> <p>-No specific health stories but employers store health data</p>

Interview Participant	Answer	Extracted Meaning
	<i>Health</i> “Em, not in the recent past, no I haven’t heard of any of that here but I don’t know what’s stored here and what the recent breach included but some employers’ retain health information which is nuts anyway.”	
26	<p>“I mean you hear the absolute horror stories of people having their identities stolen and having loans taking out in their name and having to deal with basically near financial ruin because they have to sort all of that out. I mean eventually I feel like a lot of them do get sorted out but at that point a large deal of your life has been delved into. I haven’t heard of any stories that bad personally like of people I know but you do hear it from time to time. You hear of less serious invasions all of the time and the serious ones now and again.</p> <p><i>Health</i>: “I haven’t heard any stories about health really but I’m sure they do happen and they are out there I just haven’t heard any.”</p>	<ul style="list-style-type: none"> <li>-Aware of identity theft risk and repercussions</li> <li>-No knowledge of stories of friends</li> <li>-Frequency: Less serious invasions occur very often, serious invasions less frequent</li> <li>-No specific health stories but assumes they occur</li> </ul>
27	I heard of people complaining because their information online was used or sold and I’ve heard of cases where people had their entire identities stolen which is very scary and you never want that to happen to you. You hear it a lot with celebrities but I’ve heard it happen to people I actually know and that kind of frightens you more because it happens to normal people. I think it’s happening less nowadays that things are getting more secure – or maybe they’re just sorted easier which allows you to keep some faith. With health, I’ve not heard many stories I think that industry works harder with HIPAA	<ul style="list-style-type: none"> <li>-Various in seriousness from misuse of data to identity theft</li> <li>-Aware of celebrities and friends</li> <li>-Scared by friends’ experience - vulnerable</li> <li>-Less common as security improves or solved quickly- helps keep faith</li> <li>- No stories with health, less common with HIPAA</li> </ul>
28	<p>I have heard a lot of stories only because I worked at the State Legislature office this semester. So it came up quite often. They would have lots of discussions about protecting peoples’ privacy and the dangers of stuff like that.</p> <p>I mean you hear stories (health) but much less so. I guess I haven’t worked behind the scenes to experience if privacy is a conversation that happens among health professionals but I assume it does because it’s quite important.</p>	<ul style="list-style-type: none"> <li>-Broadly Aware of stories and risk due to work experience</li> <li>-No detailed knowledge</li> <li>-Less aware of health stories due to experience but perceives it to be important</li> </ul>
29	<p>“Happens more often because people are less tech savvy than they should be. I’ve been very conscious of what I do online [since getting computer virus]”</p> <p>“Specifically for health information, <i>not really</i>, nothing comes to mind no.”</p>	<ul style="list-style-type: none"> <li>-Increased frequency of online breaches</li> <li>-Individuals aren’t equipped to protect data</li> <li>-He is more careful now</li> </ul>

Interview Participant	Answer	Extracted Meaning
		-No awareness of health data breaches
30	"My girlfriend's parents got their social security cards stolen, that was one...my best friends had their credit cards, their credit card information stolen so like charges got ran up like crazy on those...they get it back <i>eventually</i> ."	-Friend's identity theft experience -Financial loss resolved -No awareness of health loss
31	"Well ye you hear all sorts of things like Target they just lost all sorts of stuff like credit cards and stuff like that. So to be safe my husband and I we don't have credit cards, we just have one through USA but it's protected but we don't have other credit cards. It's just a scary thing. It's really crazy. And I think you hear of things like social security numbers get used all the time by people who are like illegal and they use it for tax purposes and all of a sudden you can't claim your taxes because people are working under your number and that's really bad."	-Broadly aware of large breaches -Her solution: No credit cards, only protected -Breaches are scary -Aware of risk of SSN theft.
32	"Yeah yeah lots of things. On the internet you hear those sort of things and on the tv, oh he stole that data, he stole this data so I heard THAT. I've never seen what actually got stolen or how it was used no. "	-Aware of high frequency -Unaware of specific data stolen and outcome
33	"On a far too regular basis, the news will highlight someone who has had their personal information stolen or their phone hacked etc. I feel irritated that people are not respecting boundaries and there's always a worry that it could happen to me it seems no one is off bounds or no one is not vulnerable. Hard position to be in but I guess that's the way the world is at the moment. Health: "Much too often. One story that comes to mind was a medical office discarded boxes of customer information into a dumpster with patient information put at risk"	-High frequency of breaches on news -worry it could happen to her -Resignation that it is the way of the world -Aware of health breach frequency -Recalls story of patient files discarded
34	"I follow the news like if Target got their hacked you know I'm going to watch and look for that and pay attention. And if any other company that I do business with reports some sort of data breach or hacking, I'm going to try reset passwords or do whatever they advise to do." "I'm sure some of the organisations that have been hacked might have had some varying levels of personal data that might have included health but for the most part but they're like consumer based organisations where it could be what kind of medication I buy but I haven't ever heard about a large health organisation being hacked. Or famous peoples' health information"	-Aware of breaches of large organisations -No awareness of breaches in health organisations or health information
35	"Oh yeah it happens all the time. Like they share that information with employers, so much information and it can drastically influence peoples' lives. It happens a lot. I don't seek out those stories but it happens and it happens to guys in our job. It worries me and makes me more protective of my information."	-Broad awareness of health data sharing -No specific stories but aware of people who were affected by health data sharing -More protective of his own information

Interview Participant	Answer	Extracted Meaning
36	<p>“You read about lots of stories. Some of my friends have had their credit cards misused but they got the money back eventually. I remember the big breaches in stores like Target. They were particularly scary. It was definitely concerning because I have been to those stores. I hope they’ve sorted it out now.</p> <p><i>Health</i> “Occasionally. Less so than stories like Target but you definitely hear stories about employees being fired for unethical behaviour and breaches too on a lesser scale.”</p>	<ul style="list-style-type: none"> <li>-High frequency of stories in news.</li> <li>-Friends have had experiences</li> <li>-Big breaches cause fear as she has been there</li> <li>-Health stories are less common but aware they occur</li> </ul>
37	<p>“My mom was recently diagnosed with type II diabetes and I swear not even a week later I was getting phone calls from they sounded foreign and they were asking about it and they were trying to sell her diabetes products and her doctor’s office claims that they know nothing about how it happened but I sincerely doubt that and they hounded her for months until I visited her and got the phone number down so we made sure that they couldn’t call us and I signed them up for the U.S. do not call register so those calls have stopped but it was just kind of scary how quickly her information was released uh so ye I think it’s definitely important.”</p>	<ul style="list-style-type: none"> <li>-Negative experience with his mother’s health data</li> <li>-Scared of how fast her information was shared</li> </ul>
38	<p>“I really don’t know but they might use it. It depends if it’s something which they have cured it, it was something like a big disease or something which they have done then most of them I think they share it.”</p>	<ul style="list-style-type: none"> <li>-No specific stories</li> <li>-Aware of the many uses for personal information but less aware for health</li> </ul>
39	<p>“It happens all the time. I was in the Blue Cross batch that got stolen.”</p>	<ul style="list-style-type: none"> <li>-Personal experience of health data misuse (see privacy invasion table)</li> </ul>
40	<p>“Not really. I mean I’m sure there are but I haven’t really paid attention. Like I know it happens to people but I’m not really tuned into it, I don’t watch out for it and I’m not sure it’s in the mainstream news enough to make me think about it. If someone I knew had a bad experience I’d be more likely to remember but I can’t remember any of my friends or anyone I know having an experience like that.”</p>	<ul style="list-style-type: none"> <li>-Does not pay attention to stories</li> <li>-Not in mainstream news</li> <li>-Would be more familiar if friend had a negative experience</li> </ul>
41	<p>Hear of celebrities all the time.</p> <p>My friend’s crazy ex-boyfriend took over her Instagram, it’s kind of scary</p> <p>Obama birth certificate “to me that information is private”</p>	<ul style="list-style-type: none"> <li>-Aware of celebrity and friend’s breaches</li> <li>-Unaware of health breaches</li> <li>- Fear of breaches in general</li> <li>- Views health information as private</li> </ul>
42	<p>“Not really. The only thing I think of is my mom used to work in medical transcription and sometimes like I know of times she would bring files home and we could see them and I kind of thought this <i>may be kind of a health risk</i>, when she got into digital transcription you’d pull</p>	<ul style="list-style-type: none"> <li>-Unaware of specific health stories</li> <li>-Aware of possible risks of misuse</li> </ul>

Interview Participant	Answer	Extracted Meaning
	up all their health file online and I'm thinking I'm a good person so I'm not going to do anything but if I wasn't I guess I could. But I haven't really heard of medical data being stolen."	
43	<p>"So a person like that and they popped up and they starting say this stuff and this person was talking in a way where I know that was NOT my friend. Oh yeah like Jennifer Lawrence and all that. Poor thing you know."</p> <p>"No. I think health information, to my knowledge especially with HIPAA and everything is so locked down. I've never heard of anybody losing their health information."</p>	<ul style="list-style-type: none"> <li>-Aware of friends' experience with social media</li> <li>-Celebrity breaches</li> <li>-Unaware of health breaches</li> <li>-View health information protected</li> </ul>
44	"I haven't really looked into it but ye I believe most people might have their information misused. At least with me I use my browser more securely, I disable tracking, I won't go on websites that track I block them explicitly, so for me it's a little bit easier being into to technology but otherwise I believe it would be much more challenging."	<ul style="list-style-type: none"> <li>-Does not search for stories</li> <li>-Views self as more careful and secure t</li> <li>-More challenging for others to protect themselves</li> </ul>
45	"I've heard of privacy breaches in general when it comes to electronic information, I mean we, I feel like in the last six months we've heard several of them when it comes to peoples' credit card information, that's like been posted on CNN, credit card breaches which worries me about everything else that's going on there. Healthcare wise, I guess I know there are needs but then there is, it's like where does that line happen, and I do worry about it but I also it's not at the forefront because, I don't need to go to the doctor as often anyways so it's not like my forefront but I know there's going to be a time where eventually I'm going to start having kids, that's going to be a BIG concern and then I'm eventually going to be older where it's a requirement that I'm going as often as possible that will be more of a concern, now not as much, but when I am in that situation I do think about it."	<ul style="list-style-type: none"> <li>-High frequency of online breaches</li> <li>-Aware of financial breaches, causes concern</li> <li>-Healthcare risk causes concern</li> <li>-Will be more concerned in future when older and has children</li> </ul>
46	"I hear a lot of the breaches and it scares me for my own information. I do not give the health information to anyone but the school."	<ul style="list-style-type: none"> <li>-Frequent occurrence</li> <li>- Fear over own information</li> <li>- Only discloses to health centre- control</li> </ul>
47	Not my personal story but celebrities' photos and things being stolen "I don't understand what the motive would be for taking something that a person didn't give you permission to have and then sharing that with others or with the public, that would be a bit scary"	<ul style="list-style-type: none"> <li>- Celebrity story</li> <li>- Doesn't understand motive for taking information</li> <li>- Fear of information being taking and <b>shared</b></li> </ul>

Interview Participant	Answer	Extracted Meaning
48	“Yeah definitely in the news it’s something you hear. I mean I can’t think of anything super specific other than like <i>Sony</i> , big things like that. I think one friend like lost her debit card and like it was used by whoever found it but none of my friends have never been hacked. “ <i>Health</i> : “I have never heard of anyone’s health information actually being stolen like in terms of people I know or in the news. Like I, because of the things I’m involved like I work at Obesity Solutions, I volunteer at the hospital because I’m involved in those things I’ve done a lot of HIPAA training so I know that it does happen and it’s really <i>important</i> but I’ve never actually heard of it happening to someone.”	-Personal information broad awareness of news -Health information: no stories in news or friends. -Aware of potential for misuse and importance of privacy
49	“I’m not extremely scared of it because the media only reports when something goes wrong. I don’t necessarily think the risk is necessarily as bad the media suggests?”	- Aware of frequency in media - Media exaggeration of risk - Discounts risk to self
50	“Not to anyone that I know, you hear stories on the news about that kind of thing but not that to any person that I’m involved with but I’ve heard stories. I know for me, if someone wants to take a picture of my chest X-ray I’m like okay, for me the financial kind of personal information is potentially more damaging to your reputation or your life than health information. If someone somehow cracked into a hospital and got my student health records, unless there’s a social security number or personal information that could be used to come back to the financial stuff, if someone really wants to look at my blood test results or an X-ray, to me that’s not really that big of a deal.”	-Broad awareness of news stories but no stories of friends -Views financial information as more damaging than health -Less concerned as doesn’t see negative repercussion of health information’

## APPENDIX L: INTERVIEW ANALYSIS: PRIVACY INVASION EXPERIENCE

Interview Participant	Answer	Extracted Meaning
1	<p>“Yeah I think, I think we always are amazed by that because even just booking a flight, they’ll know what dates you were looking to travel if you know what I mean, if you had searched before. That FASCINATES me, they remember. So I don’t like that, because then you’re not going to get it cheaper so I use another user’s name to bypass that which I probably shouldn’t.</p> <p>When I worked somebody had logged into my account, BUT it was okay, because it was one of my own staff and she needed information and at once stage I was a bit worried about it. I would hate it, I would hate to think that somebody else was reading my stuff, I think that that’s everyone’s fear that somebody is going to change, like your bank account that someone is going to change it or rob it.”</p>	<p>-Surprised by cookies</p> <p>-Solution: Technical</p> <p>-Previous work experience but was solved</p> <p>-Main concerns: someone reading her information, changing information, or financial loss</p>
2	<p>“I had a strange one, according to Facebook I went to a school somewhere in Northern Ireland, there was a whole lot of information that was incorrect so I went and I changed all the information. I changed my date of birth to 20 years younger, so that’s the way I deal with these things you know that I completely edit the information. I enquired about something a while ago, blinds or curtains, but I think they’re still coming through you know Google have selected me out for something, but their systems for kind of feeding you advertising information is phenomenal now I just can’t believe how you know you can just mention something and suddenly you’re in a box and you’ll be in that box forever you know. So the overall situation sometimes is alarming but then you know this is the world we’re in, you’d like it to be different and I don’t know if ever it will change. Like every now and then they’ll say right we’ve got this new privacy policy. One of the things that really bothers me about it is, when they say you’ve got these policies and it’s of the smallest print.”</p> <p><i>Health:</i> It’s the things that you don’t know that worry you. I got a letter from Diabetic Ireland they said we’re doing research on retinopathy and we want to take some photographs of your eyes. So the first question I ask is why, why did you send for me, how did you get this information and they say we got it from your doctor. I was interested in what these people were going to do and I said you’re examining me and you’re getting information, what’s going to happen are you going to do anything, you know I didn’t want them researching me just for their benefit, and they say oh it will help us, because I realised Diabetes Ireland is not government funded, it’s funded by people who sell products to diabetics, which makes me</p>	<p>-False information on Facebook</p> <p>-Solution: falsify information</p> <p>-Surprise: targeted advertising</p> <p>-Worry of data collection</p> <p>-Resigned to the way of the world</p> <p>-Concern that privacy policies are unreadable</p> <p>-Contacted by company for research information shared by doctor</p> <p>-Feels there is commercial aspect</p>

Interview Participant	Answer	Extracted Meaning
	believe that there's a certain commercial aspect to it that I wouldn't be too cooperative on, if they said to me oh that retinopathy we're going to clear that up that'll be gone."	
3	"There's a website called haveibeenpwned.com and you can enter your email address or a website username in and they can check if your email address has been used on a site that has ever been breached. I used it and found that my email had been affected by Adobe and obviously they advise you to change your password and you'll be fine. I try not to be surprised or expect any safety online but the Adobe breach did kind of take me back a little. Other than that, I'm never surprised."	-Experienced breach -Surprised -Outcome: change password -Does not expect safety online
4	"I don't like when I search for something on google then go on to YouTube and it's in the ads shown to me sometimes that can be a bit freaky, you can't search for something sensitive or private really. The same with Facebook ads it kind of annoys me to be honest. A few times people have said to me oh I seen your cousin is engaged– but they might not be friends with my cousin, it makes me think like if my friends like my stuff do all their friends get to see it too? I don't share secretive stuff but you've no say over anything once you put it online."	-Surprised and irritated by targeted advertising -Concerned by who can see information shared online -Perceived lack of control over information online
5	"If you google something and then Facebook or google is reminding you to take your contraceptive pill. I think it's worse if they do it with your health data because that's so personal they shouldn't be using that to target advertising." <i>Health Experience:</i> "When I started working in the hospital I was like 16 working in medical records and I had really sweaty hands, and I sent in a letter from my GP asking could I get an injection to stop the sweating and a guy I knew was the secretary for the clinic so I just didn't attend my appointment and I prayed for weeks that he wouldn't have read my referral letter and he did and he said it to me at a party and I begged him not to tell anyone. Like at this age I wouldn't mind I wouldn't be embarrassed by that but at 16 I was so embarrassed. People who work in healthcare organisation see our information and if you know them or even fear someone you know might find out it can be very upsetting. Now different things might embarrass me but it's the same principle."	-Irritated by targeted advertising online especially with health data -Experience of someone viewing her health data Outcome: Embarrassment
6	"I didn't realise how prevalent cookies had become wherein when I looked up trainers on a sports website for days after that any site I went to would have the side bar of ads with those trainers on it. And then amazon I was searching for headphones and now I get one or two emails a day of what I've searched and I get emails of what's on sale when all I've done in my mind is browse I should be able to go on and not get inundated with emails."	-Frustration with cookies and targeted advertising -Desire to browse without advertising



Interview Participant	Answer	Extracted Meaning
7	“There’s a few like searching for something on googling and getting ads for days about it. Sometimes they are useful like suggested pages on Facebook based on what I looked at or read previously or suggested films on Netflix. I think when its ads it’s more annoying because the commercial motive is so obvious. Who they share my preferences or searching with or a profile based on that is another thing though.”	-Frustration with targeted advertising when commercial element is evident -Aware of possible information sharing
8	“The questions that are asked are excessive, you’ve to answer so many questions and provide information that you deem to be sensitive. Or even when you’re filling in an application for a job you’ve to answer all sorts of questions about your health history I know some of it might be relevant but some of it isn’t and could damage your chances of getting said job. That’s scary like I don’t want the world to know this information. Targeted ads too is very upsetting. I don’t think anything is ever hidden and I know you can go incognito but I don’t think it really is. Like if you find a lump, you might just want to google before going any further or telling anyone and you want to forget you ever googled it but now you’re being targeted for breast checks even if you found out you’re okay or you’re awaiting test results its very upsetting and you want google to forget you ever searched for it but no they just won’t.”	-Information required to buy things or for job applications can be excessive and irrelevant -Upset by targeted ads especially for sensitive issues and the permanency of searches -Doesn’t feel she can browse safely -Fear of people accessing sensitive information
9	“I was ordering stuff online from a place I ordered on years ago which I completely forgot about and then they had my details, and it was my general details and it was for a previous address and it was an order from 06 or 07 so I was like you keep stuff for that long yeah so I was definitely surprised at that. With LinkedIn every time you sign in they have your emailed address entered and they’re ready to send an email to everyone you’ve ever emailed inviting them to connect with you. That one annoys me viciously and it’s automatically selected like I’ve seen people caught out and they’re sending emails to people they don’t know or people they don’t want to know or ex people and that’s the annoying part, I don’t agree with it at all.”	-Surprised by permanency of information stored by companies -Frustrated that automatic option is to connect ex. LinkedIn
10	“Some ads are tailored to your searches which is what always happens to me like say I look up River Island and then it could come up ads for different clothing sites when I’m online the next day. It annoys me because they’re taking this information and it’s like what do they know about me, what do they have and then at the same time it would only be clothes so it would only be kind of minor it wouldn’t be like a massive issue for me.”	-Targeted advertising causes worry over information collection and storage -Discounts risk as not sensitive information

Interview Participant	Answer	Extracted Meaning
11	N/A	-
12	“I was very surprised recently, I got this bowel screening thing out and I’m saying where did they get my name from, and I read the letter and it’s saying that the department of social protection have given us names and I kind of thought that was some sort of an invasion, without your knowledge. I know in one way it’s good but in another way I thought how much information is out there about me, and who are they giving it too and who can tap into it?”	-Experience of information shared without her knowledge -Sees benefit in sharing for health screening but concerned about volume of information that exists and who it may be shared with
13	“I got a letter from my gas company to say your number accidentally came up or whatever, people had robbed or got on some site where you pay your bill, that did frighten me that people were getting my pin number so I wouldn’t pay direct debit that I’d pay my bill myself in the post office, but since then I’ve gone online for all my bills, again, because it is handier, it’s more convenient. They really didn’t go into that (the risks), they really didn’t, and I didn’t ask, being honest I didn’t ask, I just took it for granted it would be safe.”	-Experience of breach (pin) -Frightened and stopped paying online but has since gone back online due to convenience and discount as incentive -Was not informed of risks, didn’t consider risks - Assumed information would be safe
14	“I was giving plasma and I understood at the time that they were just using my plasma solely and they weren’t mixing it in with anything else, but it transpired that they were using it with stuff they were bringing in from the States. Oh it was very nasty and then they denied it and like they’re all pros, they’re all doctors, the minimum qualification in the plasma clinic in the blood bank was staff nurse, minimum, they were all high tech girls. I wrote to them and didn’t get any reply and then it all turned nasty and I told them I was never giving a donation again but it didn’t really matter because I was 64. I would still give blood today if it was required.”	-Experience of plasma being misused -Outcome wrote angry letter and refused to donate further but would donate again if needed- benevolence
15	“I don’t know with ads I tend to block them, I don’t want them, I mean I’ve booked a place with like forever holiday homes but if you scroll down right at the bottom is unsubscribe so I do that. One of the worst for sending emails is Facebook and they’re telling you you’ve notifications which you haven’t, but they keep looking for details, I wrote in the box mind your own business one time.”	-Blocks ads and unsubscribes -Frustration with volume of Facebook emails and information seeking

Interview Participant	Answer	Extracted Meaning
16	“Well I don’t even know how I’m on LinkedIn. I got my daughter to delete it, I don’t want it but I couldn’t get off. And now the ads pop up on the phone all the time I could be Googling one thing and an ad comes up about it could be car insurance, it could be house insurance, it could be about cosmetic treatment, they all come up. I don’t mind I just think it’s a bit of information that comes up, you just read it you don’t have to do anything about it, you don’t have to act on it, so it doesn’t alarm me because it’s only general information. But if it was more personal, I wouldn’t like it, I would be too alarmed by it.	-Negative experience: LinkedIn unaware how she got a profile -Okay with mobile ads because they’re general -Personal ads would cause alarm
17	“I think Facebook is very invasive, now all my kids are on it and I know I’m on it because they have me on it right, I think to find out how to use my iPhone and my computer that’s where I’m at the moment I don’t need another thing confusing me you know. There’s too much information on there you know. I do get the ads that does come up I just go into the red button and turn them off, I never click.”	-Views Facebook as invasive too much information -Solution does not use it -Avoids ads -Limited comfort with technology
18	-	-
19	“I don’t trust Facebook; I think the older people are more scared of it than the younger people. And I don’t think I need it you know and I would hate to think that they’d be putting photographs of kids and all that up on Facebook. And I really don’t think that if I go to a party in your house that anybody strangers taking photographs of me should be free to put them up on the Facebook, there’s too much freedom on it for other people you know for people who don’t want to be on it. And I think that’s your choice not to be, and other people can put you on it because you’re at the party. So does that mean you don’t go the party?”	-Doesn’t trust Facebook -Lack of control over photographs appearing on Facebook
20	“A few years when they introduced the location on Facebook. I was at my ex-boyfriend’s house but then I came home and I uploaded a status by accident. The status had underneath that it was posted from where my ex-boyfriend lived, but it was wrong I was home at the time the phone just hadn’t updated. Anyways people commented why was I still there. I deleted it but the damage had been done, it was very embarrassing. That really got to me because it was putting information out there about me that wasn’t true and even if it was true, it was information I didn’t want to put out there. Since then I make sure all apps like Facebook have location services turned off. Another time, I booked a hotel conference centre using my work phone, email etc. and a few days later I started getting emails about the spa and holidays in the hotel to my <b>work email</b> . How unprofessional. So I rang them and I made them remove my email and all my details so they didn’t send me anything like that again.”	-Experience of false information shared – embarrassment -Solution: turn off location -Emails received to work email -Solution: Complain

Interview Participant	Answer	Extracted Meaning
21	"I've noticed say that Facebook ads tend to be targeted, for my age profile and that, despite the fact that I've put in a false date of birth to avoid giving away good information because I feel like that's a very stupid thing, it's how, it's how they make their money. My understanding of free internet services is that if you're paying for a service you're the customer and if you're not paying for the service you're the product. So, I haven't been surprised by privacy breaches because I'm fairly careful."	-Targeted ads: aware of commercial aspect of online services -Solution: Falsifies information -Views self as careful
22	"All the emails, the spam wrecks my head but I know that everything you do is monitored even on Facebook you get ads for you and you're just like how do you know that I was looking up these sites? I suppose like it's the world we live in though really. I know you're tracked for most things you do online even when you're doing your shopping they're looking at what you buy and they're sending you out special offers, so I suppose yeah everything is tracked."	-Spam causes annoyance -Aware of monitoring online and resultant ads and offers -Resignation to the 'way of the world'
23	"If I pay by credit card and you type in your name and all the details come up automatically that surprises me and it may not have been the same website and you're trying to remember how did this company get your credit card. That surprised me initially but now I kind of expect it. I remember saying to my husband 'How did that get there?' and there are times when I feel strongly about it and I say what that's ridiculous that's my details but I'm used to it now."	-Surprise of Cookies -Expects it now but often feels strongly about it
24	"I'm an academic so a lot of the information about me is online and it has to be because it's a global academy and so in that sense, I'm always a little surprised when someone has heard of me but I guess no I haven't had a major impact that I can think of but I'll keep thinking about it because I feel like I'm missing something."	-No specific examples -Aware information is online about her but surprised when it travels
25	"I've certainly given information out but I wouldn't be frequently giving anyway I was concerned about. So no, not myself. But I don't think we understands what happens to the information we disclose. Without getting too philosophical, if everything is based on data then individualism and you know people doing something because they just feel like it and not because they're likely to do it based on the sample we've looked at, that will be problem. In fact, it probably already is. I mean I would prefer people to trust the serendipity a bit more and not just do what they're expected to do you know."	-No specific example -Careful with information disclosure (frequency and information type) -We don't understand what happens to information -Fear focus on data has negative societal impacts
26	"I don't think you're always going to have the control you did in the past. That's the world we live. Information becomes a fact of life. I've had two credit cards stolen in. Everything was sorted within a	-Previous experience: financial

Interview Participant	Answer	Extracted Meaning
	week, I feel like that's something that will happen more and more going forward but they sort it quick and easy. That helps take a lot of the negativity away from the experience. I think there's enough safeguards in place and these companies do whatever they can to protect you and take fraud very serious. My credit card company return any charges I deem fraudulent but I think it will be a much more commonplace occurrence going forward."	<ul style="list-style-type: none"> <li>-Outcome: sorted by company quickly</li> <li>-Less control over information than previously had</li> <li>-Likely to become more common but sorted quickly</li> </ul>
27	"I have never had it happen to me personally, I mean I don't know if my information has been used in ways I disagree with, I guess I hope it hasn't. Now that I think of it my credit card was used by someone before like \$500 but it was sorted out really quickly which helped, it eased my mind a little. I think things are getting more secure but you always need to be careful. I wouldn't post too much information and wouldn't buy online from sites I don't know.	<ul style="list-style-type: none"> <li>-Unaware if information has been misused: 'hope'</li> <li>-Financial loss: resolved quickly</li> <li>-Perceives security is improving</li> <li>-Limits disclosure and purchasing</li> </ul>
28	"It's not happened to me that I know of at least, maybe it has happened before but nothing that I know of."	<ul style="list-style-type: none"> <li>-Unaware of any invasions</li> </ul>
29	"I've gotten viruses on my computer before so that has the potential for my information to be misused but not I'm aware of that. I had surgery two years ago on my right wrist and that's when I became aware that my information was being shared because I was a special case so they shared with other arm and hand surgeons but they told me that and that would be the only time that I am aware that my information was actually shared that publicly."	<ul style="list-style-type: none"> <li>-Viruses: potential misuse but unaware of any resultant misuse</li> <li>-Health information widely shared as special case but was aware</li> </ul>
30	"It's weird now when you sign in on any computer, when I go to Google Chrome all my favourite tabs are there. It's weird that it looks the same as my laptop because it knows it's me but nothing really scary has ever happened to me."	<ul style="list-style-type: none"> <li>-No invasion experience</li> <li>-Surprised that all computers 'know' it's him</li> <li>-No scary experiences</li> </ul>
31	"No but it's true you have to be careful with what you put out here. That's the first thing we do here when we hire we go on Facebook and other things, it tells a lot about who you are.	<ul style="list-style-type: none"> <li>-No experience but stresses need to be careful about</li> </ul>

Interview Participant	Answer	Extracted Meaning
		disclosure as contributes to online identity
32	“Not really because I know most of the stuff I use, like the ‘Lose it’ (diet application) right it’s recorded online and all my calories and things I ate and I’ve to log into my account. I’ve never been like a victim of oh how do they know that, I don’t what that information out.”	-No experience as aware of information disclosed so no surprises
33	“I’ve noticed if I have pages open at the same time my Facebook is open, the site will start showing ads or information related to the topics from that page. I’m kind of resigned to it, but it’s still kind of creepy, and I often close all the other pages before I access Facebook. Mind your own business! In terms of security breaches, not that I know of! I hope not but they happen so often I could have been involved but not informed how bad would that be?”	-Facebook ads surprised but resigned to it. Closes pages -Aware that her information may have been breached but she has not been informed
34	“My identity got stolen this week. It’s been a pain dealing with, thousands of dollars were charged and I was getting credit score notifications, so that sucked. I had to get my cards closed, get new cards issued so I’m waiting for that and for them to refund money. It was surprising and it’s weird because I don’t use my debit card a lot I try use credit cards but we all pay things online and so I’m wondering if that happened. It’s scary, do I go about business as usual or am I doing something wrong should I be more cautious? It’s the second time. It happened over five years ago. I think we have a false sense of security and people are not very savvy with internet security. And there’s always going to be people that try and take advantage unfortunately so it’s more likely today than ever before.”	-Identity theft experience x2 -Financial loss and credit rating -Unsure how it occurred and how to prevent -View that will become more common due to false sense of security
35	“I actually have. In order to do my job, I have to be in tip top health, I have to get a physical almost yearly. We’re watched pretty much. So I’m very sensitive about my health information because any potential mistake on my physicals or applications has the potential to put me completely out of work. So I go to a physical and I go to a third party, an industrial doctor he and so I get the information. He says I have to send this off to your union doctor I said ‘wait a minute you’re a doctor and I’m here so we’re going to pass this information off to another doctor, I don’t like it’ and I actually didn’t sign the consent form. So I get a call from the union and they actually have a doctor that looks for mistakes on the physical but I don’t like my information shooting out everywhere, it’s very critical that everything is right.”	-Experience of health information sharing -Refused to consent but when informed of reason consented -Protective of health information due to potential impacts on career
36	“None that I can think of. I think it gets used a lot but I’m not too aware of these uses and I can’t think of any examples of surprising uses. There have been some major breaches in recent years but none that directly affected me that I have been aware of. I hope not.”	-No experience: Hope -Unaware of how information is used

Interview Participant	Answer	Extracted Meaning
37	"I don't think, not that I know of. I've actually been good. I get my healthcare through the VA in 2006. Tricare the main healthcare insurance in the military had 5 million users' information stolen. I don't think I was a part of it I don't think they sent me a letter to say I was included."	-No experience to his knowledge
38	"No not much."	-No experience
39	"“I was in the Blue Cross batch that got stolen. We got a notification saying that it's possible our information will be used and to monitor every time and if they need to they would pay for identity theft recovery if they need to which is you know terrifying especially you know with health stuff you don't think of it as being something that you know maybe that's going to affect how I receive healthcare in the future. So they don't confirm which numbers were taken and which weren't so you're left in limbo.”"	-Health information experience -Unaware of whether information was subsequently used -Terrifying could influence future healthcare
40	"I guess I just know that they always track you. I know if I search for something I'll get ads for it. I know they do that. So even if I'm searching like say I have a client who is taking some medication and I look it up then I'll be getting ads for that and I know it's not necessarily related to me it's because I know that I did that search so then it doesn't really bother me."	-Aware of targeted ads but all searches and ads don't relate to her so doesn't cause concern
41	"My first shock initially, like wow someone else can see my data and my information was my first credit report. I was like what happened here. Or how people can just go into a store and get my social security number how easily they can pull up my information and I guess that was shocking how everything is linked when you give them some information. I guess I've never experienced someone just taking my information but even that like I was like that's my information like why do you have that, how did you get that, why do you need it sort of thing which now I understand in some instances like the credit report."	-Surprised by data linkage and ease of access to information -Understands need for information in some cases
42	"I've gotten identity protection twice from Sony because their record banks have been hacked so I've gotten 3 or 4 years of identity protection from them because they took names, addresses, credit cards, browsing habits. And it was bad enough that however many million people that were subscribed to this particular service got identity protection from them like who knows if they did anything with the information so that was definitely the biggest one. I was also involved where people had like names, phone numbers, addresses stolen from Target and they had to send everyone information saying 'hey you could be involved in a lawsuit you could stand to gain it all depends on whether or not your information was used' So like 3 or 4 significant times I can remember getting something in the mail from those companies so. The first time it happened especially with Sony I was afraid I thought what are they going	-Several experiences of large breaches -Identity protection gives sense of security -Less fear with each breach

Interview Participant	Answer	Extracted Meaning
	to do with my information, I changed all my passwords, I looked at the company I was like what am I getting in my identity theft protection stuff. Second time it happens I was like <i>really you couldn't fix it the first time</i> . And every time since then it bugs me but I worry less because I have identity theft protection now so I'm not as worried about it as I could be."	
43	"I've had my email hacked and I've had my Facebook hacked. I had to totally close down my Facebook and start another one because somebody decided to hack. Luckily I'm not that important of a person I don't think, so I'm thinking really 'why would anyone care' and how would they ruin my life. I don't feel like there's anything that could be done to me. I don't have anything like that but potentially a person could get kicked off their insurance but what can you really do? I don't really understand the detriment there you know what I mean. I could see where like say I'm a transsexual. That being exposed could cause more of an issue."	-Email and Facebook hacked -Discounts concern as not high profile and no information that could be sensitive -Doesn't see any repercussions for self
44	"No I use my browser more securely, I disable tracking, I won't go on websites that track I block them explicitly, so for me it's a little bit easier being into to technology but otherwise I believe it would be much more challenging."	-No invasion experience -Perceived safety due to security measures
45	-	-
46	"No I don't give the information online. I give my health information to the school here because we have to, we are asked to do that...but I don't give my information to anyone else especially about my health information. I would not like to give it to lots of people."	-No experience as limits information disclosure
47	"When you're checking your email and things come up from websites you didn't sign up for things like that when I know I didn't sign up for that, I know it's someone probably selling the information that I gave them and it bugs me. My parents just had their social security numbers stolen and that was probably from one of the big breaches but with everything being as interconnected as it is, I think it's almost impossible to avoid that happening. It obviously doesn't feel great being violated like but unless they come up with a great security system at some point it's probably unavoidable with how interconnected the world is."	-Ads cause concern for information being sold -Views breaches as unavoidable due to connected world
48	"In one of my classes we were talking about surveillance and how everyone's information is like completely exposed but it's not super surprising but one thing I don't like is the tracking of what you're searching for and how much they tailor advertisements, it's kind of creepy."	-Aware of tracking -Finds targeted advertising creepy
49	"The first time when I realised the power of data was when I identified as gay and then ads targeted at gay people started coming up it took me aback a little. I'm okay with now but I was surprised at first."	-Surprised by targeted ads due to sexuality -Became accustomed to it



Interview Participant	Answer	Extracted Meaning
50	<p>“I had my debit card accessed and I went to the grocery store and my card wouldn’t swipe. I checked with my bank they had actually suspended it because of suspected fraudulent charges so someone had got my banking information. I had to close the account and get a new card and all that nonsense. But the bank spotted it first and it was weird because I noticed one charge I couldn’t remember and I was like alright whatever but then a couple more happen and the bank themselves said no that’s not right and they shut it down. I wish they would have told me but that’s actually cool they did. I use online stuff all the time, so it’s going to happen eventually, fortunately it wasn’t that big of a deal it wasn’t thousands of dollars and the bank was able to reverse those charges.”</p>	<p>-Experience: financial loss          -Minor and resolved quickly          -Resigned to the fact this will occur online</p>

## APPENDIX M: INTERVIEW ANALYSIS: HEALTH INFORMATION SEEKING

Interview Participant	Experience	Process	Views on risks and credibility	Extracted Meaning
1	“Not for me because I’m quite healthy, but my son had boils and I looked that up online and I read all about it, so he went to the doctor and he got an antibiotic. He was actually doing a lot of training and he wasn’t showering immediately after, I was like you have a sore and then there’s an infection so I <b>learned</b> . I think it’s very good that you can look up stuff. The doctor didn’t ask that question it was only I said it.”	“I just put in the question and whatever comes up, it needs to capture my attention immediately and not waffle on and then I go back, or sometimes I go to page 6 you know what I mean just to see because sometimes you get better information, so sometimes I do that with searches.”	-	<ul style="list-style-type: none"> <li>- Doesn’t search for self as healthy</li> <li>-Positive experience identifying a health issue</li> <li>-Source of useful information</li> <li>-Process: Search for issue, concise information, search for secondary sources</li> </ul>
2	“I certainly wouldn’t be rushing to myself, but I would look for somebody I know who’s unwell. My sister has dementia, and I would look up everything I could find about dementia. I wouldn’t for myself, I would for my wife. She had breast cancer so I looked up that when I got the computer to see the prognosis long term. I don’t know why because it was a very worrying time, and I got prostate cancer so that got looked up. So you do get curious about certain things, but maybe because I don’t have a lot of illnesses at the moment you don’t really have any reason to go on a pessimistic view.”	-	-	<ul style="list-style-type: none"> <li>-No strong desire to seek information for himself</li> <li>-Seeks all information for sick relatives</li> <li>-Seeks information for self in certain situations i.e. serious illness</li> <li>-Views information online as negative</li> <li>-Reason for seeking: curiosity</li> </ul>

<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
3	“Yeah well, who hasn’t?! If it is something I don’t think is going to be serious I’m going to google what it is before contacting a doctor or pharmacist.”	Google search. “For exercising Reddit is very good exercise I’d learn a lot on there.”	“Well like I don’t think you can really trust what you find online.”	-Assumption of normality -First port of call for non-serious issues Search engine and Reddit - educational but not trustworthy
4	“I’ve googled symptoms. When I was pregnant I’d search to see if the symptoms I had were normal or if I was worried about anything. I’ve often searched for diet tips or recipe tips if I was following a diet but I used it a lot more when I was pregnant. I don’t know if it was because it was my first baby whereas I know if I’ve a headache on a normal day I could be dehydrated.”	Google and ‘fertility’ forum. People from all over the world were part of the forum. When I got pregnant I shared my story. I never gave my real name but it was good to hear stories from people with the same experience. It was great for advice but I never shared my struggles.”	“I mean I wouldn’t search on a normal day if I had a headache because you could get any kind of answer... you might end up thinking you’re dying just cause you’ve a headache.”	-Searched more during specific period: pregnancy due to inexperience -Risk of ‘extreme’ answers and ensuing worry -Benefit of community environment -Limited information disclosed to positive and anonymous ( <i>information boundary theory</i> )
5	“Yeah all the time. A lot of the time I look up diet tips if I get on to the newest fad diet I’ll look up for tips on that or what people are saying about it. I also look up the newest exercise fads and recipes like healthy eating recipes. I’d get a lot of information about how to be healthy that’s where I get it all actually. I look up types of headaches. I often look up stuff for family too like symptoms. Any strange symptom like a strange sensation in my thumb I’ll look it up, the internet would be my first port of call.”			-Regular user -Variety of health information -Seeks information for self and others -First port of call for symptoms and source of all ‘healthy living’ information

<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
6	“I have. One time when I got results back from a doctor and I didn’t want to go back to the doctor I looked up what it could be on the internet and decided I didn’t need to go back to the doctor when I found out why my bloods could have been slightly off. What I found online made sense for me. Sometimes I look up random stuff not always related to me when I hear something on a show. I would look up weight training programmes and I would go on websites like Men’s health the magazine.”			<ul style="list-style-type: none"> <li>-Experience seeking information to explain health issue</li> <li>-Information received was valuable</li> <li>-Seeks information out of curiosity</li> <li>-Seeks fitness information often</li> </ul>
7	“Yeah. It’s kind of a cliché not to look up your symptoms online but it can help it can at least give you an idea. I find with diet as well I struggle to put weight on so I often look up high calorie foods.”	“I’d use it more so for sporting injuries so if I have a pain in my hamstring I might look up how long should this strain take? I don’t have access to a physio so you have to kind of self-diagnose that kind of stuff unless you want to pay.”	“I wouldn’t take anything I see online as given.”	<ul style="list-style-type: none"> <li>-Views internet as helpful source</li> <li>-Uses for sport and diet information</li> <li>-Need to self-diagnose</li> <li>-Exercise caution with online information</li> </ul>
8	“I am a deviant for searching google for everything. I recently had a bad creak in my neck so I was diagnosing myself with every illness under the sun due to what I found on Google. But I would kind of google anything that kind of worries me, which can be a lot. “	“My son recently had tonsillitis and laryngitis so I was googling baby’s loss of voice anything that’s wrong with my son I would google first and then maybe contact a pharmacist or doctor.	“The information online you have to be careful with how much you read and what sites you’re reading because it can add to hysteria.”	<ul style="list-style-type: none"> <li>-Very frequent user</li> <li>-Searches anything that causes worry</li> <li>-Asks person first, then internet before seeking professional advice</li> <li>-Need to exercise care as information can be extreme</li> </ul>

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
		Well first I'd ask my own mam or other parents I know cos they're a more trustworthy source."		
9	"Yes I do all the time if I feel queasy or if I had some symptoms I'd google it straight away and if it comes back with generally what it is then ye I would go to the doctor if it was serious."	"I just basically pop in it to Google and see what happens, I don't look at one site, I'd look at 2 or 3 or 4 and if there's a correlation between them all I'd probably assume that would be the right answer."	"I think if it was something generic like a cold I think that's okay but if it's something more specific or if there's symptoms that are like something else are like a common cold but are actually something more drastic I think that's where it can be dangerous."	-Very frequent user -Searches prior to seeking professional advice -Google search utilizes many sources and self-diagnoses -Danger in misdiagnosing serious conditions
10	"I do all the time, yeah. I wouldn't really do it to get a diagnosis I'd more do it for peace of mind, I wouldn't be like oh my god I'm dying I have cancer I'm going to die in the next 5 minutes, I'm more like okay this is fine it's nothing too serious."	"I'd mainly use Yahoo answers which is not a great site, or else WebMD."	I know not to (trust it), it's completely inaccurate like everything on the internet but I just really do it for peace of mind so I kind of would trust it for that but if I knew myself something wasn't right I would go straight to the doctor I wouldn't go to the internet."	-Very frequent user -Use for comfort -Uses sites -Does not trust information for diagnosis
11	"I needed to get an operation, so I Googled and got quite a lot of information on it and some of it I didn't like. I did Google, and I did Google the aftermath and how to take care of it."	Google	"I did use the internet for that purpose, but it's broad, it's subjective, its commonality, and it's for everybody. I wasn't looking up my own records."	-Experience during specific event: operation -Used it as an information source -Does not view his use as specific or customized to him
12	"Yes, yeah I do a lot of the times because I've had a problem with my hip for the last	"I google stuff like the Mayo Clinic."	"I do go into these sites alright for a bit of craic and	-Very frequent user – related to health issues

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
	5 or 6 years and I've seen so many orthopaedic guys, this time one tells me it's my hip, one tells me it's my knee, the other tells me it's in my back, so I'm all the time googling."		somebody says I've a pain in my big toe do you know what it is, and you hear all these funny answers you but if I want information I stick to the safe sites like the Mayo Clinic or there's one in England which is good."	-Uses 'credible sites' -Aware of forums and 'funny answers'
13	"Yes. I had to go for a procedure about 5 years ago, and of course I googled the procedure and I nearly knew how to do the procedure when I got into the theatre, and I got myself so nervous that my blood pressure was like so high and I had myself so frightened, and I should not have done that because it told me the pitfalls, yes there's pitfalls to anything but of course I zoned in on those pitfalls you know about what could happen fatally to you, instead of the positives you know. I still do it even though I know I shouldn't."	The Mayo Clinic I go on to, I find them very comprehensive, they're renowned so I go into them a lot because I trust them. I've noticed too sometimes when you Google something you'll get peoples' opinions and that surprised me. I think Mayo would be from medically trained people."	"I think that can be very dangerous because it's always like the most fatal. I tell patients not to do it. I think if they go online sometimes they can misread, especially if you're not trained and even if you are trained, you can misread and read more into it that there is, you know."	-Used for specific purpose and in general -Views as dangerous for medically trained and untrained people – danger of overreaction -Uses Mayo Clinic due to reputation
14				
15	"Oh I do. Not personally, well I have, I'm very healthy, but my wife fainted, so she went into hospital and all, so I would go on and she'd have low blood pressure and I'd look you know at the causes things like that and try and find out, I found out for her eczema actually that you can get ultraviolet lamps that do help, they won't heal it	"Eh if it's something specific I'll just put it in I don't google the site, I'll just put it in to Google, click and see what I get."	"I don't believe it, a lot of it I don't take their word for it, I go on and look and the reviews."	-Uses for wife -Useful source of information -Search engine -Doesn't believe all information -Looks for reviews

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
	completely obviously but they do help ease it.”			
16	“I Google a lot about health issues, especially when my sister had cancer, I Googled an awful lot about that. When she got Motor Neurones, I had no information I Googled all about that. I Google an awful lot of things that relate to my family. When I got an operation on my foot, I Googled it all the time. I had myself driven mad, because I got too intense about it and I used it too much. I didn’t Google it beforehand, I only Googled it when I couldn’t move. It affected my emotional wellbeing.”	“I wouldn’t be too familiar with it because I’m not that great on the computer, say I want to find out something about diabetes I’ll just type that in (to Google), I wouldn’t know individual ones (websites).”	“You can get obsessed. I was diagnosing all sorts of things that weren’t happening, I thought I’d never walk, for 3 months, Googling and looking at surgeons performing operations. I took it to the extreme and it got dangerous. You could you’re at death’s door, that’s very dangerous, some people are obsessed.”	<ul style="list-style-type: none"> <li>-frequent user for family issues</li> <li>-Used for self for specific purpose: operation</li> <li>-Negative impact due to information online</li> <li>-Searches on search engine and reads as much information as available</li> <li>-Danger of hindering recovery due to information online</li> <li>-Misdiagnosis</li> <li>-Danger of addiction</li> </ul>
17	Yeah because I was put on this Fodmap diet for a Barrett’s oesophagus, and I didn’t want to be on that thing looking to see what I could shop for you know, but I did, I would know how to do that now. Or tablets you’re taking I would look them up for more information, yeah. And that never goes it’s always there. I remember I was sending away for something for down below, right, and I tapped it in and all these sites came on, no you can’t control what you get back, I said no that was it, that’ll be in my history. Now that’s what I would be nervous of, we have no security and I feel there’s no privacy in computers and I would be nervous of that.”	Google	“I looked that up so I knew what was wrong with me, or I knew words that they were using that I might not know what they would mean. I would look that up but not necessarily I would take what they say on the computer as Gospel.”	<ul style="list-style-type: none"> <li>-Little experience</li> <li>-Feels lack of control over information received</li> <li>-Fear of permanency of searches</li> <li>-Exercises care in interpreting information online</li> <li>-Uses for diet information and understanding medical terms</li> </ul>

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
18	No	-	"I've often heard of people doing that but no I think you can get caught up in different things you think you're dying."	-No experience -Aware of extreme information and outcomes
19	"Not really, I've never done that. I probably would like to. Well it would be something I should have done a long time ago if I was all that interested wouldn't you think?"	-	Well they kind of always say don't Google it don't they? No matter what it is don't Google it because you do become addicted you know. I wouldn't like to become addicted."	-No experience -Aware of risks of becoming addicted to seeking information online
20	"I would do. Irregularly. It would mostly be for fitness I might look up healthy recipes. I have friends working as personal trainers so they post healthy meals and tips on Facebook. I would look at them and might try one. I also look up new exercises. Dad is a diabetic so I look up things for him, tasty recipes. I wouldn't look up anything related to actual <i>illness</i> too often."	Social media Search Engines	"I think it can cause unnecessary worry and panic. A lot of the stuff isn't validated it's just someone's opinion but it could have a really bad effect on you, so I try not to do that. If it's something trivial but unusual I might google it but I would never take what I find as gospel."	-Experienced but irregular -Predominately for health and fitness (self & family) -Potential to cause unnecessary panic -Aware of validation issues -Would search for non-serious issues and exercise caution when interpreting information
21	"Pretty rarely, 've heard of the terrible disease of internetitis, so I would tend not to."	"...Except for the NHS.gov.uk because it's organised by the NHS in the UK, it has some sort of substance behind it.	"There are too many complete loads of nonsense on the internet to be taking anything else too seriously."	-Rare user -Aware of addiction issues -Uses health department website -Aware of possible false information
22	"Yeah. I diagnose myself with things all of the time. When I worked as a nurse and was a condition that I really wasn't ofay with I'd	"I just pretty much Google and see what happens, everyone uses WebMD	"Some of the information might be skewed. I'd go to the more medical sites and you'd	-Use personally and professionally -Speed and convenience



<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
	definitely Google it and look it up you know. It helps me with things I wouldn't understand or look up a drug that I wouldn't know it's much quicker than using the Mims or going to the big textbook. I do think it's a good source I wouldn't base my whole you know nursing care off the internet, or I wouldn't maybe want my doctor to fully diagnose me based on typing in symptoms but I do think that for a quick overview, informative yeah I think it does have its benefits."	and the Doctor Net. Yeah I wouldn't really have any particular ones I'd type like 'cystic fibrosis nursing care' and you're bound to get something with the diagnosis and the nursing care is around it.	find as you work your way through that some people would be giving their own opinion and there would be scary stats and stuff but I'd look it up for a quick overview.	-Search engine and uses multiple sources including medical sites -Aware of skewed data and non-validated data -Useful for overview information but not complete diagnosis
23	"I search a lot for recipes because I like cooking so I do that a lot. Health information, touch wood, I'm a healthy person I think, and I don't, I might Google something some time but I don't pay too much attention to it so I'm not mad into health information online. My sister swears by it and I think she takes it so seriously it's probably put me off, she Googles pain in the hand and she knows exactly what's wrong, whereas me no."	-Google	"	-Frequent for diet -Infrequent for health -Reason 1: Healthy -Reason 2: Doesn't like health information online
24	"Yes, possibly less than most because my husband is a doctor so if I have a question he would have better access than I do, but you know I would use his database of expertise, but basic things like how long should it take to cycle 20 km or not so much out of fitness or health as interest, So very basic stuff but not really."	"Google, just Google yeah which is probably not efficient or useful, but no nothing specific, my husband uses a website called up to date, but that's not accessible to the general public."	"Am I dying? you always are on Google."	-Infrequent searches for basic information -Husband for medical information -Search engine -Aware of extreme information -Use: for interest

<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
25	“Yes. I would, only if I have cause to. Sports injuries that kind of thing, I’ve been lucky I wouldn’t generally have to look up much but if something came up I would look it up.”	“I would just Google I wouldn’t, I mean I was signed up to VHI there was sort of a nurse thing there, I remember using that in the past but not, no not really. I would not have a go to health website that’s for sure.”	“Well you’re going to fool yourself one way or the other, so I wouldn’t, it’s only for the very minor stuff, if I was feeling very unwell looking it up wouldn’t help me.”	<ul style="list-style-type: none"> <li>-Use if has health issue</li> <li>-Infrequent due to good health</li> <li>-Uses search engine, has previously used health insurance website</li> <li>-Aware of danger of self-diagnosis</li> <li>-Use for minor issues</li> </ul>
26	“I had a bad habit of relying on Dr. Google for a while so if something doesn’t feel right I’d look it up and find out that I was dying so I try not to do that anymore.”	Google and if lots of online sources say it’s serious I would probably go to the doctor to get it checked out.”	“I found I was getting really anxious over things that weren’t serious just because of what I read online. It really wasn’t good. It’s not a healthy habit I don’t think.”	<ul style="list-style-type: none"> <li>-Previous frequent user</li> <li>-Negative effect of anxiety due to online information</li> <li>-Combines sources and then visits a professional</li> </ul>
27	“Yes a lot because of the programme I’m in I do research a lot of health related things online. I used to google symptoms a lot online but I don’t really do it as much anymore. I find myself second guessing what I read a lot more and not trusting everything but I do still check sometimes like last week I had some bug bites on my hip so I googled how to treat them but that’s cos they’re pretty much a standard issue if it was something more serious, I wouldn’t be inclined to google or if I did I wouldn’t necessarily follow all the information or take it as the truth.”	Google		<ul style="list-style-type: none"> <li>-Frequent user for education purposes</li> <li>-Tries to use for minor issues</li> <li>-Exercises caution when interpreting information</li> </ul>

<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
28	"I really don't. Well not too often because I haven't been sick since September, knock on wood but I don't remember the last time I had to look up something for my health. I am constantly exposed to it though because my research project is about fitness blogs so I read fitness blogs all day long not for personal purposes but I still am exposed to it all the time but I wouldn't necessarily go out of my way to research fitness or health."	Blogs	-	-Infrequent for personal purposes due to good health -Frequent for education -Does not actively seek information online
29	"I'm a fairly healthy person so I don't have many symptoms that I would be looking up but maybe once every two weeks if something arises."	"I Google and then check a bunch of different sources. For instance, my dad hurt his leg so I checked a bunch of different sources. I don't rely on one, if I had to I would probably rely on WebMD but normally I try to get as many sources as possible before I make a decision."	-	-Fairly frequent user as need arises -Healthy person so no serious issues -Use for family -Search engine and uses multiple sources before making decision
30	"No. I guess if I have a bug bite or something that's bothering me I might check it out but not very often. I would probably ask someone first before I would do it on the internet."	"I would go to WebMD first because that's what I've heard of and that's what I know."		-Internet not first port of call -Uses site due to familiarity
31	"I really really don't. I'm going through a lot of stuff health wise right now and my	-	-	-No experience

Interview Participant	Experience	Process	Views on risks and credibility	Extracted Meaning
	does look up that stuff and I said as a <i>teacher</i> nothing annoys me more than when a parent walks into my class and said I read this about my kid and I think you should test them for this and it <i>really</i> irritates me and so, because of that I don't look things up and I don't go to my doctor and say read this."			-Has health issues but does not use internet as not qualified to interpret -Personal decision not to use
32	"I might look up a condition, if someone says they have this condition and I don't really know what it is like coeliac disease for example."	"I usually just search Wikipedia and say what's <i>coeliac disease</i> and find out what it says and then if I want to know more detail I might try specific websites like WebMD, or some specific sites that are more detailed."	"A lot of times you'll see things like oh this is terrible. You go to other places and you go well there's no real data to support that or. So there is some risk because you can overreact to something, but for me it's only if you're using it as your only source, to me. Like when I'm doing it I'm like well I'll still go talk to my doctor or to someone that knows more about it."	-Looks up information on other peoples' illnesses -Wikipedia for overview and specific sites for detailed information -Aware of extreme information and risk of overreaction -Solution: look for data supporting and talk to knowledgeable people offline
33	"All the time, probably at least every other day. I suffer dysbiosis, which is a problem with the digestive tract. So I look it up regularly and try gather information and tips from different sources."	"I usually google a certain topic, like dysbiosis, and then visit numerous sites. I like Dr. Mercola's website. I visit that quite often. He's quite helpful and shares interesting studies on various issues and provides health tips."	"You have to be careful and use your brain as to what sounds logical or reasonable. And if you can find multiple sites that support a specific opinion, then check with folks you know to find a consensus. I think finding a balance between searching for answers and supplementing that with	-Frequent user due to health -Search engine and multiple sources including specific website -Reason: information for health and illness -Importance of combining information found online with professional advice -Exercises care and logic

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
			advice given to you by your practitioner and friends. I don't think you should try everything recommended online."	
34	"Yes, maybe once a month. I guess I research more natural or holistic approaches to issues. So I'm already on medication for stuff and I don't want to be on it for the rest of my life or I don't want to have to take a bunch of medication so I'm more researching like what can I do health wise, but I know a lot of people who spend a lot of time in blogs about their health issues, more so to connect with other people with that same issue. I don't really have anything like that."	"I search and see what I get but I go to the more official websites so whether it be a hospital website or a government website or something like that a more trusted site. Like that I definitely don't value Yahoo Answers and random things."	"It can definitely give you some stress and anxiety because no matter what symptoms you have, they're going to be a part of the symptoms for something really horrible, so your mind immediately goes there."	-Experienced user -Focus on holistic or natural remedies -Searches and seeks official websites not forums -Aware of potential anxiety due to extreme results
35	"Sometimes, yes I do. WebMD, I do that sometimes for my daughter also, you know get the background."	WebMD "just because it's so comprehensive."	"A lot of that stuff will scare you to death so you have to be careful."	-Uses at times -Reason: background information -WebMD: Comprehensive -Aware of extreme information
36	"Yes, I would do quite often, I'd say several times a week."	"There are websites I use regularly, I found them based on google searches. So WebMD is the main one for any strange symptoms or illnesses, it's quite good. I still do a google search to see what	"Those two websites are quite respected I think and they're offering validated information and real peoples' stories. I think you have to be careful with random sites but I've found good ones that I like to go to."	-High frequency user -Uses two websites for symptoms and fitness -Seeks validated information and information from people -Aware of need to be cautious -Does not contribute but likes to read

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
		I find. I also visit a isagenix.com regularly. It's a popular fitness website. I would buy health products and read stories of peoples' progress. I wouldn't post, but I like to read them."		
37	"I've done it before but I don't take it seriously. Because I'm not a doctor, so I could at most use it to assist the doctor or the nurse practitioner or who I'm seeing, maybe the website describes what I'm feeling <i>better</i> than what I can describe it. So that's at most what it could be useful for, so the user has to be cognizant of that fact."		"I get a feeling that users are not (aware of use of health information to assist doctors) as a general, so I think there may be a better push to make people aware of that. "	-Infrequent user -Use: aid in describing symptoms but not self-diagnosis -Need to educate individuals to use health information purely to assist health professionals
38	"I have googled a few things. I mean I had PCOD two years back. I was really afraid to approach doctor at the initial stage so I thought I'll just go through what is it and I tried natural remedies. So it didn't work but when I read on the internet and spoke with friends who had the similar problem, they told me that it's not so huge. So I approached the doctor. But I have used the internet and it helps us a lot."	"I just search it. I mean general things we know Vitamin A is good for eyes right, so I mean I just type in vegetarian food with high content of Vitamin A. So I just go and Google it and if there is any particular website which is giving all the information then I go to it."	-	-Experience of use due to health condition -Used prior to seeking professional help -Positive experience -Views internet as useful information source -Searches on Google

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
39	"Yes. I used to work at a hospital too so I'm pretty familiar with health terms and with the HIPAA laws and stuff like that."	-	"I don't think there are any risks as far as people being to trace it back to you, no but you have to take everything with a grain of salt for sure."	-Experienced -No risk to identity -Need to exercise care when interpreting information
40	"No not necessarily, well...I would I have googled that stuff but I don't really rely on it I may use it more so like for health information related to a client or a diagnosis they have or most often a medication they are taking that kind of stuff but not really for myself."	Google	-	-Use for professional for information on clients -Used personally but does not rely on information
41	-	-	-	-
42	"Oh yeah. I'm notorious, my sister told me one time that when I become a mom you're going to be terrible to live with because you're going to think everything is something terrible, so ye I'm bad at that."	"My default is WebMD or the Mayo Clinic generally if I know it's on there, I'm like it's probably okay but sometimes I'll even look at like health blogs."	"(with health blogs), you need to be a little more careful cause it's just people posting and you don't know if it's verified but it can be useful for homeopathic stuff."	-High frequency -Comfortable with information on credible sites -Exercises care with health blogs but useful for homeopathic information
43	"Not for myself as much because I don't feel ill that much. I did it a lot when my children were smaller like is this something I have to take them to the doctor for. Even, my husband had a black tongue and I did look it up on WebMD, sometimes pepto bismol will turn your tongue black so that was like a funny health story."	"I think the one that's been around longest has been WebMD so I kind of just go straight to that um my paediatrician also has a site that they link to so sometimes I do that."	-	-Experienced for family -Use: minor issues -WebMD and practitioner website
44	"I try not to, but once I, have like something that's going on for 3 or 4 days that's not		"I have heard of the WebMD symptom where the more you	-Experienced but infrequent user

<b>Interview Participant</b>	<b>Experience</b>	<b>Process</b>	<b>Views on risks and credibility</b>	<b>Extracted Meaning</b>
	because of stress, I then write it down and try to figure out what it is. If I have itchy scalp I might look into it, if it persists. Not if I feel nauseated and I might have the symptoms, on most medical websites there's a list of symptoms that are very common. I don't really like to go and look those things up. “		read, the more you think you have that symptom, so I try not to.”	-Use: minor uncommon issues -Tries to not use internet -Does not use for common symptoms -Risk of misdiagnosis due to information online
45	“Not, not really. I'm very weird about medical stuff in the first place. I don't trust everything I see online but I also don't trust everything I hear from a doctor so I just kind of wait it out which probably is not a good idea. I think once I was having pain in my head and I tried to get as specific as possible and then I figured I haven't seen the dentist and there might have been a toothache. I maybe would look and see if I should be alarmed, that's as far as I've gone.”	-	“It goes from take a Tylenol you're fine to you need to see the doctor because you could be dying. It goes from too many extremes, if you're a person looking for a certain diagnosis because you have it in your head when you see that diagnosis you will freak out. So it can be more hurtful than helpful.	-Does not like to use internet as a source of health information -Previous experience limited use for peace of mind -Information can be very extreme -Can cause harm and lead to false self-diagnosis
46	“Yeah. I usually use the internet because I think to make an appointment with the doctor is very difficult because I need to wait a long time so for little illnesses I always just search on Google to find out how to solve them or what happened in my body.”	Google	-	-Frequent user -Minor illnesses -First port of call over doctor -Uses to self-diagnose and treat
47	“Once or twice a year if I have rash or something I'll probably google it but I would very rarely do it. I do Google health	-Google -Yahoo	“It's not that reliable. It depends on the source the CDC or a government website	-Frequently uses for education and fitness



<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
	things for classes. A lot of times if I see a link or something, on Yahoo or on a news website ill click on it and it might take you to another website so I'll read about different nutritional things or exercise routines."		probably carries a little more weight for me than just a random one. So, normally I'm kind of wary about what I read and the person's credentials."	-Rarely uses for personal health -Search engine -Views official websites as more credible -Looks for credentials
48	"If I am googling symptoms its usually for school like honestly I'm taking the MCat (med school entrance exam), I also took an Emergency Responder (EMT) course, but it's not really for me it's more for learning."	-Google -WebMD -Mayo Clinic	"I would probably trust WebMD more that comes up quite a lot and I would trust the Mayo Clinic, those two are the ones I would trust more and I usually I don't think this is the definitive source of information, it's usually confirming or if I want to get a jist of what it is."	-Uses regularly for education -WebMD and Mayo Clinic -Use: for an overview but not as definite information source
49	"If anything comes up I do Google it but I wouldn't say that's often because my health is fairly in good shape and I never really have any health concerns."	"I usually search and see what I find and I am a critical reader so I would assess the source I find on the Google search. The Mayo Clinic is the most reputable from what I've heard."	"I know that WebMD can be problematic from what I hear especially problematic when people self-diagnose."	-Searches irregularly due to good health -Search engine and assesses source -Aware of risks of self-diagnosis
50	"I get training articles, nutrition articles, research articles again for my own benefit. I've done the WebMD or just Google search hey what is this, or should I worry about this for various health reasons,	"I will go to WebMD but a lot of the times, I'll go into Google scholar and look for research articles. It depends what I'm looking for, if it's public	"I'll tend to trust the Mayo Clinic or WebMD kind of more straight up but if it's Jill's Health blog, then not so much, then I tend to double check the	-Frequent use for work -Uses research articles and health websites -Use for personal less frequently

<b>Interview Participant</b>	<b><i>Experience</i></b>	<b><i>Process</i></b>	<b><i>Views on risks and credibility</i></b>	<b>Extracted Meaning</b>
	allergies, injuries, whatever the case may be.”	health orientated I do more board searches into the topic as opposed to going straight to a journal or website”	answers or actually go into the literature.”	-Trusts health websites but often confirms information by reading research

## APPENDIX N: INTERVIEW ANALYSIS: TRUST

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
1	<p>“The doctor I trust because he knows me, hospital I am a bit dubious because an awful lot of people have access to the information. The only thing that would bother me would be if someone that knew me is, that if they didn’t understand what I had, even if they were a clerk and they saw that I had scoliosis but they didn’t know what scoliosis was, and they didn’t bother to look it up, and they’d be saying do you know she has scoliosis, that’s a danger but the chances of that happening are again slim. But if something did that you wouldn’t know that’s bad, but if they were on a system trying to access it they could be caught.”</p>	<p>“I’d trust a technology company because I’m a total stranger to them. The technology company, they’re normally very big and the chances of someone coming across it are less.”</p>	<ul style="list-style-type: none"> <li>-High trust in doctor due to relationship</li> <li>-Less in hospital due to information access</li> <li>-Could be accessed by unqualified people</li> <li>-Trust technology company as a stranger</li> <li>-Views risks as people viewing and interpreting data but nothing beyond</li> </ul>
2	<p>“I had an accident, my leg off swelled up but the doctor wouldn’t be available until Monday so I went to the D-doc and she said it can take 3-4 weeks for that to go so eventually it sorted itself out, being a diabetic you have to be very cautious, and when I came back to my own doctor he knew everything that was going on because the D-docs had made a report, that was extremely beneficial.”</p>	<p>“I assume they would use it, a company like Google you can almost always assume that they’re not giving you anything for free.”</p>	<ul style="list-style-type: none"> <li>-Positive experience of information sharing for benefit</li> <li>-Assumes technology company will use data</li> </ul>
3	<p>“I definitely trust the doctor, if you don’t like your doctor find another one. There are so many out there and you need to have some rapport, because you have to give them a lot of information so they can treat you.”</p>	<p>“Some apps the information is just going between your wrist and your phone and stored locally, that’s fine. For FitBit you can have an account and store information on their site but you don’t have to send any sensitive information it would be how much you walked and I don’t mind them having my height and</p>	<ul style="list-style-type: none"> <li>-Need to trust doctors due to information disclosed</li> <li>-Change dr. if no trust</li> <li>-Is okay with data stored locally or sharing ‘non’ sensitive data</li> <li>-No trust in unknown/cheap</li> </ul>

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
		weight. I wouldn't trust cheap devices or unknown apps."	technologies
4	"The level of trust in should be very high. From working in a pharmacy, I know the pharmacist might not always keep information to himself, often it is in the interest of the customer. There is a good level of trust but it's not always well placed, it makes me think before sharing with pharmacists but I think the level of trust with doctors is really high, well it should be. Older people have built up higher trust with their doctor. I go to different doctors so I don't have a relationship with one doctor but I trust them when I tell them my symptoms."	"The trust is much lower; I don't think there is any level of trust. The internet and applications are anonymous where as you know the doctor. Online you could get a thousand different answers and who says what one is right. I wouldn't trust any of the information online about health really it's something that's too important to take a chance on whereas there's an ability to go back to doctors. I would feel more comfortable talking to a doctor face to face."	-Trust is important in health -Tech is anonymous and information may be incorrect -Can return to doctor, have Relationship and physical interaction -Older people have more relationship but she trusts doctor with symptoms
5	"I have good experience with doctors so I have high trust that they have the information to help and they're qualified and knowledgeable so they can help, that's based on the experience I've had being treated. I trust my doctor wouldn't misuse my data or tell other people but I've not had any illnesses I've ashamed of. Overall I'd be very trustworthy going in to a doctor."	"With technology I'm always sceptical. There's something about making money or an angle. With my Fitness pal I did enter my data and they could be giving it to marketers, I'd have a lot less trust in that because there's no face to it."	-High trust in doctors' competence and integrity: good experience to date -Less trust in technology due to commercial element -No face – could have sold her fitness information
6	"Default wise I have a good level of trust in a doctor, I trust their ability to treat me, they would have to do something blatantly wrong to make me question them. I go to a healthcare professional with trust because they're qualified and they've chosen that line of work I trust their intentions with my information and care. I don't think they would enter that line of work without care for people. They've taken that job and part of that is confidentiality so I assume they are that kind of person."	"For technologies and apps it depends on the developer or if it is well known and has a good reputation for security, then I would trust them more. I would still rather have a person than an app though."	-High default trust in ability and integrity- professional -Assume they care -Tech: if well-known and good reputation – higher trust -Prefers person than technology

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
7	“If I go to my GP, I know him I know he’s trained in treating me and in dealing with my information sensitively, well I trust that he is.”	“I’d personally be wary going to the internet because you can’t control where your information goes and although leaks do happen in the hospital setting, there would be more controls in place. If I’m on an online forum and Joe says he has 20 years’ experience as an MD, I wouldn’t want Joe knowing my information, I don’t know him, I don’t know if he’s qualified or if his intentions are trustworthy. I trust my doctor infinitely more; I wouldn’t share anything on the internet.”	-Trust doctor competence and integrity -Can’t control where information travels online -Can’t confirm qualification online or benevolence -Trusts his doctor more -Wouldn’t disclose health online
8	“I think you need to have some level of trust in your GP but sometimes the GP doesn’t listen to all symptoms they’ve diagnosed. In pregnancy you might be worried and phone a midwife, they could be rude and you can lose trust in midwives and the next time you have a worrying symptom you might hide it and that can be very dangerous, trust is so important in health.”	“With apps it’s definitely lower like people will give you strange diagnoses. I had an app with a forum and people would say that’s a serious symptom, I wouldn’t trust the validity of the information, it can cause terror. I still would go on the app and see how my baby is developing but I wouldn’t trust their answers.”	-Importance of trust in health -Bad experience can reduce trust and lead to withholding data -Less trust in internet and information validity
9	“I’d say a lot of them would abide by confidentiality but there’s some rogue doctors who will just say oh I had this guy they obviously don’t name them but they’ll still talk about the person. In the majority of cases doctors are trustworthy. Luckily I haven’t had to go much but when I was down the country and I had to come up to Dublin and they didn’t share the information that annoyed me but other than that, not a problem with doctors.”	“That’s different, I trust them so far as they’re only getting my basic information but health is different, I suppose if they got hacked and it was out there to the world like someone could google all my records, I’d be shocked. I’m all for better technology but it’s not always the cure”	-Trust in integrity of most -Little experience: good health – annoyed by not sharing his data -Technology trusts as only basic data disclosed (IBT) -Fear of hacking - technology not the answer
10	“I don’t think our health system is too good, the availability of beds is ridiculous my mam had a seizure before and she was waiting 7 hours in casualty to be seen. But I would definitely trust doctors’ ability to treat and	“I wouldn’t say they have great intentions for my information, it wouldn’t be private, it would be shared quite easily, and I wouldn’t be happy with that.”	-Mistrust in health system -Trusts health professionals’ competence - understands

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	diagnose me. With my information it's not something I really considered before but I wouldn't trust because I understand they need it for research but at the same time I want to keep some private information to myself."		need for research but desire for privacy -Doesn't trust intentions of technology vendors – fear of data sharing
11	"I trust the health professional more every time. Because they're specifically trained and you like to think that they still broadly observe the Hippocratic Oath which demands that they focus their knowledge and their expertise on the patient they are treating and not their own benefit and not anybody else at a given time."	-	-Health professionals are trained -Hope they observe Oath of benevolence -Benefit patients
12	"None. It's my experience for the last 6 years, traipsing around from one to another and I ended up at a neurologist. I brought the most recent MRIs and he looks and he says there's nothing wrong with your back, so he said I'll give you this to read, and I said what are you treating me for, and he said stiff persons' syndrome, and when I read the article it says one in a million get it. So I was at the chiropodist and I said I've got stiff persons' syndrome and he said 'do your muscles twitch?' I said 'no' and he said 'you "haven't got stiff persons' syndrome'	"At this stage, I would probably trust a technology company more with my information, well I reckon the information I get there would be equally as good, I know what sites I use. But I would be worried that a technology company could use it lot more, I would hope that there's ethics within the medical profession."	-Low trust in health competence due to experience with diagnosis -Trusts information online due to reputable site -Does not trust technology re secondary use – hopes health professionals wouldn't use data
13	"The people I work with would keep confidentiality, we don't get into the lift and talk, it's in your training and out of respect you wouldn't do it doctors would be very discrete. Our area where I work isn't confidential because two people are getting tested at the same time, but even when I verify their date of birth I don't shout it out.	"I would hope they would put some statement or ethos because I don't think it's fair if everybody's' information is out there, okay you have to learn and if they were doing research and they asked for consent I don't have a problem with that if you ask the person first, and ask do you understand, that's respecting the person."	-Trust in integrity due to work experience -Trained to be discrete -Technology hope for ethos -Expects consent before using data - respect

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
14	“I would have high trust in my GP yes. My cardiologist yes. Some health professionals no. There’s an enormous amount of pressure. Should have a disposition to care for people, and that isn’t always the case and there are some health professionals that are not very caring, most of the ones that I’ve come across are okay.”	“No, they’re commercial companies, yes they’re commercial. Like Google know more about me than my wife does, because I use them as my search engine so they all know, that’s in a bank somewhere sitting and they can tap into me.”	-Trusts his dr. due to good relationship -Some don’t have disposition to care -Doesn’t trust technology companies -commercial
15	“My doctor is a very friendly man, I would very rarely go to the doctor, I have macular eye degeneration and you take a multi-vitamin and that’s all I’m on, that’s pretty good for my age, I’m 76. Generally, I would until they prove me wrong you know. But you don’t know where that information is going, is it going to drug companies?”	“I wouldn’t. To me, big companies, no principles, no nationality, there’s no faithfulness, they’re just there to make money, and that is the bottom line. And I would be short on trust as to what they would do with that information. I wouldn’t give it to them.”	-Trusts his doctor but rarely sick - No choice but to trust but suspects data is shared due to media coverage Doesn’t trust tech – wouldn’t disclose
16	“I would trust them but I would question them more than my mother’s generation because they were like gods, but they are human they make mistakes, I would trust them but I’d question them more, and I if I had an ailment, I’d want all the information. Unless I was asked for permission I would be very disappointed if it wasn’t kept private. I’ve never been in the position to question the doctor because I have a good relationship with her but that file should be between the doctor and the patient.”	-I wouldn’t trust them. With the click of a button they could put that worldwide.	-High general trust but would question and desire for information HLOC -Health data should remain private – expects permission if not Good relationship with her doctor -No trust in tech – fear information could spread
17	“I totally trust my doctor, she’s brilliant. I was going to another doctor, that doctor was brilliant but as I got older, he made insensitive comments. So I made an appointment to see this other doctor. When I went into Beaumont I couldn’t have got better treatment so I do trust my doctors. I know people who are going from billy to jack and getting nowhere, but I’m very lucky. I have to trust them, but it’s there in their records, so I can’t say	“I don’t trust them. Straight up. I wouldn’t give them my health information no.”	-High trust in doctor competence - relationship -Need to trust -Always risk to information -No trust in technology -Wouldn’t disclose health data

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	they can 100% protect my information, if somebody else comes in, I trust them personally, but I don't trust their office."		
18	<p>"I think myself need a knowledge of what your tablets look my husband often got the wrong tablets, they can make mistakes, you should know what you're looking for so you know if you got the right thing or not you know.</p> <p>Doctors they're only human too. It's important to have faith in your doctor because there's no point in going to somebody about your health if you don't think they're good. The doctor I go to find him extremely good, he follows up on everything. I'd say my doctor keeps my information safe and private."</p>	"What would they do with it, unless you had something brilliant or very unusual, I don't think anyone would be interested in Googling my health information but I don't think I would be inclined to give Google or any of them my information. I don't give them any information. Then again I'm not actually sick, so I don't have anything to give them"	<p>-Need to be aware – HLOC</p> <p>-Trust in doctor is very important -for health</p> <p>-Trusts her doctor's competence and integrity</p> <p>-Wouldn't disclose to technology but doesn't see risk as no unusual illness = doesn't understand all health data that exists</p>
19	"90% I trust them, then I don't have a lot of issues. My GP is good. We always had our own GP now they're part of a group where you might see different ones. I think most times its confidential. And of course it's on computers synced up and you don't know where that goes but you have to trust them. I did have an operation a couple of years ago and I did pick the same doctor I had an operation with 14 years earlier because I trusted him because the last time I had good results and this time I had good results. If you know someone, or if you know someone who knows them, it does help."	"I think in this age we have to, we've no choice because it's all going with somebody, it's all in the cloud, we don't have a choice, we can't stand still. I would only give them information if I was benefitting. I wouldn't just give it to them for no reason."	<p>-90% trust but healthy-</p> <p>-Good experience – chooses based on expr and recommendations</p> <p>-Need to trust doctors</p> <p>-Need to trust technology – no choice – data is going to these companies</p> <p>-Wouldn't disclose without benefit</p>
20	"Higher than in many other areas. I trust their motivations is to treat you. I think they can be dismissive at times which is unprofessional as part of their service is to comfort. I think nurses are great with comforting patients. I think some doctors have ego issues and	"I wouldn't. I understand commercial goals and those principles underlie technology companies. Their purpose is to make money. If they branch into health technologies, there is a strategy behind that and a strong financial revenue model.	<p>-Trust doctor's competence but need to improve comfort</p> <p>-People often afraid to question dr. need to</p>



Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	patients often feed that with their fear of upsetting the doctor or asking too much but when it comes to your health you need to probe and you need to know your doctor is competent. I'd rather probe at the start before something goes wrong. But overall I trust their competence."	It's not a strategy I'm interested in helping them realise though. I understand the motivations but when it comes to health you have to remember the human this data relates to. It's more than a means of using this information to make money."	question to ensure competence -Doesn't trust technology-commercial motivations -Health data is too personal Not for profit
21	"The ones I've come across are grand, I generally trust those. Any of them that I've come across are people that I've had a relationship with for 10, 20 years, so I would know them quite well and it would be, based first of all on the fact that they are a health professional and but also based on the fact that they've a proven track record for a chunk of time. I've never had any negative health experiences from health information going astray."	"I don't trust them at all. I don't see why they should be acting in my best interests, surely they should be acting in their shareholders' best interests. I wouldn't trust them with my health data and wouldn't give them it if I could manage it at all."	-High trust in health prof due to long relationships & no negative experience -Trust as professional and due to track record -No trust in technology- not in his interests -Wouldn't disclose health data to them
22	"I have a high level of trust. The only thing I'd be worried about is workloads. I saw that a lot in the hospital. Same with nurses. I think they are competent in treating you, maybe they're a bit stretched at times. Mistakes do get made but there are systems in place to help. People do talk, even nurses and doctors on the ward I think it's innocent enough but if you think about it, it could be a breach of their confidentiality. I do trust the doctors and the nurses to you know keep things private, they talk among themselves which is fine but I think they would have their boundaries and they would respect it."	"I don't know if I'd trust, you're always worried is this going to be sold or am I going to get targeted ads now or is my employer going to find out my past medical history. I'd have nothing to hide but if there was something sensitive there you could be embarrassed if your employer has access, if it did become so open, it could be used for the wrong reasons. I don't know if I trust Google and these large corporations they're going to be benefiting from it in some way."	-High trust but worry of overstretched -personal exp. -Trust in integrity- would respect personal boundaries -Fear secondary use and access and how they would use that access -Technology companies would benefit somehow
23	"I have strong trust generally, across the board, I've no reason not to, I've never had a bad experience and for my family the same, we'd be trusting of the profession. There's a history there, there's somebody who can say I see last year you had this, so that's a trust you genuinely	"Not quite as trustworthy, because I'm not as familiar with it and that would be me having to learn really how to trust and to share because I haven't done it before, but technology	-Strong trust in health prof due to good experience -Rapport and caring relationship

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	feel that somebody cares even though they might be reading it but it is a caring, engaging relationship.”	companies in as far as I use them and as far as I know I would trust them.”	-Trusts technology but needs to learn more
24	“Broadly high, medical professionals are fairly ethical and in my experience, I’ve a lot of friends in the medical profession and I’ve never had information be revealed to me that would allow me to identify somebody, they’ve told me about cases. I’m not sure that the administrative support is there, I’m not sure that they are sufficiently trained in data handling, so I think that it is probably easy for them to make mistakes. I trust them, but I don’t think they’re beyond fault. So I trust their intentions.”	“I’m less trusting of those entities, mostly, because medicine doesn’t operate for profit whereas these corporations do. That doesn’t necessarily mean they have bad intentions but I think profit comes before treatment. I don’t necessarily look over my shoulder particularly, and if all that happens is I get a pop-up ad the odd time I don’t really mind. I would worry more about the security of my data at an intentional level with a corporation than with a doctor although in practical terms, the risk is probably the same.”	-Broad trust in integrity due to personal relationships & experience -Risk of errors due to poor training and support -Less trust in technology due to commercial motive -If outcome is minor (ad) it’s okay -Trusts doctor’s intentions with data more
25	“I would generally trust their competence and I would trust health professionals with my information. Because I’m paying the health professional for a health service. and I’m dealing with them directly, I’m paying them directly, I know exactly what I’m giving them and they know exactly what it’s for. I suppose a health company could start reselling your information but that would seriously undermine their ability to business in the future so it’s really in their interest. But a faceless technology company that barrier doesn’t exist.”	“The technology company wants my information to monetise it, nobody is doing anything for free and if they’re monetising it they only way they can do that is by selling it or by selling a service that attaches to it.”	-Trust health prof. competence & integrity -Pay for health service -Aware of data disclosed and purpose -Aware of potential for health orgs to sell data but Not in their interest -Tech companies want data to monetize
26	“It depends on the level of the person you’re seeing. I think if I went to get a shot at a drug store I wouldn’t necessarily trust that person a lot. But for your primary care physician you should do a lot of work in vetting that person. When I moved here, I did a search through work and was recommended some people. And the person I	“Anytime you get a business involved, I think ethical practices can go out the window and the focus is on making money. More often than not you can see problems with that. I think you’re responsible for doing your own research on anyone you give your information to especially	-Depends on rank of prof. -Importance of trusting GP -Research and comfort and building trust -Only seek information they need -trusts in their integrity

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	went for I had a meeting with him before I fully decided. Trust is something you build with them, it's really important to have it and it starts by good research and selecting someone you're comfortable with. I trust that doctors have my best interest at heart. I mean if they ask me for some information I know it's because they need it. I come from a professional background where I'm trusted with peoples' personal and financial data so I have an understanding that doctors only request information they need and that they're trained to protect it."	health information. I would be comfortable giving some information. It shouldn't be a blanket assumption that they should have access to all my health information. If I could control what I give them I'd feel a whole lot more comfortable. FitBit get the number of steps I take every day, my weight. They don't really have anything, also have an email address but other than that they don't really have a lot."	-HLOC to do research on dr. -Tech: focus on making money -Okay disclosing certain information – IBT -Desire to control disclosure increase his comfort -Hasn't disclosed much 'health' data
27	"I trust healthcare professionals absolutely. There are laws in place and they only ask for my information to help me and to treat me so I don't think they'd use it for any other purposes."	"I don't overly trust. Fitness is important to me I don't mind giving it return for what I get. I don't give anything sensitive just fitness information, as I'm healthy I'm not concerned about how it could be used but if serious information did exist I would be concerned."	-Complete trust – health -Only use data for treatment -Trust technology less -Discloses non sensitive information for benefit -If wasn't healthy would be more concerned
28	"I wouldn't necessarily trust them right off but sometimes you're not given any option with health insurance. So people take what they can get and if they have the worry of the privacy or how it is protected then goes on the back end, people care more about getting treatment first. Trust isn't something you always have the luxury of building with limited options, the same with privacy concerns are not the first concern, our health is so important."	"No. I wouldn't trust them at all because health is a big industry with data mining and selling information to other companies for marketing purposes I wouldn't trust them at all with my health information."	-Trust isn't automatic -Often don't have luxury of building trust -Treatment first and privacy after – health is important -No trust in technology health is a big business -Selling data for marketing
29	"I've been to several types of health professionals, dermatologists and they were very professional knew exactly what they were doing and I don't believe that	"With electronic services in general my trust would be much lower. It depends on the service they're offering. Stuff like the fitness trackers	-Positive experience with health prof-competence

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	they would share my information because they seem so authentic. With my hand surgery they were very open with what they were doing with my information and they tried to find an answer by discussing it with other surgeons. I don't go to general healthcare professionals as often as I should but I suppose ASU health services is an example I trust them not to share my information because they have a lot at stake me being a student. I haven't had much experience with health professionals who aren't as knowledgeable as I feel they should be so I haven't really had an issue with their authenticity and I've had no detrimental effects from sharing my information."	the entire concept hangs on your health information if you're not honest or completely truthful with everything it won't give you the service that you're looking for so there's almost no point not sharing information if you are wanting that service. I trust them less because they don't have everything riding on this confidentiality because Microsoft or Apple have tonnes of other things, they have less to <b>lose, if they</b> were caught sharing information. I suppose I would still trust them because of their overall integrity."	-Trusts integrity-open with previous sharing -No negative effects from sharing data so high trust -Trusts technology less as less to lose -But need to disclose accurate information to use health technologies -Trusts large technology companies due to overall integrity
30	"I completely trust I don't have any reason not to trust them. I'm going there for them to help me and I expect for them to have an answer. I really never get sick so I've only been sick a couple of times and I've gotten over it quickly because of the medication they've given me. I've broken my arm once and the doctor that I dealt with was like really nice and helpful and they performed surgery and it went well so the doctors I've had experience with have known what they're doing. I trust them to protect my information because I don't really know what else they would do with my health information."	"I wouldn't trust them as much as my doctor because you're putting information on to your phone and I feel like they can do whatever they want with it since you're putting it into their system they can use it however they want to but, the information that I currently put into it I mean it would just be my name, my age, my height, my weight and then it reports how many steps I take how many calories I burn so I don't feel like there would be an issue with privacy with anything I put on there."	-Complete trust in health prof. competence due to positive but limited experience -Trust in integrity as no reason to use his health data -Less trust in technology due to many possible uses -Doesn't disclose sensitive data so doesn't see privacy risk
31	"The doctor knows the rules better but a tech company is going to have more safeguards. I mean my chiropractor knows HIPAA inside and out but he locks his doors at the end of the night, his wife has keys, the guy who cleans it has keys. I mean anyone who wants to can get in there. They may know HIPAA but they're not going to know technology and how to lock it down"	"A company is going to have more safeguards that your doctor does. A tech company they might not know HIPAA but I think if they're working on a medical thing they're going to know what they need to know. They would know technology better and how to lock it down better."	-Health professional know HIPAA but not technology -Technology company know security better

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
32	"I'd prefer the health professional to know the data but who should be securing the data I don't think a health professional can do a proper job of that."	"Tech companies if they have the right requirements could probably do a good job of doing it. It's almost like I want a health professional that's an I.T. person, an I.T. person that's a health professional who has the same <b>do no harm</b> professional attitude about the data."	<ul style="list-style-type: none"> <li>-Trusts health integrity but not securing data</li> <li>-Wants technology with 'do no harm' ethos</li> <li>-Tech could do well with right requirements</li> </ul>
33	"I'm sad to admit I have very little trust in the U.S. style of medical care. From my experience, I have food allergies, with a lot of sinus congestion and coughing as a symptom. The doctors, regardless of specialty, make you wait long periods of time, give you a maximum of 10 minutes, toss you a prescription and send you on your way. There is very little training in nutrition and many doctors seem to be dismissive / condescending if you ask too many questions. That's one example but having that experience over the years really reduces your trust in them. You hope for the best, and I do often ask who has access to the information, but most front office staff don't really take you seriously when you express concern."	"I expect my information will be shared, and try to limit the ways I share it. Information is money and it is used to advance the corporate side of health data, not the patient. That's partly why I wouldn't use any of those apps offered by random tech companies."	<ul style="list-style-type: none"> <li>-Little trust in competence and benevolence due to experience</li> <li>-Hopes data is safe – has asked about access but didn't get comfort</li> <li>-Expects technology companies to share information -commercial</li> <li>-Doesn't use health applications</li> </ul>
34	"I know a lot of people that work in healthcare so that influences my opinion and I the people that I know are very educated and compassionate people, so I have a high level of trust because for they are very highly educated and that influences their knowledge of ethics and morality and of course there are unethical people certain people have definitely been taken advantage. I've never experienced that and I've never known anybody to experience that and who you choose to receive healthcare from is a very intimate and personal thing. I have always gone through word of mouth and I pay	"I would trust them less because I don't have a personal relationship with that company. They're in the data business not the curing people, helping people business."	<ul style="list-style-type: none"> <li>-Friends in healthcare influences opinion</li> <li>-Educated, compassionate with high ethics</li> <li>-No bad experiences</li> <li>-Healthcare is intimate, if doesn't feel comfortable will not return</li> <li>-Less trust in technology as no relationship and their business is data not health</li> </ul>

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	attention to my gut and do I feel comfortable, do they seem compassionate, and if they don't I would not come back."		
35	"As far as healthcare professionals, I trust them implicitly. They make mistakes; you have to be part of your own healthcare. I go over the physical to make sure everything's checked and quite a few times I've found the wrong information. They're not used to those forms. But as far as the professionals, I've no problem with their integrity, it's when you start getting involved with all corporations that own doctors' offices and the hospitals and the drug companies and pharmacies, it's not the doctors I'm worried about, it's the corporations, I have no trust in them. Information sharing, its money for them."		-Trust health professionals' competence & integrity -Need to do your part to check – HLOC -No trust in health corporations – commercial gain from data sharing
36	"I trust health professionals but have had some that I don't feel put their patients best interest at heart but for the most part, health professionals have chosen this path because they want to help and to heal people but there will always be some not upholding the high standard we expect from health professionals. I believe they do their best to protect my information. I hope they have some good security in place but they do their best. When it comes to really large health providers, my trust would wane a little. With all large corporations, it seems they'll do whatever they need to make money."	"I'm unsure about whether I trust them. I'm not too informed in reasons why I should or should not trust them. I don't think I give them all of information far fitness related but I don't see what harm that could have for me."	-Generally high trust in benevolence but some don't upload high standards -Do best for information hopes security in place -Less trust in big corporations – commercial -Unsure of trust in technology wouldn't disclose all data -Discloses fitness data as no possible negative outcome
37	"I was trying to get a doctor I had to wait almost an entire year just to see someone and luckily I'm healthy It' a double edged sword my data is protected so far but if I'm	"No. I don't because it's worth a lot of money. I would not trust them with any kind of data. I don't feel like they have my best interests at heart	-Trusts VA integrity but professionals may be overworked – dangerous

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	not healthy I can't get the healthcare. It feels like they don't care either their attitude or because they're so overwhelmed. I think it's a combination of both, that can be dangerous especially with healthcare."	and so they'd have to show me, they'd have to prove it to me that they would keep my data safe. Until then, no I wouldn't give it to them.	-Doesn't trust technology as data is valuable -Need to prove data will be safe – won't disclose
38	"The only person where we wouldn't lie is with doctor because we really want whatever we are facing to be cured. I expect them to keep our information confidential. There wouldn't be any point in lying or withholding information, it's better to tell and trust them completely."	"Maybe a few years down the line, technology would be the ones ruling. Now, we can trust them but maybe not completely, it will take time for technology to become common to everyone so we can trust them but now not completely."	-Need to trust them and disclose all information -Can trust but not completely maybe in future
39	"I probably trust my doctor more than technology."		-Higher trust in health prof.
40	"I definitely trust my doctor and you know the nurse practitioner I see."	"I would be sceptical of technology companies because they want to sell me something."	-Trusts her health prof. but wary of tech: commercial
41	"I hold them to a high standard. I really hope they're keeping all of that confidential and doing their best to make sure that information never gets leaked, that it's stored away and only if I'm in the hospital and they need to know if I'm allergic to something then they can pull my record but if not then it shouldn't be being used."	"Probably not. It's not official. I'm not consenting for them to have all my information just the information I've provided because I've accepted their app but I wouldn't be giving them any detailed official health records I wouldn't trust them with that information."	-Hopes they keep confidentiality -Expects no secondary use -Tech- consents to data she discloses would not disclose official health records
42	"I tend to go to places friends or family members have gone to, because they have good experiences. I know doctors can be negligent I've experienced that, it's not fun so you have to be really careful and know your own rights so you can be sure. I trust them as long as I can sort verify them a bit. I had a broken wrist and the doctor said you don't need any painkillers and fused it back into place. I probably shouldn't have listened. We had to re-break it because he did it wrong. I lean toward trust but also I'm wary. Regarding medical records	"Applications like FitBit or Apple or Microsoft with limited stuff like how much I weigh or my fitness plans, that's fine. I wouldn't put all my medical information on there but I would like to, that would be really interesting. I would need security, tell me how it's stored is the server locked down, can anyone access the server. I'd like confirmation from them that they're doing everything they can, because like FitBit I don't know where they're storing stuff. If the app was tied to a big health branch like	-Chooses healthcare prof based on recommendations -Had negative exp. – need to be aware of rights and question dr. – HLOC -Trust in information security in health -Technology trusts with non-sensitive

Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	though I feel like the systems are pretty good even if they're just files the rooms are locked."	Mayo I would be more inclined to give them stuff."	-Unsure for sensitive data but sees the benefit – would disclose if had reputation
43	"Why would a health professional screw up unless they feel like they're going to get money for dumping information. Being overworked somebody could make an error but there should be things in place to catch it. In terms of treatment? Yeah that's what they're there for but when you put so much data responsibility on somebody who's trying to help the sick I don't know how you reconcile that."	"No. They would have a motivation to release your data and it gets lost now I can sell the next security thing. It's the same with Microsoft and McAfee and all those guys, they do have a business model reason, they'd have to prove to me they didn't have a completely business model reason to screw with peoples' information. I don't know trust those guys."	-Healthcare no motivation to sell information – tech has business reason to sell -Health professionals may make errors – not technical people -Trust their competence
44	"They think it's protected but it's in a file cabinet which is not really safe, it is not impossible or it's not tough to break in to, how tough is it to break into and get information. So is it really safe or if there's a fire and papers go flying off, that's where the security is. If you go into a hospital, everyone from the nurse up can see that private information which may not be necessary."	"Yes. As long as they're built in correctly with the right amount of knowledge. I don't think Healthvault has anything for emergency responders. So if I have a heart attack, I cannot necessarily give emergency responders' access, they should be able to send a request and it should be approved within minutes or automatically."	-Physical storage isn't safe but hospital IT can be too open -Trusts technology companies if have safeguards but need to enable access at times
45	"They know what they're talking about but some doctors heavily rely on the technology. I had to get my eyes checked and the majority of the time the doctor was filling out information on the computer, I felt I wasn't getting an actual doctor experience. I get they're notating everything but I don't know how much they're listening to me. So I've noticed when technology comes into play, my trust in what I get diagnosed as starts to waiver."	"I'm more trusting in the doctor than the app because these are like mini computers so whatever you put on there, potentially <i>could be</i> viewed and I don't know exactly what, like they have all those privacy things they tell you before you download, but I don't know everything that they say and I don't know how far they go	-Trusts doctor but reliance on technology reduces trust in competence and reduces interaction -Less trusting in apps as doesn't know how they use data or where it goes
46	"In the health centre at ASU, I am not always sure they can help me. I remember one time I told them that a bug bit me and they could not solve my problem. They did	"No I would trust them at all. Of course not. Online, I don't give any health information at all. I just describe what is happening or maybe	-Not fully trusting in health centre competence -Fear of sale of data



Interview Participant	Health Professional	Technology Vendors	Extract Meaning
	not know what it was. Sometimes I worry that they will sell my data to a database. That is scary to me.”	gender to get a better result, but I don’t give any name or history of my health. I do not do that.”	-No trust in data companies -Does not disclose personal health data online
47	“Well I trust them because my experience with doctors has been good and if it wasn’t I would do something about it. My local pharmacist would always call and let me know if something might have counter affects, so that was trust building knowing they were looking out for me and I am a person. If they’re not being nice I might not trust them or tell them as much. I sign something every time I go to the doctor saying my information is protected and if they don’t they get sued. I think and hope that they wouldn’t be revealing health information because that’s a small thing that you could get your license revoked for.”	“I wouldn’t put as much information. I don’t have an issue saying I am allergic to this and putting that in but with the doctor they know a lot about you, regardless if you want them to or not they do because if you’re being treated for a condition you have to disclose all of that. Whereas with Healthvault and that you only put in the information you want to. That’s why I probably wouldn’t feel as violated if the information on Healthvault was ever stolen or like you know I’m allergic to something what’s that going to do.”	-High trust due to experience – personal -Trust integrity as waiver -Hope’s they wouldn’t release data as they would lose license -Trust is important need to disclose -Healthvault disclose some information that wouldn’t impact if stolen
48	“I guess my personal experience with my doctors has been really good, they’re super nice like I’ve shadowed them, they’re my family doctors so for sure I trust them and then my aunt is a doctor so like I would trust her a lot I know that they’re human but my experiences have been really good so I trust them.”	“I would y trust them a lot less, technically, a doctor’s primary motive is to keep you healthy whereas with an app or something like that the primary motive is profit so that makes me more sceptical, so I would trust it less than a health professional.”	-High trust in health prof due to positive experience and good rapport -Dr motive is benevolent -Less trust in technology due to commercial motive
49	“I have a new a general practitioner and I certainly trust her competence a lot. She’s been rated one of the best professors and she was one of the best graduates and she has a lot of integrity. She’s young and very personable. I disclosed everything that there really is to, the biggest thing I suppose being that I’m gay. A lack of trust impedes a lot of medical cases where people are afraid to say things that are important especially involving STIs and that makes it more expensive for the healthcare	“I trust technology quite a bit, it does depend on the specific site and how the company is viewed and I how I deem its credibility and trustworthiness but for the most part, I trust technology and I think it has incredible potential to improve everyone’s health but I would definitely do my research before using something new to track my health and when I do get any results I wouldn’t just take it from that	-Trust his doctor competence and integrity -Need trust withholding information damages both -Trusting in tech but depends on his view of credibility -Research prior to using technology

<b>Interview Participant</b>	<b>Health Professional</b>	<b>Technology Vendors</b>	<b>Extract Meaning</b>
	providers and it increases the risk for the patient being even more severely injured.”	source. I would look at what other sources say and if I had any confusion I would go to my actual doctor.”	-Technology offers potential to improve health
50	“From the health professional side if they’re going to be using it for other purposes then I would want to know about it but as whole I’m not really concerned; I don’t have a lot of health information.”	“There isn’t much the technology company has about me and I don’t have much health information in general.”	-Not concerned as little health data exists -Desire to be information of secondary use

## APPENDIX O: INTERVIEW ANALYSIS: RISK

Interview Participant	Health Professionals vs. Technology Vendors	Extracted Meaning
1	-	-
2	-	-
3	-	-
4	<p>"I thought on the app the information would be anonymous. Maybe on the internet the risk is bigger because the information is associated with you. Maybe I'm being naïve but the apps I've used I don't reveal much information, if any. I think the internet is a bigger risk to hacks or maybe I haven't heard of stories about apps or aren't experienced enough. With doctors, there's always a level of risk, its smaller than in other contexts but there's always a risk they'll tell someone, or their computer could be robbed or lost or their secretary could look, there's always a risk but because there's a face to the doctor and your health is your wealth, you need to tell them all the information even if you're afraid or worried."</p>	<p>-Low risk of apps – little data disclosed, no stories of breaches, little experience</p> <p>-Some risk with doctors could reveal, lose data or access but need for treatment outweighs fear</p>
5	<p>"The loss is a different audience. In the healthcare setting, the audience is smaller, in the internet setting there's a much larger setting of who the information could go to. But on the internet you could be one of thousands and they might have your data but they don't care who you are they just want your profile, whereas in the hospital or GP your name is linked to it so there's different risks. It's more dangerous for the person in the local healthcare setting as their information might get back to them or a neighbour, but on the internet for the community, its more dangerous that our health information could be at risk because the amount of it. If thousands use an app or thousands of health files are hacked there's huge consequences."</p>	<p>-Different audience</p> <p>-Healthcare dangerous on the local level</p> <p>-Internet more dangerous for society</p> <p>-Internet larger scale of breaches</p>
6	<p>"There is risk. Anyone could try to hack a computer but you have to have a trust that there's security measures in place. But an app I wouldn't trust as much, I think someone could get your information easily. Maybe it's not different like your information from a doctor could be in a server somewhere and the same for the information you put in an app and anyone could try hack that server so there's always risk. With the doctor you already have built up the trust."</p>	<p>-Always risk</p> <p>-Need to trust security</p> <p>-Trust built up with doctor not technology but risk exists with both</p>
7	<p>"It's never going away, there's a tangible record of it in a computer or on a server. Health information is inherently linked to you, it represents your health, your physical or mental condition and that belongs</p>	<p>-Always a risk – permanent record – can't control</p> <p>-Perceived ownership</p>

Interview Participant	Health Professionals vs. Technology Vendors	Extracted Meaning
	to you, if it's in systems or servers or roaming the internet you can't control it, so there's always a risk. <sup>2</sup>	
8	"Having worked in a pharmacy, you have easy access to all the people in the community and can see what prescription they are getting. Having seen that I think it's risky in all settings that people might find out your health conditions. There's locums in pharmacies all the time, anyone could walk into the pharmacy and say they're you with the address and ask for your medications. In apps I didn't give all honest information but there's always a danger of your phone being robbed or your data being in the cloud and they might not know your name but they can use your collative data to build a picture so it's ever risk free."	-Ease of access to health data – always risk -Falsified data in health apps but always risks of data collation or theft
9	"A lot of the hospital systems are outdated legacy systems, so it could be risk with everyone if they're not on the same page, it could be either one's fault if they're not up to speed on the regulations. Doctors have to know this could be a risk and then the provider needs to be secure so. I think the onus should be on the doctors to know that everything is secure and not enter into an agreement where things could be hacked."	-Risk with health professionals and vendors -Doctors should ensure system is secure
10	-	-
11	-	-
12	"I would be worried that a technology company could use it, a lot more. I would hope that there's ethics within the medical profession that they wouldn't. But I think hackers can get in to either."	-Technology- higher risk of misuse -both at risk of hacking
13	"I think there is a risk they could lose my information. Although if the system is built correctly they probably wouldn't use it. I hope they wouldn't misuse it. If they had to share it, if they asked I don't have a problem but misuse, I wouldn't agree with that, I would hope they wouldn't misuse it."	-Higher risk of data loss than misuse -hope no misuse
14	-	-
15	"The risk is high with the technology company, because of profit margins, I'm very suspicious of big business."	-Higher risk with technology due to commercial aims
16	"The risk is higher on the apps. I think it would be safer in a hospital. A technology company is more of a target for hackers than a hospital."	-Technology risk for hackers -Perception of safety in health setting
17	"The risk is higher with companies like Google, definitely, I trust my doctor more."	-Higher risk with technology due to trust in health prof.

Interview Participant	Health Professionals vs. Technology Vendors	Extracted Meaning
18	“Your doctor wants your information to help you and if there’s anything wrong to treat it, but Google is only in it for if you have such a thing or if 100 people have a particular thing, then they go into things that can supposedly help this. Life is all about money right?”	-Risk with technology due to commercial aim – broad understanding of difference
19	“If you put it on the internet yourself because a lot of them have privacy things in the corner of the screen that it’s supposed to be private or when they put it on, but I don’t know if you’ve got that yourself when you put it on. I think they can go from your Facebook to my Facebook or other peoples’ Facebook and I do think, it’s open because people can read all about you, I don’t know whether you have to go on and only be with your friends. Are they free to everybody?”	-High trust when disclosing information online – unaware of whether data is secure online -fear information is open online
20	“With technology companies definitely. They have sophisticated methods to prevent against attackers but they always have vulnerabilities and within the organisations or the fact they are large companies makes them a target for hackers. The risk of them harnessing the information for their own benefit higher too.”	-Risk higher with technology companies, hackers, employees or undesirable uses
21	“Looking at my own GP surgery, it’s possible they could lose it because there’s only 3 doctors, so I’m not sure that anybody is clued into I.T. I don’t think they would misuse it, the great thing about a small doctor’s surgery is if anything happens everybody hears about it. So I’m lucky in that regard, you wouldn’t be in the city. I don’t think there’s much chance of them deliberately misusing it, incompetence is a possibility.”	-Low risk of doctor deliberately misusing data but risk of loss due to technical incompetence
22	“I think the risk is higher with companies like Google. The hospital uses it for the patient’s benefit. With something like that because they’re not offering you healthcare advice they don’t necessarily have to comply with legislation, things are already sold about you online, data you think means nothing but to companies it means big things. I think they would misuse it more, I can’t really see how the hospital would, I suppose if you had access to everything maybe the hospitals would say ‘no we don’t want you here, you were a bed hogger in St James’ but they can’t do that, I don’t think they would be as maleficent with their use, not that Google would be bad, I think they’d sell it, and you’d start getting pamphlets for mindfulness classes and people be like why do you need them, I think people would know everything about you then.”	-Higher risk with technology -Health use data for benefit wouldn’t use negatively -Technology companies would sell data -Danger of people knowing everything
23	“Technology companies are the greater risk. It goes back to trust and what you’ve built up with your healthcare professionals it doesn’t mean they wouldn’t have the same potential to do it, it’s probably due to the remoteness or the lack of connect with technology companies I feel that, I could be wrong.”	-Higher risks with technology as no relationship & remote -Could be wrong

Interview Participant	Health Professionals vs. Technology Vendors	Extracted Meaning
24	“If someone takes a look at your browsing history they’ll get a sense of what you’re wondering about, that can be relevant or not. It’s not as precise a danger as we think because I search for things I’m interested in as well as things that I’m concerned about, so you would not get a particularly clear image of my health from what I search but I think that there is a danger that searches could be relatively easily accessible and could be exploited by marketing, I that’s the risk we take with Google I think, and I think it’s something that we have begun to build into our consciousness, there are risks but I think they are relatively minor.”	-Risk for marketing but not all searches are relevant -Risk in using Google -Becoming more aware -Minor risks
25	-	-
26	“There’s risk everywhere. You have to trust people with the information you give them and that they have your best interests in mind. I think health professionals rank a little bit higher than other normal people. I think you can control what you’re giving up, what information you give to your own comfort level so that can help with the risk level. If they were to ask for my social security number that’s a red flag for me, I wouldn’t give it and I’d really think about who the company was that was requesting that information.”	-Risk everywhere -Need to trust -Can control disclosure to own comfort level, eases risk (IBT) -SSN is his boundary
27	“I am aware, there are plenty of possible uses of health data, identity theft is a possibility so I would be concerned to a degree but I am careful about who I give my information to, especially health. I give it to my doctor but he needs it to treat me. Technology websites, I’d like to know why they want it and how they’ll use it before I decide otherwise it would be too risky. With health professionals if they asked for anything excessive, I would want to know why. Fitness information isn’t too sensitive but I need to track.”	-Aware of risks to data -Cautious with data disclosure -Dr. needs data but excessive would question (IBT) -Discloses fitness data as not sensitive (IBT)
28	-	-
29	“Electronic companies would be a higher risk because they have no personal connection so they would have less remorse for sharing that information because they have no human ties to it. “	-Technology higher risk as no connection with data
30	“More so with technologies. With the doctor it’s face to face you can have more trust in that person versus the company or the organisation that you’re uploading your data to.”	-Technology higher risk as not a person – not physical
31	“I wouldn’t think my doctors would do that. I would be mortified. I would be really upset if they did that. I assume when my information goes to a doctor’s office that it never leaves. I just it’s used to treat me.”	-Assumes no risk of misuse by health prof.

Interview Participant	Health Professionals vs. Technology Vendors	Extracted Meaning
32	“Probably a doctor would be more dangerous because they see so much of it, it might not be as big of a deal for them. If a tech company has a responsibility of making sure that data is secure then they would follow their procedures and do whatever they were required to do.”	-Higher risk of loss with health prof as so familiar with data -technology would keep secure
33	-	-
34	“With a technology company they’re more savvy with security whereas in a doctor’s office somebody can walk away with a file, or copy a file, so you’re more at risk to just unethical people in a doctor’s office whereas with the data company it’s who they’re sharing and selling your data to, whether or not they have security protocols that prevent them being breached. It’s a different level of risk.”	-Different risk. Health risk of unethical people & physical -Technology risk of intended misuse but more secure
35	-	-
36	-	-
37	-	-
38	-	-
39	“There is probably a greater risk with technology companies but I was in the Blue Cross batch that got stolen.	-High risk with technology - privacy invasion experience
40	-	-
41	-	-
42	-	-
43	-	-
44	“I worked at Microsoft so maybe it’s different. Since HIPAA laws came in, I think major corporations are much more scared than your doctor. Your doctor goes through a training which is maybe four hours, for HIPAA. They learn this is what you’re supposed to do, this what you’re not supposed to do, you’re supposed to put it securely not defining what securely means, does it have to be vaulted, does it have to be double vaulted? So that’s why I rather prefer either corporations or the government to put technology in. They have a lot more to lose so they make sure that they design it correctly.”	-Health prof limited training -Technology have more to lose so design systems better
45	“The risk is higher with technology, I would say.”	-Technology higher risk
46	“It is definitely riskier to give it to technology companies. I do not do that.”	-Technology higher -doesn’t disclose
47	“Trusting a website is not like a person, you don’t know them you haven’t built like a relationship with them, if you’re trusting them with your health information then you’re taking that risk. I really don’t	-Taking a risk disclosing information to technology

<b>Interview Participant</b>	<b>Health Professionals vs. Technology Vendors</b>	<b>Extracted Meaning</b>
	understand why you would disclose certain things to them like on Fitbit I don't like the necessity, so I could see insurance companies trying to get information from technology companies."	companies – doesn't see the need to give them health data
48	"It's riskier to give that data to technology companies, definitely."	-Technology higher risk
49	-	-
50	-	-



## APPENDIX P: INTERVIEW ANALYSIS: SENSITIVITY

Interview Participant		Wider view
1	“Some people are very private, I’m the opposite so it wouldn’t bother me if an insurance company, life insurance, if they saw my medical history and, because I’d have nothing to hide, so therefore why would anyone have a problem, if they’ve nothing to hide?”	-She isn’t concerned as nothing to hide
2	-	-
3	“Health information is very personal. Like financial information I think that’s the information we want to protect most, maybe more than financial information. It varies too some information like sexual health or gastro problems, you would be even more protective of. But sometimes people need the information. Like mental health, in some cases revealing that information could help you but I think individuals with those issues would be very sensitive.”	-Personal information -Want to protect -Some types more sensitive
4	“Definitely. Especially some types of health information about your fertility, or any tests. Then mental health and sexual health they’re very personal. Your health relates to you as a person like it’s very personal and you wouldn’t just want anyone to know it. Other information I really wouldn’t be too bothered if people knew.”	-Sensitive especially some types -Very personal -Desires privacy
5	“Yeah. Really sensitive to me. It’s so personal. For me, my diabetes, like I hate the idea of being labelled because I’ve an illness. So I don’t think my diabetic status should be known by anyone really. I think mental health is obviously extremely sensitive and so is genetic information. Like that can have a massive effect on families like only very necessary parties not even my GP. That makes up a person.”	-Highly sensitive -Doesn’t want label -Other types sensitive
6	“Yes. I don’t have a huge health record but I think it is sensitive. I think people with more health information would be even more sensitive about it but generally speaking it’s very personal. Mental health that’s extremely sensitive and I’d want my doctor to know and if you went in to counselling I’d want to be able to get my previous notes for them. But no one else should know after that. DNA or genetics as well I don’t think I would want any doctor to have that I might get it done to see what the results are and once I see it I’d shred the results and not want anyone to see them.”	-Doesn’t have big record but views it as highly sensitive -Mental health and DNA very sensitive -Limited access to info
7	“Yes. I do think some information is more sensitive than others. I have asthma it would come up in general conversation I wouldn’t have any problems telling anyone. Thankfully it doesn’t really affect my life now. I wouldn’t really want everyone to know what inhalers I’m on or anything. It’s not too sensitive but if it was more chronic I would probably have a different approach. Domestic abuse is extremely sensitive I wouldn’t want people to know I would want my doctor to know but to respect the sensitivity of it. Substance abuse then is very sensitive.	-Difference between being aware of condition and accessing information

Interview Participant		Wider view
	It would depend a lot on the stage of it but that's just the whole idea of people knowing and even if you tell your story to motivate others that's very different than allowing people access to detailed notes. Mental health could harm your future employment and sexual health is sensitive too just for embarrassment."	-Some types more sensitive than others
8	"Definitely. I personally wouldn't want my weight shared with many people if any. When I was pregnant for example, because I have had problems with eating before I didn't want to know my weight, I spoke to my doctors and said I didn't want it in my chart but it was in my chart because I accidentally stumbled across it. So for me that's particularly sensitive and I wouldn't want it shared with anyone. I'd also be more sensitive about dental away probably due to my experience with my teeth I wouldn't want to share that with loads of people. And my eating disorder or could be pregnancy symptoms. I just wouldn't want the world to know.	-Highly sensitive -Doesn't want information shared -Has expressed this desire to healthcare professionals
9	"I think it should be, like some people have conditions like you could walk by them a 100 times without even noticing and then someone might say something oh this person has whatever and it can change your view of someone. I think it should be kept confidential, that should be kept between people you trust and people like your doctor, and people who need to know in an emergency. If someone wants their stuff private they should, for every condition."	-Changes view -Should be kept between limited parties -Control to keep private
10	"It's more sensitive than other types of information because it's something you want to keep to yourself, whereas you choose to put on Facebook I study this, but I wouldn't choose to share I have this wrong with me, it's more sensitive."	-More sensitive as less willing to share
11	"I do. Most people are sensitive about their health. Some jobs require a lot of written material and a person with dyslexia is afraid if anyone gets wind be denied job after job, so from a job point of view, they might find that extremely sensitive and guard it with jealousy. It's down to each individual person's confidence or their sense of what's right, whether they declare certain things. Maybe some people should be under an onus to declare so that it's known and they get clearance for doing whatever. I tell you what the one word in that encompasses a huge amount, is 'reasonable'. In any given situation or any given circumstance, if what you do or what you say is, you can be expected to do what a reasonable person with your position, with your knowledge, with your tiredness or whatever could be expected to do at that time, and you honestly do that."	-Most people are sensitive -Job opportunities -Should be reasonable and declare if necessary
12	"Yes, health information could be misused in the wrong hands so I would think it's much more personal than other types of information."	-More sensitive as can be misused
13	"I think it's a very private thing to be honest but if the wrong people get access to it or they look at it and say oh look what she has or something, whereas if they, it all depends on who's looking at it you know. People could look at it and say well I won't hire her or I won't hire her."	
14		
15	"Personal details and health details should remain private."	Should be private

Interview Participant		Wider view
16	“Much more sensitive than other information and especially if it’s mental health. If you’re suffering with depression or anything you won’t want the whole world to know that.”	-Very sensitive wouldn’t want people to know
17	“Yeah. Yeah. Very sensitive.”	-Sensitive
18	“Yes. It’s personal.”	-Personal information
19	“It depends on who you’re dealing with, your practitioner or specialist. I think in most cases you have to trust them; you can’t go saying I’m not going to tell him that. It is supposed to be confidential and I think most times it is.”	-Can be sensitive but need to trust
20	“It definitely is. It’s so personal and private. I wouldn’t want people knowing if I was sick. I mean if I had a cold I wouldn’t mind but anything more than that I just wouldn’t want people to know. When it comes to your health that’s not something you’re going to share with the world, I wouldn’t share it with many people at all at all.”	-Private and personal -Wouldn’t share health data with many people
21	“It’s up there with financial information because it leaves you very vulnerable to decisions other people make about you, it’s highly sensitive. The most sensitive I’d imagine is addiction, HIV, mental health and life limiting conditions.”	-Highly sensitive – vulnerable to decisions based on information
22	“Definitely because there could be stuff there that you’re embarrassed about or stuff that could be used against you even your employer, it might sway their decisions against you like you’re sick more than other people or I don’t know like you have this disability you know yeah. The most sensitive might be psychiatric issues or eating disorders or chronic conditions that people could be sick more so with.”	-Could be embarrassing information or misused -Psychiatric and chronic most sensitive
23	“Yeah there are two areas, one is health and people are very protective of their health information, and financial information. I can understand people being quite sensitive about health information because it does very often affect attitude towards you if you know if again the areas that shouldn’t be but they are you know mental health issues there’s an attitudinal change if I know you have a mental health issue and if I didn’t know I would treat you differently you know. So I think those areas are HUGELY sensitive.”	-Extremely sensitive -Can change attitudes towards you
24	-	
25	“Health information is very sensitive to me yeah”	-Highly sensitive
26	“If I had diseases, I didn’t want certain people to know about then would definitely understand being more concerned or if there was a health history that might affect hiring decisions then I could definitely see myself being more concerned but I see myself as generally pretty healthy. If I had some kind of chronic disease that would have some sort of implication on whether I was insurable, on whether I was hireable, that’s something that would not necessarily	-Would be more concerned if had illness that could affect insurance, employment

Interview Participant		Wider view
	want to give out if people are going to make a determination on you based on that. Obviously sexual health is important but that remains a touchy subject and I think addiction issues could be something you don't want surfacing again."	-Sexual and addiction information: sensitive
27	"Health information is more sensitive than other information. It does depend on what health information though. In general, I have no illnesses and I am healthy so I don't think generally my health status at present is too sensitive. Other information like mammograms or pap smears, those are really personal and I wouldn't like them to be shared with people that don't need them. I think sensitive health data like sexual or reproductive information is really sensitive and I'd put that on the same par as financial information, I wouldn't want either of that information getting out."	-Ranges in sensitivity -Some data is very sensitive -Desire for that data to not be shared
28	"It could be more sensitive than other information based on whether or not you are healthy and based on whether or not you have an extensive history of bad health or health problems The most sensitive types of health information are domestic violence, abortions, chronic illnesses, heart problems, those would all be really sensitive to me."	-Potentially more sensitive depending on information type
29	"It's sensitive information that people generally don't want to share, they may share it with people they need to, their doctors, and they may search for symptoms that they have, but they don't generally <i>tell</i> other people and they wouldn't <i>want to tell</i> them. So keeping that information private unless they're okay with it being shared or they're informed of it and consent to it, should be very important."	-Sensitive information -People don't want to share – privacy should be important
30	"Yes, it's pretty personal so if you had someone's financial information that could be a lot more dangerous as someone could steal all your money, but if someone had your health information that's <b><i>your personal information</i></b> so I think it's sensitive. Your sexual health would be something people like to keep private and that's nobody else's business and also addiction would be another one because you don't want people to know, I guess if you're an addict it helps sometimes to talk but it's not a piece of information that should be just given out that's at the person's discretion."	-Sensitive and personal -Views sexual and addiction as sensitive -Disclosure should be at persons' discretion
31	"There's not a lot to my record that I wouldn't want people to know. Like I don't have HIV or anything like that so I don't care what my doctor knows, I wouldn't care if my boss found out about my osteomatoses you know what I mean I just don't. So for that matter, I don't really have anything too sensitive in my system."	-Doesn't have sensitive health issues so more open to trying HIT
32	"There is more sensitive health information especially sexually transmitted diseases that would be very highly sensitive. You should tell everything to your doctor but that's private, it could change the opinions of acquaintances and friends and family, there's a stigma attached with some things. So it could be damaging to your relationships. Health information, it's so powerful and the ability to have the information is so easy it's so hard to put boundaries on it."	-Need to share with dr. -Should remain private can change opinions -Hard to control
33	"I think it's becoming a target of fraud for identity thieves, but I'm not convinced it is more sensitive than a social security number, which could have a broader negative impact on a greater portion of someone's life if it were stolen. It would have different impacts more emotional and could lead to blackmail or something very distressing but the	-Target for fraud but not as sensitive as SSN

Interview Participant		Wider view
	social security number is the key to identity theft so that's the most sensitive piece of information there is about a person."	-Emotional distress or blackmail
34	"Health information is private and it should be their choice whom they share it with and whatever motivations, companies have shouldn't be more important than the individual's ability to control their information and to choose who knows it, who shares it or doesn't."	-Private information -Individuals should have control
35	"Yes. Oh absolutely. My mother any problems she has they're looking to link it to smoking. You know that's the joke around my family, you could go in with a broken finger and they say oh you smoke, you know. That's the cause."	-Yes as changes opinions and treatment
36	"It depends on the person. For me, no it's the same as all information. There are some desirable uses for all information and some needs like you need to give health information to insurance companies for that to be paid. I think there's also lots of possible undesirable uses for these information types and you would want to keep both out of the public domain. But I don't think health is more sensitive."	-Not more sensitive -Needs and undesirable uses -Shouldn't be public
37	"Yeah, health information is worth a lot of money to a lot of different companies."	-Valuable information
38	"It is important because I had the polycystic ovaries problem and if a girl goes to gynaecologist they think a girl is just pregnant. That's a really wrong approach so I was afraid to go, even though I had this problem I could not go because I was thinking what will society think. If they do not know what PCOD and its like taboo. I do not really want anybody to know my personal health information unless they know what is that. It's kind of demotivating."	-People don't understand health issues -Wants her information private
39	"It's more sensitive than other types of information."	-Comparatively sensitive
40	"I consider myself a pretty private person in all areas. I think there's places to share that and there's places not to. So I think I'm kind of a private person in that way. I feel my health is nobody's business unless I want to tell them."	-Private person -Health is private
41	"I think it's more sensitive because, it doesn't define you but it's definitely a part of you. To me it's very sensitive, if I'm not willing to give you where I work I'm definitely not going to tell you what health issues I've gone through."	-Very sensitive not willing to disclose
42	"It depends on the level of health information. Test results I would rank up with there with my social security number. It's the stuff you don't want getting out it could be used against you by either employers or even family if you have a malicious family. It's something that can affect you and it's not something the world needs to know."	-Some health data is extremely sensitive - negative outcomes
43	"Illnesses where they look healthy get a different backlash because people are like you don't look sick why are you getting this stuff, you could probably work. Then there's another thing of you are representing my mortality, and I have no way of dealing with mortality, so I prefer that you're not here. My mom had breast cancer and some people couldn't deal with her mortality or their mortality. Mental health, I think people are like if I don't pay attention to it,	-Different ways of treating people -Don't understand mental health -She doesn't talk about it

Interview Participant		Wider view
	it won't be there. But a lot of people have mental health issues and depression runs in my family but I would never talk about that. Most people are scared of it, they don't understand it. It's like fix it, or they ignore it."	
44	"I do. A future employer may not hire you because of your health conditions so I think it is information to be more sensitive about."	-Sensitive as employment prospects
45	"Yeah. I don't have any major ailments, but if I did I don't know that I would want to share that information, like that to be potentially sought after by someone in my family or to employers or to school because I know their take on it might be different than what the actual diagnosis."	-Sensitive -People may misinterpret
46	"Yeah of course. It is more important than email or other things."	-Sensitive compared to other types
47	"All information is sensitive to me. I don't really feel stigmatized because of a condition, if I did, maybe I would feel it was more valuable or I wanted to protect it more than other types of information but I think our lives are so dependent on the internet and we have a lot of other personal information available even in your email. For me, they are all more or less equal but with health information I could be nearly more open because there's nothing that stigmatizes me."	-All information is sensitive to her -No possible repercussions
48	"It's pretty important. I'm trying to think of a specific type of information that's far more crucial but I can't. But things that would jeopardise your life or lead to stigma or jeopardise your financial situation that's sensitive. Like if you had an addiction that leads to stigma that could lead you to not be hired, that is quite traumatic like character changing things are maybe what's most sensitive. My health is pretty good. But if I did have something that might jeopardise a job, I would be more concerned. The fact I'm healthy definitely affects how I see health information sharing."	-Important information -Healthy but would be more concerned if not -Data that jeopardize jobs most sensitive
49	"Anything that has to do with sexuality is particularly sensitive because western society is particularly taboo about this topic people aren't too comfortable discussing that topic. I think the biggest criteria for me in determining sensitivity in this context is what can people use to blackmail you and what is extremely personal to the person and I think that sexuality, reproductive and addiction are some of the most personal issues that people encounter."	-Sexuality due to taboo -Information that can be used in blackmail
50	"For me, financial personal information is potentially more damaging to your reputation or life than health information. If someone cracked into a hospital and got my student health records, unless there's a social security number or personal information that could then be used to come back financial stuff, if someone wants to look at my blood test results, to me that's not really that big of a deal. There's a bias towards people who have diseases like obesity or diabetes, or depression, if that type of information got out, it could have a 'real' impact on your life, they can say, this person sometimes goes through severe depression so we're not going to hire them. It's how the	-Financial more sensitive for him -For people with illnesses could have impact on job side -Less problematic for healthy people

Interview Participant		Wider view
	information is used downstream that may be more problematic than someone having the information, but if you're healthy it's less problematic."	

## APPENDIX Q: INTERVIEW ANALYSIS: HIPC

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
1	<p>Sec Use: "it's going to benefit everybody, it might benefit me, it mightn't, but down the road it might benefit somebody, so I'd have no problem. I would hate marketing companies just do my head in. So, market research no, market research is all about making more money so why would someone want to make money out my illnesses."</p> <p>Control: "I imagine they request your permission and once I gave my permission."</p>	<p>Access: "I don't think there's any need for an employer to know all your medical history, if it's relevant to the job you do they are entitled to I believe in honesty. So if they're not going to be honest, maybe these employers <i>should</i> have the information, but then where I think some employers would abuse it, would be if somebody is recovering say from cancer and they're in remission, they might not give them the job I think they don't need to know the inside information"</p>	<p>-Research okay with consent -benefit -No to marketing due to profit -Employers only relevant data could lead to discrimination</p>
2	<p>Sec Use: "If my doctor was feeding information about my health to some Health Company, unbeknownst to me, that would concern me. A place said we're doing research on retinopathy it is not government funded so it's funded by people who sell products to diabetics. Now I found this was a way of getting around to sell more products which makes me believe that there's a certain commercial aspect which I would be too cooperative on."</p>		<p>-Sec Use a concern -Received letter from company for research not willing if commercial aspect</p>
3	<p>Coll: "I don't mind giving it to a doctor. I would rather them have the information necessary to treat me once they look after it but that kind of information I wouldn't give to an app."</p> <p>Access: "I'm sure it happens. Right now I wouldn't lose any sleep over it but I know it could happen anywhere someone could break into my house and steal my laptop but if I did have really sensitive health information maybe I could think about it more"</p> <p>Control: "I'd like an account with my doctor and log in and check the information is up to date. I'd like to be</p>	<p>Sec Use: "If they are storing lots of information and doing research but they keep my data anonymous I wouldn't mind I'd prefer they ask for my permission but once it was superficial like not in-depth analysis into my information. I wouldn't like them to share my information with any third party because you don't know what they're going to do with it and you only agree to the use by the doctor"</p> <p>Aware: "I do feel quite unaware of how my health information is used, some of it should definitely be regulated like clinics storing information should be</p>	<p>-Coll to dr. if needed wouldn't disclose to app -Access greater concern if had sensitive data -Desire to access &amp; change data -Research if anonymous, consent, and superficial</p>



Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	able to log in and check if everything is correct and make changes if I need to. That would be a comfort but it would mean that the information is exposed to the internet so that's a downside."	audited to make sure the information is encrypted, and backed up. I'd like that to happen and I'd like to be informed about it." Errors: "There's always a chance of human error, the computer is designed wrong or they entered it wrong. I would like to check my information was correct especially if I did have any more illnesses"	-Desire for awareness of security -Risk of errors greater concern if sick
4	Overall: "I'd definitely want the information kept private. I think my health information should only be accessed by the people who need to see it to treat me." Coll: "If my doctor asks for stuff that's irrelevant I wonder who it's going to be shared with I don't want it given to people I don't know even if they are doctors, I feel it should only be given to the people that need to know. And if I downloaded a health app and they asked me for loads of information that I thought was too much or irrelevant then I'd leave it blank if possible or if they insisted I wouldn't use it I'm sure there would be other similar ones I could download without giving information I didn't want to give. Access: "Sometimes it does not bare thinking about cos that information is more personal to me than any other information so when I think about it I would get very concerned and worry who can access my information I feel it should be just stored in the doctor's office."	Aware: "I don't think they share it. I don't know what happens with my information once I give it to the doctor to be honest...I think there should be some communication between doctors and hospitals if I was taken into the hospital and needed a follow up they should contact my doctor and give him the information. Control: "I'd definitely like to be able to control who can see my file and what they can see I don't think every doctor in Ireland should be able to access my health information. I wouldn't want it to be a database that you just type in a code and can see information about me...if I go to a new doctor I should be asked can they access my past information...it's not that I wouldn't agree I just want my permission to be sought before Sec Use: "I'd be worried about what my information is used for.	-Only necessary parties access -desire for privacy -Would withhold data from tech company -Importance of consent and permission -Concern of access can cause worry -Assumes private -Desire to control access and volume of access
5	"Yeah I would be definitely. Extremely concerned. I'd get frustrated if I was using an app for a specific purpose and it was asking for information that I didn't think was relevant and I wouldn't finish adding in the information and wouldn't use the app. In the healthcare setting, it depends on the level of authority for me and some trust in why they want the information I guess."	Aware: "Yeah that's probably the main thing if I knew where it was going and I could consent that would be fine but like a system or an app you don't know how many people that's fed to how much of it used or what measures are there to protect things. It's not that I'm embarrassed about my health but it's not knowing who is finding out things and what are they finding out."	-Coll concern if irrelevant -Access occurs accidentally, less concern for malicious -Risk of errors -Desire to be more aware of use & access

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>Access: “I would think it might happen and I know how easy it is for someone’s chart to left open or for someone to forget to log out, it can happen but I think the likelihood of it coming in to the wrong hands are very slim but I think it happens accidentally way too much.”</p> <p>Errors: “Yeah there’s definitely mistakes in everything from my experience its human error. I think paper is more susceptible to errors but the electronic systems are updated by people who make mistakes.”</p>	<p>Control: “I don’t have control and that’s an issue, it would be nice to have more of an understanding of what’s done with it, what it’s taken for. I wouldn’t like to have to spend days and days filling out consent forms but it would be nice to have some input and be able to click a box to say okay he can see this she can see that.”</p>	<p>-Desire to have some control or input</p>
6	<p>Coll: “It does because if I’ve given information before and they ask for it again I’m wondering where the information is gone. And a health app say you put all your information in and then you say it’s a crap app and you delete it where does your information go it doesn’t mean they delete it.”</p> <p>Sec Use: “A doctor there is some concern but it wouldn’t be too high. I think an app it would be because so many times you hear of things like that happening. I think a hospital can be held accountable but apps if they sell data or get hacked they’ve less accountability so I have more worry that my information would be misused.</p> <p>Errors: “Yeah there’s always a concern that you’re supposed to get surgery on one leg and they do the right one. I think the doctor should check smaller things are right so errors don’t go too far.”</p>	<p>Access: “I would be worried about that but mostly because you don’t have control over who sees it or how it’s protected”</p> <p>Aware: Yeah it would bother me that I don’t know how my data is protected or used you just make a big blanket assumption that it’s in a safe place and the only people that access it are those that should</p> <p>Control: I think it comes down to the information and how pertinent it is I think if there’s no need for a healthcare professional to know the information then they shouldn’t know. Like I can’t control who has access but it would make me feel better</p>	<p>-Coll concern of where information gone – apps retain data</p> <p>-Concern for apps to misuse as no recourse</p> <p>-Concern for access due to lack of control</p> <p>-Lack of awareness causes concern</p> <p>-Control could appease concern</p>
7	<p>“I’d place utmost value on it. I alluded to it earlier that things can have an impact on many aspects of your life such as your job you really don’t want it getting into the wrong hands say you’re on the internet someone could conceivably blackmail someone with this information as well. It’s particularly sensitive I’d place a lot of value in the privacy of my health information.”</p>	<p>Access: “It is a concern for me I might tell a cleaner or receptionist about an illness but I want to be in control. I don’t want people snooping. It’s something I would worry about I’d want total control and I’d want it set up in a way that was the most uncondusive to your data spreading.</p>	<p>-Values privacy of health data</p> <p>-Doctor needs data but wouldn’t disclose elsewhere</p> <p>-Control specific uses</p> <p>-Lack of control over access causes concern</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>Coll: “Not so much for the doctor I’d like them to know as much as they can. The more they know the more informed they are to diagnose. I wouldn’t give any of that information online.”</p> <p>Sec Use: “It would be really helpful if there was a list of set purposes they could use your information for and they could ask you beforehand then you’d have control and you could explicitly state you don’t want your information used for marketing purposes. And for the internet there are copious different ways it could be used most of them not necessarily what you’d want. So again not my plan to be offering information online you have no control at all.”</p>	<p>Control: “It’s the lack of control I have that concerns me a lot. It’s my information I should be informed and my permission should be sought”</p> <p>Aware:” I’m wary but not aware. I don’t know what’s happening to it and I don’t know legally what they can do. I do think a list of where the data can go would be helpful I know some people might not mind but I’d like to know. I don’t enjoy feeling uninformed. I think ignorance is the opposite to bliss in this situation</p> <p>Error: “Human error will always be there so it is a concern you never know what can creep in to things and its exponential then as the data is transferred from one party to another the errors spread and the risk of more errors increases.”</p>	<p>-Should have consent</p> <p>-Not aware</p> <p>-Errors can spread and cause damage</p>
8	<p>Coll: “If you’re there for one thing why they need to know everything else it might not be related it might be personal or embarrassing. Especially in phone app they don’t need to know everything. It’s personal it’s your own body or your own mind.</p> <p>Sec Use: “I do half think my phone is more secure than it is. I think especially small apps could be created by someone they probably wouldn’t have a need or obligation to secure that data and if he’s offered money to share information he probably would sell it. Like what’s his obligation. I often think my phone is safe cos I have my passcode but I think that perception of physical safety then makes me underestimate the potential uses of the data I already have disclosed. Even the diet apps like my Fitness pal there’s a lot of uses and what’s to stop them selling it or using it.”</p> <p>Aware: “I’m not aware of how the hospital is using my information. I don’t even know what they do with the</p>	<p>Errors: “I was near labour I got an infection and it wasn’t in my chart, the files had been faxed over to the wrong clinic and they couldn’t find them it was quite serious so they had to search for the results and make sure it was true and treat me.”</p> <p>Access: “I don’t have copious amounts of personal data but some of my data is very sensitive. Some older GPs don’t understand the danger of computers they might use them but don’t protect the information on it. For example, the GP I used to go to anyone would access the computer in the waiting room. I would be concerned about that which is one of the reasons I left that doctor. You want you know your information is safe when you confide in a doctor.”</p>	<p>-Coll relevance</p> <p>-Assumes safety due to physical protections</p> <p>-Unaware of uses</p> <p>-Control could appease concerns</p> <p>-Experience of errors with data sharing</p> <p>-Negative experience of access to data caused concern- left doctor</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>blood they take from me and do what they should be doing and nothing more like I've no idea.</p> <p>Control: "If I had more control I would feel better. I would like to control who knows what and who it was shared with and why."</p>		
9	<p>Coll: "with the doctor it doesn't, but for me putting all my details just to Microsoft or whoever, I would be concerned, I would give it to a doctor who is manually putting it in but unless it was a facility for a doctor I wouldn't do it. Doctors need the information and it's the experience it's an actual person whereas the computer doesn't care about anyone"</p> <p>Access: "I've wondered that a few times I know from experience that the information doesn't travel as a disadvantage as far as I know it's kept between the doctor and the patient. With technology, it's not your data really so they could be sending it to hospitals or whoever wants in that Fitness space, but it's not your data once you give it, sure it's not saved on Irish servers so it's not in your jurisdiction so you can't really do anything about it."</p>	<p>Sec Use: "I never really thought about but if it was anonymous then maybe it would be okay it could help if Pfizer or one of these companies can drum up something that can beat cancer or something miraculous then definitely I don't mind that as long as it's anonymous but if I went through the other route through Microsoft they're just getting the information for nothing and then selling it on, I don't think it's a great system, ethically."</p> <p>Control: "To a degree we have control we can decide where our health data is stored, there's always these new applications and people just sign up for them they don't even think but does it just serve the purpose of the company, so like with the health service I don't know it would be good sometimes it would be bad but as long as it's stored securely among people that can only access it if they need it Even consent or notice definitely or even at the start of a consultation say can I send this off for research, it's totally anonymous."</p>	<p>-No concern with dr. wouldn't give to tech unless linked to dr.</p> <p>-Didn't consider sec use research okay with consent and anonymity</p> <p>-Can't control once disclose data</p> <p>-Not aware would want consent before hand but research could benefit</p>
10	<p>Coll: "No it's important that they actually have that on hand to you know just treat you. With your doctor you have a special rapport you know you put your trust in them, whereas a technology company I wouldn't trust as much."</p> <p>Sec use: "No it's never really crossed my mind, it's just been I go to the doctor they help me and like they have my information on hand and that's it really. I assume</p>	<p>Control: "I don't feel we have a lot of control because I'd say for most people they just go in, say what's wrong and get diagnosed and that's it. I personally wouldn't about who is seeing this information. I'd like access to the information. I'd like to I'd certainly provide my information for research but I wouldn't want my employer to see it' I'd only really want people to be able to see what</p>	<p>-Coll no dr. need data less trust in tech wouldn't want them to have all data</p> <p>-Didn't consider access only necessary parties to relevant info</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>that's all it's used for. I wouldn't like a technology company to have it all and to use it."</p> <p>Access: "No it's never really crossed my mind. I wouldn't want everyone to be able to access it but I don't spend time thinking about who might be doing that. I think the doctors in the GP office, the nurse, and doctors in the hospital I but that's all only health professionals really. With technology I've never really thought about it. I've just assumed I put my information in, I've really never gone beyond who is actually reading this?"</p>	<p>they need, so if they are researching about I don't know skin issues, only what's relevant to them.</p> <p>Aware: "No I wouldn't be aware. We kind of live in an age where it's like, 'all my private information is out there I don't care' but I think we should care a bit and because of the society we live in, I think doctors should be saying I'm going to use this for research is that okay there should be communication and permission there."</p>	<p>-Didn't consider sec use research okay with consent</p> <p>-Desire for access and control of access and use</p> <p>-Not aware but desire for more awareness and consent</p>
11	<p>Sec Use: "Purely for the purpose of keeping you as healthy and safe as possible at all times for the entire duration of your life. I mean there is no other legitimate use that I can for an individual's health information. Now if a group of specialists needed access to a big wide database, in order to get objective view of a trend or whatever that could help research and fight illnesses or ailments, then they need to ask them with a clear explanatory thing saying what's needed and they want to access your data purely for X, Y, Z purposes, people have a chance to say no. It should be anonymous. Again identifiers in terms of male female, other than that the individuals should not be able to identified. If a big pharma company wants information to assist in legitimate research that's fine, same caveats, same requirements for, give people the opportunity to preserve their own general privacy considerations. But at the same time, it shouldn't be I think something that is made inordinately difficult, if there is no danger that an individual's specific identity being known."</p>	<p>Aware: "Yes with consent but sometimes if you go to somebody with a form and say our company is carrying out research you might make them frightened quite unnecessarily, they might not begin to understand what it's about, it's something that might help them or their family in the future, and it's only if it's done in a way where the company concerned would not be even able to gain access to the person's name and address to send out an invite to do a questionnaire, then that's the safeguard in itself, that you're only talking about a broad basis. So yeah personally, I would have no qualms about somebody know I had a hernia operation or whatever."</p>	<p>-Main use to keep you healthy</p> <p>-Research for legitimate reasons only not commercial</p> <p>-Anonymous no way of identifying or contacting</p> <p>-Inform citizens but can lead to unnecessary worry</p>
12	<p>Access: "This neurologist guy when I got the report from the GP the last page of it was CC'd to every consultant I had ever seen and I was thinking, I saw an ENT guy with</p>	<p>"If it was something that would help other people yeah I wouldn't mind that, once they ask me but I don't think names or anything like that could ever be</p>	<p>-Concern of sharing w/out permission</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>the Sjogrens but he doesn't need to know whether my hip is gone or anything else. I didn't think that should have happened without asking me first, he should have asked me or said I'm going to send this on."</p> <p>Aware: "No, they don't and I think unless you push and ask them questions they don't give you the information that you're really looking for."</p> <p>Control: "I'm not so sure you know after getting this thing (letter re bowel screening), as to who has the information, or what they need it for."</p>	<p>used because that's personal information, and you don't know who it's being shared with and somebody could pick it up and say oh 'I didn't realise she had a mental health problem.'</p> <p>"I would want to know who accessed my information, and how much they seen and why."</p> <p>Aware: Education would be a pre-requisite for otherwise people would go blindly and not fully understand what they were committing to."</p>	<p>negative exp. of oversharing relevance</p> <ul style="list-style-type: none"> <li>-Aware need to ask Qs, need to educate</li> <li>-Desire to control access and audit log</li> <li>-Sec use if could help others – need consent and anonymity</li> </ul>
13	<p>Access: "In that area of speciality, if it's going to benefit the population that's what they're trying to do in the Mater, that one hospital can access another and if something is going on in one hospital that they can share."</p> <p>Sec Use: "Number one to treat the patient and number two research because how do you find out how to improve something unless you do research. Consent is just a matter of respect. When my dad died, I get a call about three weeks later to say we didn't use any of his organs. That upset me, I said 'I didn't give you permission and if you did' I got extremely angry, I was shocked to get such a call to think that they could just go and remove peoples' organs. Now I know it has been done with babies and parents didn't know. Now if you give consent to do that, that's fine. I wasn't even thinking along those lines, it's just disrespect of the person's dignity."</p>	<p>Sec Use: "I don't know, because the drug companies make so much money so sometimes I question that"</p> <p>Marketing: "If the information is valid, but I think you have to be careful that the information is correct because if it isn't it could do damage and I wouldn't be for it. People might feel stigmatised. I don't agree with giving that information to use just for profit unless they said I'm going to give your information and if they said okay, well then fine but I think that if they don't agree to it, then they have the right."</p> <p>Aware: "I send it thinking this person is getting it and it's a message. I never think of how it might be used but don't use health technologies. The hospital could get into a lot of trouble if they did that. And technology companies, I would hope they wouldn't do that, it would be unethical."</p>	<ul style="list-style-type: none"> <li>-Data to treat patient and medical research</li> <li>-Consent important for respect and dignity</li> <li>-Marketing importance of accuracy could lead to stigma – right to opt out</li> <li>-Unaware of uses for any data – does not disclose health data online – hopes no secondary uses</li> </ul>
14			
15	<p>"I can understand medical people for research purposes because I've helped out over the years and I've no problem with that to a certain extent but if I think people are getting too nosey then I get suspicious. If I volunteer or something like that, I don't like things being imposed"</p>	<p>Control, Aware and Uses: "Not always no. You don't know what they do with it. Maybe they use this for research and developing products and but I don't like the fact of people knowing, strangers, big companies or faceless individuals knowing too much about you. Now I can understand to a certain extent</p>	<ul style="list-style-type: none"> <li>-Believes sec use happens</li> <li>-Research only when voluntary</li> </ul>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	Sec Use: "It doesn't keep me awake. I think they do give it drug companies. I don't like the secrecy."	that they have to develop products but it's the bottom line that counts, there's not a clear definitive answer to that."	-Should be more open and be able to limit information disclosure
16	Coll: "If you had to repeat it every time it's very stressful, I don't think you should have to explain all your health history, they should have that at the click of a button" Sec Use: "I haven't actually ever thought about it like that, but I wouldn't like it to go all different places. If a doctor asked permission, I wouldn't feel as bad about it as someone just gaining access to it. I'd freely give information if it was to help other patients, I wouldn't mind it, or if it was research, but not just a free for all, I wouldn't like that at all."	Control: "I'd like to be able to say don't use it for profits just use it for research and helping people, anything to do with money or profit no." Aware: "I thought once you gave it to the doctor that was it, it was just you and the doctor, that door was closed, it was behind closed doors what was said in that surgery, that's how much I was aware." Access: "the receptionists I don't like them knowing my business, that should be just the medical profession. I never really thought anyone could have your information I thought it was between you and the doctor"	-Coll should be stored -Access only health prof. -Assumed no sharing -Okay with research if consent Desire to control uses no commercial -no awareness assumed safe
17	Coll: "You're not going to give information unless you have to, you have to give it to the doctor, you don't have to give it to Google." Sec Use: "I always thought my file was in there in the hospital, sure anybody can get it you know, the same way that anyone can get it on Google, but it's different, if it's in the hospital it's different, you have a sense of trust."	Access: "Only doctors, only medical professionals that you are face to face with, that need to know your information, it's on a need to know. I really don't think like receptionists or any of them should be looking into your files now, personally."	-Greater trust in hospital to protect data -Access only health professional, not other health workers
18	Coll: "Their computer could be robbed but if you want a doctor to treat you, you have to tell him your information and you can't expect him to remember it so you have to let him do that. I wouldn't be inclined to give it to Google or any of them." Access: "I suppose their secretary or nurse can see it. The only reason you give your health information is for the doctor to treat you so that's the only person that should really see it."	Control: "Not 100%. I'd say if the doctor was asked, it would be anonymous, like they would just be doing a survey on a particular thing. Anonymous, I wouldn't mind, if there's 3 people, but if they're going to say that this person, I wouldn't like." Sec Use: "I've never really thought about that. I suppose it could be used for a survey if they wanted to look into how many people had different diseases. I'd like to give permission if they wanted to use it"	-Coll doctor needs data wouldn't give to tech -Access only dr. as needs data -Okay if anonymity and consent
19	Coll: "I suppose your family if you trust them, and doctors that are treating you."	Aware: "I suppose they just have it on the computer that's it, I don't suppose there's very much security"	-Access doctors and family

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	Sec Use: "I assume they just use it to treat me. I don't think the health information should be given to Google or any of those who could use it for something else. Because things do get sold don't they? If it's no names that's okay because I do believe in research and people have to learn	apart from the office being locked. But I don't see why somebody would want it you know, I think if they're breaking into a doctor's surgery it's not for my file, it's for money or drugs."	-Assume no sec use, okay with anonymous research with consent -Views risks as physical
20	<p>Coll: "With a doctor it's fine. It's his job and he probably should store it electronically. Once he has some sort of security on his files. With specialists if I think they're asking about things that aren't too relevant I would ask why they wanted to know and then decide If it was an app asking for all that information I wouldn't give it definitely not. Oh I'd delete the app. Come on why would I tell them I've low whatever vitamins?"</p> <p>Sec Use: "It doesn't keep me awake at night but I have thought about it before. And if I had any health conditions that were embarrassing or serious I would be far more concerned. I would like to think that my information isn't used for anything but to treat me. You need to have that faith in health professionals. If I gave it to a technology company, I'd worry that they'd use it for all sorts of things. Like even with my running app, I'm sure they use that for research maybe sell it to marketers and that would bother me but if it was information related to my actual health it would be a whole lot worse. I wouldn't mind with doctors or hospitals doing research once I was aware and I could give permission. It would have to be anonymous but helping someone else is a great motivation to put yourself at some risk."</p> <p>Errors: "I think so definitely. I would hope there's none but it would be great to be asked like to double check the information is correct at times, for the safety of both the patient and doctor."</p>	<p>Access: "I have thought about can they receptionist see everything? Because she's not qualified to interpret the information so she shouldn't be able to access it she'd be making assumptions that weren't accurate. Again with technology companies I'd worry whether all employees can access data and see personally identifiable information too to link it to me and whether they were sharing it, they've the commercial motivation to share it."</p> <p>Control: "Not enough. Like I said I would hope it isn't really used but if it was to be used I would definitely require full details and to give my permission if that happened without my permission I would be far from impressed. Some control can really help reduce fears especially with information as personal as health data."</p> <p>Aware:" no but I would really like to be. I could ask more questions and they could be more forthcoming in explaining okay everything is safe and not being tampered with. I think it's trust and doctors have the attitude that they should be trusted automatically."</p>	<p>-Coll need once secure</p> <p>-No sensitive data to apps, not relevant</p> <p>-Has considered sec use – more if had illnesses</p> <p>-Hopes not used but assumes tech do – would be worse if sensitive data</p> <p>-Risk of errors hope there is none</p> <p>-Access concern if unqualified people</p> <p>And in tech companies</p> <p>-Not even control - more control could reduce concerns</p> <p>-Desire to be more aware</p>



Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
21	<p>Coll: "It's probably more sensible to do it electronically than to have bits of paper lying about, if I was nosey it would be far easier to flick through a big cupboard inside than to hack into the computer."</p> <p>Sec Use: "I would expect them to be using it for research in that I would expect to benefit from this doctor's experience, it would have to be anonymised. I would be concerned would be that the technology company would be using the information to sell off to some other company and unless they're explicitly penalised for doing so, they would do it. It sounds like a nightmare; you can see your health insurance company saying but you told us you're looking after your health but you've only got 500 so we're not covering your last heart attack. They're not getting it for free, then I've got to ask why are they doing it, if the product is free, then I'm the product."</p>	<p>Access: "I don't have very much health information and it's pretty localised to one GP surgery."</p> <p>Control: "I've some control over that. It's based mainly on trusting him"</p> <p>Aware: "usually there's some kind of consent forms I would assume for things like that. My own GP has never asked for me to consent for any studies that they're doing, that might be because they aren't doing any studies."</p> <p>Errors: "I'd say generally the computerised records would be more reliable but if they go wrong they really can go wrong."</p>	<p>-Electronic storage safer</p> <p>-Anonymous research okay but unaware of research assumes consent</p> <p>-Access not concern little data exists</p> <p>-Concern for technology companies using that data wouldn't disclose</p>
22	<p>Sec Use: "If the patient consents I don't see that as a problem I don't know whether you could track, your family's past medical history if your granny had the breast cancer gene would that be flagged then on your file, but then are you using her private information to better the health of someone. It could get messy. I think even for education purposes, for student nurses and doctors and it could be good for them to see with patient's permissions. It's a grey line again, would you sell it on to drug companies and then they're targeting Ireland with these certain drugs I don't know. But maybe if you do they could carry out research in these areas in a way you could be benefiting the patient but then are you just benefiting the company to get all this information and then design their drugs and make their money."</p> <p>I would want to be able to consent, I'd want to be informed why they want it, how they're going to use it,</p>	<p>Control: "I suppose you can request our files and I think that online is more permanent whereas if there was a mistake and you forgot to sign for a drug and it was paper based you could get rid of it fairly easily whereas if it was online maybe not so much. Even So I think something like that you could see when the doctor was last online like I checked her. You could prove it then."</p> <p>Aware: "I'm sure there's a lot of information online like cookies that are tracking me and I don't know what it's used for. And I think most people are unaware. I'm sure there's so much data used for me that I'm unaware of. I think with health kind of stuff people should be made aware of what it's being used for and if someone else is using it. I'm not really aware of how they use my data, map my run could see exactly where I run and how past I</p>	<p>-Research with patient's consent grey line of profit vs. benefit</p> <p>-ethical uses of data</p> <p>-Desire for consent and awareness prior to uses and genuine reason not profit</p> <p>-Control of audit log</p> <p>-Not aware of data uses potential of fitness data use and profit but not sensitive so not worried too much</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	but I'd see why if I was in the hospital and someone was like we have a student nurse or a student doctor do you mind I'd be fine but I would want a reasoning behind wanting my information not just to be sold to pharma companies"	run around those areas so you know and maybe they could send that data and people could make money off it you know but I suppose maybe I'm not that worried about I guess"	
23	Control: "I don't think so. I think there's a bit of a free for all out there at the moment, I don't think it's controlled properly. I don't think consent is sought for lots of things, there needs to be tighter controls." Aware: "Straight forward no because it could be happening and we don't know about it. It's only when it gets to a serious situation that somebody might find that their information is out there but I'd say there's a lot of information out there that we don't know about our health, that we haven't agreed to.	Sec Use: No problem with research with consent. "I have two brothers in research in drug companies and I see the value of them getting the proper information, so again I wouldn't have a problem with that if I had <b>consent</b> , and it's not the mundane that's shared anyway but I don't think I'd have a problem, it's for development of drugs and I know they make big money out of it. I don't mind that if there's an opt out option, it wouldn't bother me as long as I can get out of this and say no"	-Lack of control need for greater controls -No awareness data could be used without permission -Okay with research and marketing if can opt out
24	Sec Use:" guess the sort answer to that is that I would like to see it used to streamline processes in order to maximise the benefit to patients of systems. S like I said if I have a heart attack on the street, if I have an identifying a name, or number whatever that paramedics can use to access records so that they know I'm allergic to penicillin for example, I think that is potentially very useful. Em knowing the way records get lost in hospitals, I think it would be useful to have a central database but you need hospital buy-in as well, it's not just individual em so that's I think possibly an obstacle. I said insurance companies could have access to some of it again that could streamline processes and speed up kind of coverage and so on. I mean there's also the side of it that people can take some control of their own health and their own again the phrase wellbeing. Em and I think people like doing that, you know there's a sense, an illusion I would	In principle yes, in principle yes and in practice if for example I were unconscious that becomes a bit of a problem em so yes I would want it to be standard practice but I suppose that would have to be worked around, next of kin perhaps something like that em to grant access, I think that would be okay, yeah so if you can't find a next of kin then you can't access it I think, yeah that would be my position on it. <i>Okay and what about other uses like being passed on to pharmaceutical companies?</i> Ahh for what purposes? I mean again if we're talking about for research em on the same basis I think em consent every time ahh and I would like to be told what for in the case of pharmaceutical companies' access. Em and in terms of marketing I'd rather not em I mean I don't know how that would be different really, but I feel it would be different so. As I said	

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>say, but a sense of control and I would be I've no problem with that in principle but I would be a little concerned with how the data would be used.</p> <p><i>Okay and what about research?</i></p> <p>Yeah, em I suppose I guess in the same way as technology approaches this, I would want to be asked. I would actually have no problem with my medical data being used for research but I would to be asked, em you know when your computer crashes when word crashes and it says do you want to send an error report, that's as much as I would need, but I would want it, and each time I would want that consent, so blanket consent is not something I would be comfortable with but it would be opt-in rather than opt-out for me I think.</p> <p>Access: Not really. Em no, not really. I mean in any situation that I've been aware of where somebody who isn't directly working with a patient goes to look at their information is where somebody has asked them to, somebody is a friend of somebody and says can you just have a look over that so no not hugely I wouldn't be overly concerned about that</p>	<p>earlier I have questions about the ethics of access to data for profit purposes and I understand that research is very often tied to profit, but I think it's still different em yeah.</p> <p>Yeah. So I think, I mean there are always ways around this in terms of where a company operates and things like that. Again I'm sort of talking in a perfect world, but I would prefer that any data related to my personal health given freely or otherwise would electronically be subject to some control from me. So third party use of data I put into this for example glow app, I would want to be able to be asked when, and mostly they do, mostly there is a box saying we want to pass this on, but I would want that to be quite stringent, and easily trackable, I'd like, I think that would be useful to be able to trace, if I could see where my information is I think that would be useful.</p> <p><i>So kind of like an audit log?</i></p> <p>Exactly. I think that makes sense and I don't think it would be too difficult.</p> <p><i>And do you think it would be important that we would be aware about what happens to our health data?</i></p> <p>Yeah I think so, and I've already said I'm pretty lazy about this stuff, 9 times out of ten I think I probably wouldn't bother even checking but I would want to know that I could check and that I could have some input into saying where my information goes, not necessarily how it's used once it's gets there, in the sense that if I say yes to marketing and they market me something I don't want well that's just, I can live with that, em but if I decide that I'm not comfortable</p>	

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
		<p>with for profit use let's say across the board then I would want to be in a position to be able to say I don't want this being done and that there should be some system of redress if I find out my data Has been wrongfully used and possibly a way of I think you could, if you had a sort of centralised profile which I think all this would be based on, if I could set like automatic bars so for example I wouldn't be asked whether a pharmaceutical company can have access to my data because I've issued a blanket ban on that so those types of settings might go some way towards making it more secure. I'd also have some concerns not about usage but em about unauthorised access so hacking that sort of thing, I mean that's something we kind of live with now.</p> <p><i>Do you have that concern now with your health information?</i></p> <p>My health information not really but that's partly because I'm in perfect health, so there's nothing to be gained from any of that information em but I think if I were suffering from an illness or particularly a mental health issue, then I might have concerns I don't know. I would have the same amount of concern about health as I would about money I think. Em ballpark I would guess so yeah.</p> <p><i>And now do you feel aware of what happens to your health information when you give it or where it goes?</i></p> <p>Em probably slightly better than average, but probably not much better. Em I have a sense of what happens to the information that is taking in hospitals and doctors' offices but that's incidental it's not something that I've sought out particularly. With</p>	

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
		regards to health apps, no, I have a sense of where it goes but no, and it's quite hard to trace the information in any meaningful way I think. So yeah I wouldn't say I'm massively concerned about it but I'm aware that I don't know much about it.	
25	<p>I would have in the past but I mean all this is probably eh academic in that I'm sure I've signed it away somewhere down the line without even realising it so I no longer worry about it.</p> <p><i>So what kind of uses for your health information would you be okay or comfortable with?</i></p> <p>If it's anonymised research I've no problem so I mean your date, not your specific date of birth but your age range, or where you live, your race and gender you know the area you live etc. I've no problem with any of that, if it's used in research I've no problem with that. Your name shouldn't be used. Anything that can be used to easily [emphasised] identify ye, I'm sure with enough extrapolation you'll get there but anything that just has a big sticker on the top that says this is information related to me, I would have a problem with that being shared. But the data itself to giving it in question or to give an understanding to researchers who need to know what is happening with the health of men of a certain age in a certain area who lived in a certain place during a certain period none of that really bothers me.</p> <p><i>Okay and would that be with consent or automatic use?</i></p> <p>Eh I would prefer if there was consent, but if it was anonymised to a good degree it wouldn't eh I don't think I'd be too upset, I wouldn't sue them for it.</p>		

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p><i>Okay and what about any further uses so selling it to drug companies or to companies to market towards you or anything like that?</i></p> <p>Totally unacceptable.</p> <p><i>Okay. Do you think that happens or would you be worried about it?</i></p> <p>That's happening, 100% that's happening. I don't know if it's happened to my data but absolutely 100% it is happening. Now in fairness, we expose ourselves to it immediately upon doing a Google search for anything. So if you Google 'gangrene' and you've logged in using your Facebook login or whatever it is or your Google+ then you are, somebody somewhere has got that information now and they can link it back to you. So when those advertisements, you know the ads pop up advertising gangrene cures that's why, so yeah it's already sold, it's already gone. But it's not detailed and it has the step, there's that gap between, it's not reality, it's still not the real world, we can pretend it is, but it isn't actually. So if somebody says to me 'You Googled gangrene', well so what it doesn't mean I had gangrene you know what I mean. Whereas if the doctor records he has gangrene, and that's sold that's a different thing.</p> <p><i>At the moment do you feel aware of what happens to your health data once you give it to health professionals?</i></p> <p>No.</p> <p><i>Do you think we should be aware or will be ever be?</i></p> <p>Em I don't know, well we could be, should we be concerned about it to a degree yes we should be, we should be aware of it yes we should be, it could be quite complicated, it could be difficult to explain that as it is. Em but if it's a straight up we don't tell anyone who you are but we use the information regarding your health</p>		

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>status without anyone knowing who you are for research purposes, I don't think, I think most people would have absolutely no problem with that, in fact they'd encourage it.</p> <p><i>Okay. Do you feel like we should more control over what happens to our health data?</i></p> <p>Yes, consent should be required for anyone who is a third party regardless of what it is used for. I mean you could put the, your classic whatever you called it opt-in, we're opting in to include the anonymised data for research, I don't think that's a problem, but I mean I had calls to run in with the Data Protection Commissioner a couple of times in a previous life and their definition of personal data and what I would believe to be personal data are widely at odds. I don't believe a name and address to be personal data whatsoever, I mean your name is public record [laugh] you can change it if you want, and your address is in the phonebook unless you take it out but even then you need an address but that's deemed to be highly sensitive information I wouldn't put that anywhere near as sensitive as blood test results, anywhere near, it's a totally different planet. So if you divorce the two then one means nothing and the blood test results mean nothing.</p> <p><i>Because they're not tagged to the person?</i></p> <p>No.</p> <p><i>So if a technology company then had access to your health information, do you feel like you'd have control over it then?</i></p> <p>No.</p> <p><i>Do you feel you should in that context?</i></p> <p>Yes, it's probably, I mean it's, probably already buried in there in your account settings, anyway. Em. They shouldn't, I mean I just full stop don't believe health</p>		

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	information I don't know why you'd want to record medication etc. on your iPhone, I have to say that baffles me.		
26	<p>Coll: "I can see it being a concern in the future. I control would always play a part in that. Whatever I feel comfortable disclosing is the control I want especially with technologies. I guess as ye age, more things tend to go wrong with ye so I can see that being a concern for me in the future but not really now because I control what I give to the likes of FitBit. The concern would be higher with technology companies there's always that business aspect to it so you're always a bit leery"</p> <p>Access: "Now it's not so much a concern I don't think there's a whole lot out there about me I'm worried about and I think that goes back to the health I'm living in the age where if someone really wants the information whether that's a hospital porter or a hacker if someone really wants it for good of nefarious reasons they'll get it."</p> <p>Sec Use: "When you give the information away you lose that consent to so at if you've given it away it's on you."</p>	<p>Errors: "With the human aspect of it, you'll always have errors in paper and electronic records. I think you have to have faith in the system that people are doing enough checks."</p> <p>Aware: "I can't say I know how it's used. I don't think I gave them anything I would be worried about. Hopefully they're just using it when I come in"</p> <p>Control: "I would want the ability to opt-out of giving certain information or being able to raise the question of what is this being used for but once you give it, it's out of your hands, it's gone, it's protect your own self with your own questions, once it's out there it's out there."</p>	<p>-Coll future concern importance of control esp. with technology commercial aims</p> <p>-Always risk of external access</p> <p>-Risk of sec use - control what you disclose (IBT)</p> <p>-Risk of errors need to trust system</p> <p>-Not aware -hope only used for health, tech no sensitive data (IBT)</p> <p>-Desire for control to consent or question</p>
27	<p>Coll: "No, giving health information to my doctor isn't a concern, I only visit him when I have an issue and you've built up a relationship. I trust he only uses the information to help me. With technology, data is collected without my knowledge as I walk etc. and I'm comfortable with that information. If they asked for information that was excessive or irrelevant I don't know how I'd feel."</p> <p>Sec Use: "With doctors I hope they don't use it for another purpose. It is a concern to a degree that it might</p>	<p>Errors: "I don't worry too much about errors because the lack of serious information but I wouldn't want it to happen, its linked to other things like if it was accessed by insurance or used for other purposes I wouldn't want especially if it was worse."</p> <p>Aware: "I do feel aware of how my doctor uses my information. With apps I don't feel aware but I don't think they have much to use and if they did I'm sure it would be anonymous, they do have my name</p>	<p>-Coll need data with tech IBT</p> <p>-Hope no sec use is healthy, no trust in tech greater risk</p> <p>-Access: possibility but trusts in dr. and HIPAA</p> <p>-Aware for dr. but not technology but not</p>



Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>happen but I'm quite healthy it doesn't bother me too much but that doesn't mean I'd want my health information to be used for other purposes, not without my consent and knowledge. I think with technology its more of a concern because there isn't the trust but I don't give them too much information."</p> <p>Access: "It's a possibility that undesirables might have access and it has crossed my mind but I hope it doesn't happen and I trust that the health provider follows HIPAA to protect it and ensure it doesn't happen."</p>	<p>which I'm okay about because I really wanted to track my exercise. Awareness is really important for me I think my doctor could make me aware of any other reasons he wanted to use the information and so could apps then I might agree once I have the ability to consent.</p> <p>Control: I can get a copy of my file. I don't have control to say who sees my information but I'd like that, it's important. I want to be able to say who can view my information and what they can use it for."</p>	<p>sensitive -privacy calculus and IBT</p> <p>-Some control, desire for greater control over access and uses</p>
28	<p>Coll: "it wouldn't be a concern for me if my health provider asked me for information because they need that information but it would be a concern if my employer asked for that information its dangerous territory."</p> <p>Access: "It may be a concern but it hasn't been in the past because it hasn't been something I've thought about but I would not want my information to be accessed by other people."</p> <p>Sec Use: I think so. It's a big industry and any information you give in any field can potentially be used for data mining. Its dangerous territory and definitely could and may happen with health information</p>	<p>Control: "I feel like you don't have any control over it right now but that we should be able to have some control. I would like it."</p> <p>Aware: "I don't really feel I am aware of how my health information is used and I never really put too much thought into it before but I want to be more aware and know where my information is going."</p>	<p>-No health prof. need data</p> <p>-Access could be a future concern does not want data accessed</p> <p>-Potential for secondary use</p> <p>-Should have more control</p> <p>-Aware: Not fully aware but wants more awareness</p>
29	<p>Collection: "I feel people in society expect that. It would be nice to know that they're keeping it and for how long, they usually tell you. It doesn't <i>concern</i> me because it will help them if I ever come to them again. Again, I would just like to be let known. Technology companies would concern me more because I don't see an immediate reason for them needing that. I don't feel like they should ask for more than they need.</p>	<p>Secondary Use: "I do think about. Yes, a little more concerned because I can understand medical history's use in research and looking at trends. Transparency would be the biggest issue if they were to inform the person and they could use it honestly or not at all, then it wouldn't concern me as long as I'm aware of it."</p> <p>Aware: "I'm aware in the particular case of my hand that information could still be in circulation</p>	<p>Coll: expectation would like more awareness but not concern as records can benefit -technology would concern – relevance</p> <p>-Access always a risk but not a concern now</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>Access: “It’s not an immediate concern but I suppose if you’re sharing your information at all you’re running the risk of someone seeing or hearing about it, it might get stolen by a hacker so I don’t think of that but that’s just the implied risk that I’m taking by sharing it all.</p> <p>Control: “Control is something I should have but I was saying earlier you run the risk of someone having your information that shouldn’t, every time you share it at all, in an ideal world everyone who wanted to share my information would ask me and I would say yes or no and I generally trust professionals and people I normally give my information to, to tell me and ask me because if they say we’re sharing information and don’t really give me a choice then that defeats the purpose</p>	<p>but if so I’d assume they would use it anonymously to help someone in the same situation. I worry about it a little bit what if they attached my personal information to it but I would see no reason for them to do that and I would trust their integrity. With other medical information, I wouldn’t be concerned unless it was rare.”</p> <p>“Transparency could help with concerns</p>	<p>-SU: Benefit for research -consent and transparency  Aware of data shared  concern for PII attached but has trust  -Doesn’t fully have control – would like full control of access and uses</p>
30	<p>Coll: “If I go to the clinic for a tooth ache then other information doesn’t matter. I’m sure there’s a bigger reason <i>but</i> it does bother me. When I had the FitBit they have the smiley face or frown face and that’s good information for you to look back on and I wouldn’t have any problem if FitBit take steps versus how happy, that wouldn’t bother me if they told me about it first. If they were looking for detailed mental health notes from your doctor, I wouldn’t give that “</p> <p>Sec Use: “With the doctor it wouldn’t be a concern because I feel like if you’re at a hospital <i>if they are</i> going to use it for something else it should be beneficial but the FitBit when you’re uploading all your information electronically it’s the same as putting information online and anything can happen to it. There’s the possibility always.”</p> <p>Aware: “In general I don’t know where the information goes. I assume that it’s used for personal use and on your device but they could whatever they want and it would be</p>	<p>Access: “I’ve never really thought about it, for me the information I give to my hospital or doctor I trust them to use it in a good way and if there was an emergency and I couldn’t give them the information and they could access because they have it in the system so if it was a time-sensitive emergency I would want it to be available for them. With technology maybe a bigger company that owns a lot of different things and they could put all that information together.”</p> <p>Control: “I don’t have control now cos when you go to the doctor you give your information and they take it and put it wherever they see fit. And with technology sometimes they give you options but most of the time there’s not so I think they could do more at least to know where it’s going before you sign up or give the information.”</p>	<p>-Coll if not relevant  -Okay with sec use if consent &amp; not sensitive (IBT)  -Sec use health only for benefit with tech always a risk  -Access benefit in health but tech could link data together  -Not much control some options but desire for awareness and consent of sharing and uses  -Not currently aware</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	nice if companies would give you the option 'do you want to send your information here' or would it be okay to send your information here or there' or if they let you know where your information is going then at least you're aware before you give it."		
31	<p>Coll: "I just went to a chiropractor and they collected all of that and they stick it behind the desk and I think my social security is on there and, it genuinely concerns me. So I'm more concerned about instances like that than I would be with a tech company.</p> <p>Sec Use: "It never even occurs to me that they would use it for something else. I wouldn't even think that my doctors would do that. I would be mortified. I assume when my information goes to a doctor's office that it never leaves that doctor's office. I just assume it's used to treat me."</p> <p>Access: "I don't think anybody but the person that works there and that doctor should be looking at that information. I've given information to them for that purpose. I didn't give permission to a drug company."</p>	<p>Control: "I've almost no control. I don't know what they're typing, I don't know what they're putting in my records. I should be able to go online afterwards and look at and I think they would be more honest in their assessments in and diagnosis of us."</p> <p>Aware: "I want to have a frank conversation with my doctor what are the safeguards that you have for my records. That's not something I ever thought to ask, do you sell my records, what are the safeguards protecting my records is it backed up here, is it backed up somewhere else yano. Those are the sorts of questions that never even occurred to me to ask"</p>	<p>-Worry of paper loss</p> <p>-Doesn't consider sec use – no other uses would not be happy</p> <p>-Data only provided for health purposes does not want disclosed to others</p> <p>-little control desire for access</p> <p>-Not aware but desire to ask questions</p>
32	<p>Coll: "Because that's the entry point there's concern because that's going to be collected and stored. It depends I guess on how it's going to be collected so if it's on paper it could possibly leak out, that would be the first point when I would be concerned. I used to think electronic was riskier but I think it's paper that's riskier, it could get lost or taken or get in a place where it's not supposed to be."</p> <p>Access: "I'm concerned a little bit about that not deeply concerned but concerned in general because you know there might be some information that might be sensitive but not so much that I wouldn't use a device or tell my</p>	<p>Secondary Use: "I don't worry too much as long as it stays anonymous, it's not processed with my name on it. I feel the more data we have the better, as far as the information being there for people to look at and to crunch the numbers, I don't have a problem with that.</p> <p>Control: "Not a lot of control. I have some control. I filter out. I do my own set of controls but I don't have control once I give that information. I don't feel like I can say take that stuff away. I would like to consent, at least just to say you know we're studying this, would you be willing to let us use that data, that</p>	<p>Coll: concern if risk of leakage higher irks of paper</p> <p>Access: concern in general but filters data (IBT)</p> <p>-Sec use no concern if anonymous sees benefit of data</p> <p>-Control as filter but not after. Desire for</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>doctor. For me, I'm the filter for the data I want them to have, it's your information so you control that."</p> <p>Aware: "I don't know where it is. I know my doctor has a computer he carries with him when he talks to me and I know he puts that in the computer. After that, I'm not aware of where that is. I don't know if it's a private server he has or if he goes to a bigger database or I don't know. We should be aware. I think we're a little bit more trusting than we should be."</p>	<p>would be a courtesy and probably would help me to feel comfortable letting them use that data."</p>	<p>control of use courtesy &amp; comfort</p> <p>-Aware limited should be aware too trusting</p>
33	<p>Overall concern: "It would be ideal if it actually could remain private, as it should, which is one reason I try to have minimal participation in the "grid", so to speak. For instance, I don't have a computer at home, I don't have my Android phone hooked up to the internet or wireless, etc. I rarely see the doctor, so I'm good there. But still, you hear of old records being expunged by tossing them in the dumpster! They should be shredded obviously but that happens and it's quite scary. So I do what I can to limit by risk but you can never eliminate the risk. "</p> <p>Collection: "I don't see how it can be completely eliminated, but sure, it's unnerving. As I said I do what I can I don't give it to the tech guys and I'm not at the doctor's office too often but still there is some level of discomfort with it all"</p> <p>Secondary use: "Of course, and I do what I can to keep things private. But as I said there's always some risk and some sharing going on that I might not agree with. "</p>	<p>Access: "It only takes a few "talented" hackers, as we have seen at various retail outlets to create havoc. With health information, the same would quite possibly happen too. I do think as some sharing I don't believe I've consented to happens and I can't do anything about it."</p> <p>Control: "Probably not, at least not to the extent to provide complete peace of mind. Of course, it is important to be careful with that data. But, I have heard of identity fraud being conducted by the receptionist in the doctor's office. I don't think receptionists should have access to all my information but they probably do. I just don't see why; they don't require this access to do their job."</p> <p>Awareness: "I'm not really aware what levels of security being used at any particular institution. I think having to worry about that all seems pretty overwhelming but if they want to use a patient's information a good effort should be made to explain why they want to use it, how it will be used and what the potential risks are. That should be required.</p>	<p>Broad concern and desire for privacy</p> <p>Coll: doesn't disclose to technology but some concern with dr.</p> <p>Sec Use; Risk of sharing data without permission -concern this does occur</p> <p>Access: concern for hackers. Some health workers don't need access</p> <p>Control: not enough to ease concern</p> <p>Awareness: not in detail of security but believes any uses should have to clearly explained and consent</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
34	<p>Collection: It causes a little more concern because they enter everything into electronical medical records now and I don't know why it's not like paper is more secure but the likelihood of someone walking away with a file at the end of a file or stealing a file is a lot less likely than someone stealing a laptop or an iPad from the doctor's office. If a technology company required me to add a lot of information to join, I wouldn't. I mean if certain people want to share that information and they make it an option that would be fine but anything that's going to be invasive for me to participate I'm going to be cautious."</p> <p>Sec Use: "No because you sign HIPAA and they have a very strict framework for what they can and can't do. My doctor's office has participated in research but I've had personal relationships with them so they've talked about the studies. I have a scar from surgery and they were participating in a study with cream to reduce the scar and it was like if you want to use it we can give it to you but we're going to share that information with the study, they explained it well and I don't have any concerns that they're going to use it for something other."</p> <p>Aware: "That's my expectation and its back to that face to face conversation and being able to ask the questions that you want to ask, feeling comfortable with the person versus having no relationship with some online internet and having no clue what their business model is and what other companies are pursing them to buy their data. I also think that during that interaction with the organisation that especially if its health related that they should have some obligation to be open and honest and transparent with what they're going to do with that information. The problem is that people don't understand. They use</p>	<p>Access: "It would be a concern, the possibility of my employer seeing it. I understand they're subsidizing a portion of my insurance but that is a benefit they are providing and I don't think that means they get to know personal information about me. I would be concerned if they did because I would worry about being discriminated for cost reasons. So something I've reading a lot of, so the cost of healthcare is rising, now they're questioning at what level can we fund the costs of our employees' healthcare and so it is a little concerning will these organisations want to know the cost of individuals and will they make employment decisions based on those healthcare costs. Like women are costlier because we could have children. I mean I've seen it and I've experienced it, and it's been shocking because it's been other women saying well I don't want to hire her because you know she's pregnant or she's likely to be pregnant."</p>	<p>-Coll risk of theft – wouldn't disclose to technology  -SU: protected by HIPAA, positive exp. of research  -Desire for FTF to ask Qs, no relationship with tech – fear of sec use  -Concern of access and impact on employment experienced it as a woman  -Need for transparency</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	legalese and terminology that you don't understand and so you skim"		
35	<p>Secondary Use: 'Yes, when I quit smoking, I about went insane so I went to my doctor we mentioned maybe a course of weldrotin and that might be very iffy in the Coastguard's eyes, as far as the medication I've have to report it to him so I took like one pill I couldn't stand it, but in other things let's say I go to a doctor and I might be experiencing say short term depression, and I own a tonne of guns and then you know you're worried that he might report you to authorities because you might be a risk, it goes on and on. I am worried about where that stuff goes.</p> <p>Collection: "If I went for a sore throat you don't need to know a lot of stuff.</p> <p>Errors: I had a family physician he came in with the laptop and he's 55 years old and it got in the way because he had his nose stuff in a laptop trying to check boxes instead of talking to me. That's probably just a generational thing if he was younger he probably would have been flying. So there is a learning curve with technology so. &amp; fear of errors for work</p>	<p>Awareness: You see them breaking in to Walmart, Target, it seems they can gain access to any server at will, so what is my doctor doing, I have no clue. It could all be better explained.</p> <p>Control: Current control: "that's what HIPAA was all about about it is in theory. In order for the union to gain access to my information I did have to sign a consent form." Would want to limit access: On a need to know basis. Yeah no third parties, just the doctors I go see and even if I go in with a cut finger that needs stitches they don't need to know my whole healthcare background."</p> <p>Technologies: "With the health apps, someone else could be using all that. They have all the user information, but that's going to be a future concern also, I think we're on the cusp of that, it's becoming popular with Fitbit and would you wear it if the company wanted you to, and that is a huge red flag when companies start sponsoring things, like I'm a little heavy. My health is none of the company's business there's only certain questions they can ask of me but for other industries I don't see where that buffer is there, so if the company can make you wear a FitBit well that's just a, it's a horrible thing.</p>	<p>Sec Use: fear of anti-depressants due to work. Fear of sharing data</p> <p>Coll: must be relevant</p> <p>Errors: Fear for work</p> <p>Awareness: not currently &amp; concerned</p> <p>Control: some control over access. Desire to limit access to necessary parties and only relevant data</p> <p>Technology: would be concerned re secondary use and link with companies</p> <p>His health is personal to him</p>
36	<p>Overall: "I am not overly concerned but I don't feel my health information is anyone business so I wouldn't want it to be shared and I wouldn't just disclose it to random companies. It's private but at the moment I'm not extremely concerned I trust my healthcare provider."</p>	<p>Sec Use: "Yes, this could happen quite easily it could be passed on to drug companies and they might try sell drugs to me or to research on health. If that happened, I would not be happy about that. I hope it doesn't happen but it would not be good if it did.</p>	<p>-Desire for privacy not concerned as trust</p> <p>-Coll: security need to protect data</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>Coll: "Not as long as they have security protocol. The information is important so they can treat me and but security is important it's their duty to protect my information"</p> <p>Access: "This can happen with a lot of things so I am not overly concerned as long as the providers do their best to avoid it. If I thought, they weren't doing their best I would be more concerned but I have trust in my provider."</p>	<p>Con: "I have a degree of control. I can ask questions and request a copy of my notes. My doctor is quite open. I would like to have it more accessible online. That would be very useful if I could access it"</p> <p>Aware: "I am not aware but it is important. If I felt more knowledgeable of how my data is protected it would be a great comfort. Also if they were using my information, I most definitely should be told about that and be able to decide whether I agree or not."</p>	<p>-Access is broad concern – trust and effort to protect</p> <p>-Sec use: sees potential hopes it does not happen</p> <p>-Some control desire for access</p> <p>-Desire to be aware could reduce concern</p>
37	<p>Control: "I don't think we do in any sense of the word. Because when you install something they give you this big long EULA and then you just scroll and hit send, or scroll, checkmark, and hit send. I just don't see it happening. Once you consent it's lost to the wind so no."</p> <p>Sec Use: "For marketing. Of course they do. I think my mom was proof of that. If it isn't the healthcare companies or the tech companies, there's always somebody that's harvesting our data and there's always going to be that concern. I always feel like once you upload something to the internet it's there forever so there needs to be more awareness with the users on what they give away. And I believe every company, whether it's for good or for bad, there are people going to be using that data."</p>	<p>Aware: "They should in layman's terms. They've got legions of lawyers, they know what they're doing and what they're obligated to do, but it isn't clear to us, we don't have that luxury. So I'm sure they probably release all relevant data in these long winded privacy policies and I don't understand the legalese so layman's terms are important but I don't think that's going to happen anytime soon."</p> <p>Coll: "I have less experience with the health companies but in terms of tech companies they haven't collected a lot of important stuff but I think technology companies have more monetary incentives. Health companies they get a lot of money from sick people so I don't know if they're going to use that data."</p>	<p>-No control once disclose data</p> <p>-Sec use happens always going to happen once disclose need more awareness</p> <p>Aware: benefit for them of legal terms need to be able to understand but doesn't see it happening</p> <p>Coll: tech profit aims Little health experience</p>
38	<p>Coll: "no it wouldn't because they need to have my records and maintain my data. It's the general procedure followed everywhere so I'm totally fine with it. I'm really not used to using these apps and I'm really not sure how secure these apps would be, where would they store our information so I would be a bit concerned, I mean if it asked for more personal information I would be really concerned about giving, we trust people more than apps."</p>	<p>Sec Use: "They might use it if it is a special case they might use it. It is good to use it in one way because that misconception people are facing with how they are feeling they wouldn't have. So it has both pros and cons. It is good to create awareness. With Technology, I am not sure how far it will extend."</p> <p>Aware: "That's a concern. When I give information to the doctor I assume that my information will be"</p>	<p>-Coll not concern as norm &amp; needed in health. Concern with tech as no trust</p> <p>-expects only dr. and necessary health prof</p> <p>-Tries not to disclose to tech</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>Access: “nah, when I give my information to my doctor I expect only the doctor to know it and to keep it confidential and he may share it with other doctors or something to cure it. That would be the best that is just one to one, rather than one to many. I mean a technology; I am really not sure how far it will progress. It really matters to me to share any personal information with the doctor not the technology.”</p> <p>Control: “ya because I trust my doctor I think my health information is in control.”</p>	<p>protected so I think that it’s doctor’s responsibility to take care of the information. I trust him and give him the information so I can’t check whether his computer is working correctly and whether it is getting hacked or not so I think it’s doctor’s responsibility and if anything goes wrong he should be answerable to me because I am trusting him and giving him my information.”</p>	<p>-Good to use data to improve awareness</p> <p>-Control in trust less with tech</p> <p>-Not aware so dr. responsibility to maintain privacy external HLOC</p>
39	<p>Coll: “Not the fact that they’re taking the history but the technological storage of it causes some concern. If a technology company asked for that data, it wouldn’t cause concern but I wouldn’t give it to them.”</p> <p>Sec Use: “I think it may be being used for marketing because I just that even if I haven’t done a search on something online I’ll start getting lots of literature, pop-ups, ads on my computer on this health condition. It irritates me it really does. It’s none of their business.</p> <p>Access: “I haven’t really thought about it but it is a concern, not a super big concern but it could be. I have a condition that could be considered a risk, so is that going to limit my ability to get a different job down the line because it’s a pre-existing condition. If I thought other people and parties could access it, it would be a big concern because it could have a negative impact on my life. I wouldn’t give them (technology companies) any information that could affect me if it got out so. It would be more possible that it could be viewed or shared with other parties by technology companies so I limit what I give them now and in the future.”</p>	<p>Aware: “Yeah fairly. I know how my doctor stores my information. I know how it’s used because I’m familiar with HIPAA so I know what they can and cannot do. The information I give to FitBit isn’t much but I feel fairly comfortable with giving that. It’s important because the data does belong to you. So you should know what’s happening with it and that it is being protected.”</p> <p>Control: “We do on paper but I don’t think in reality we do we should. I think we have the right to give or refuse consent for our information to be used in certain ways with studies. But that could be dangerous because some patients may not have the ability to determine what a valid use of their information is and might not give permission for it to be shared with their caregivers. But broadly speaking we should have that control to say yes or no for how our information can be used.</p>	<p>-Storage a concern wouldn’t disclose ‘health data’ to tech</p> <p>-Sec use concern for marketing</p> <p>-Access concern but not huge could influence her life</p> <p>-Greater concern if tech limits disclosure (IBT)</p> <p>-More aware than others with HIPAA</p> <p>-Control on paper but not in reality should have more control over data access and uses</p> <p>-Awareness is vital as health data is personal</p>



Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
40	<p>Coll: "They need the information and that's how they store and as long as they are you know staying in my doctor's office and they're not sending it out I'm okay with that. Why does a technology company need that information? I wouldn't give it to them."</p> <p>Sec Use: "Anytime you give anyone information you're taking a risk that they could do something other than what it's intended for. So yes that I am aware that it might happen in the health context. I hope it doesn't. I don't spend much time worrying about it."</p> <p>Access: "I think insurance companies DO see it because they're are paying. I do worry about it, it's not something that I've worried a lot about, maybe that's just being naïve and thinking oh what are they going to do, why are they going to care about me. And there may be situations if I knew they wanted to release information I may be willing to sign consent to release non-identifying information."</p>	<p>Control: "Again, it's not something I've been concerned about and I feel most organisations, doctors, professionals have good ethics and they would say something to you before they did that. I trust in that."</p> <p>Aware: "I think they could do a better job of informing us, there's been so many breaches of data systems like target or big companies. So that's why certain companies like a Finance company where I'll get a thing in the mail that says this is what we have to do to protect your privacy kind of thing periodically like once a year."</p>	<p>-Coll dr. need data &amp; store to help in future</p> <p>Tech no need- no disclosure</p> <p>-Sec use a broad awareness it could occur but not concern</p> <p>-Access worry to a degree importance of consent and anonymity</p> <p>-Control trust in ethics of company</p> <p>-Could do more to make patients aware</p>
41	<p>Collection: "I'm biased, if it's my primary care physician it doesn't cause concern but if it's my dentist or my eye doctor when they ask me questions like have you ever experienced this that bugs me because I came to you for this specific health issue not any other issues but if I go to my primary care doctor then I wouldn't mind him asking about other issues like my teeth. I maybe have a different relationship with him. There's that confidentiality there too. And he provides my overall care so the questions on other issues are relevant to him." (Technology company)"</p> <p>I would feel invaded if they requested it. I personally wouldn't give it to them and if they were like well then you can't use our product if we don't have your information well then I wouldn't use it because to me, my healthcare provider I expect them to protect me because they go through all this training and they take an oath.</p>	<p>Access: "I mean yes but unfortunately with the 21<sup>st</sup> century that's just how it is. Technology is a great thing but so many things can threaten it once your information is stored somewhere and it's something in the back of mind, I know it's possible for someone to steal my medical data from my medical record. And like if my doctor was starting this new database would you sign this release form I would personally sign up with him because again I still hold him to this high standard but in my mind that's still there"</p> <p>Secondary Use: But they also use that information for marketing. I wouldn't mind if it was for research once it was anonymous and will my health data help prevent heart disease in the future and if it will then so be it.</p>	<p>-Collection depends on health prof. no concern with dr. trust, relevance &amp; confidential</p> <p>-Tech: wouldn't disclose due to profit aims</p> <p>-Access a concern always today but trust dr. so would sign up</p> <p>-Sec use: concern re marketing but benefits of research</p> <p>-Not aware desire for awareness with dr.</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>And with technology companies I know Jawbone is pro-health but that's just marketing and at the end of the day they're still a business and the business wants my information to sell my something else, I'm just a number to them."</p> <p>Control: "I would like to be able to give consent for my doctor to use my information in a certain way and to control who can access it. I would like to be able to access my records online too myself. But no now I don't have that control with my doctor or Jawbone."</p>	<p>Aware: "I'm not aware of how either uses my data. I hope my doctor would keep it confidential and store it somewhere. But Jawbone I know at the back of my mind they're probably using my data to come up with new marketing skills, or new products to sell. But I would definitely like to know if my doctor is doing something n, what is he doing, what is he doing to keep it private, what happens with it."</p>	<p>assumes profitable uses by Jawbone</p> <ul style="list-style-type: none"> <li>-Desire to control access and uses</li> <li>-Low current control</li> </ul>
42	<p>Collection: "I mean you're in the office with the doctor it's just going to one place. Sometimes they send out the people to take your blood and they're independent contractors and that's when I'm less willing."</p> <p>(Technology companies)" I would want to know what's the purpose for this information you want to collect. Like if they're looking for health history to alter how you burn calories I could kind of see that but if you want to know about broken bones or imbalances well you don't really need it so I wouldn't give it in that case."</p> <p>Access: "I've never thought about it too much. I feel in the doctor's office they have quite good storage security so I've never had a problem with it and I've never known anyone who had a problem with it directly. So I guess I've had no need to worry about it to date. " With bigger companies I would assume they're storing it securely and I wouldn't worry about it too much. That might be wrong but it's where I tend to. With smaller companies I would be more thoughtful about it."</p>	<p>Secondary Use: "Not usually with health information I give to the doctor. When submitting information to the likes of FitBit I always look for the boxes that say opt me out."</p> <p>Control: I think so for the most part. I don't have a really extensive history so there's not a lot out there but I feel like I do know the offices I've been to; I know the labs I've been to. (Control is important) "... because it's about <i>you</i> and you want to know where it's going and I think most people don't have problems submitting their reports if its anonymous as long as they know."</p> <p>Awareness: "It's important. Like it's not something that keeps me awake at night at the moment but I think it's something that definitely should be looked at. FitBit could be better about telling us how they use our data and even if they were to say hey guys we want to send out some of our users' foot tracking data even just a general group from this area here's how much you have walked like that would be cool but I would like to be told."</p>	<ul style="list-style-type: none"> <li>-Importance of relevance (IBT) – wouldn't disclose</li> <li>-Access in drs. good security no worry – no negative exp.</li> <li>-No concern with technology companies re access security but smaller companies</li> <li>-Sec Use: no concern with dr. -opt out for tech</li> <li>-Awareness important but not high concern currently – open to sec use with consent in some situations</li> </ul>
43	<p>"I would want my doctor to do their due diligence, well I don't really care I don't see how it could be used against</p>	<p>Awareness: I imagine they send it to the CDC and that doesn't bother me I think that's for the public</p>	<ul style="list-style-type: none"> <li>-No concern as no negative outcome</li> </ul>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>me but if I did have a more controversial record I would think my doctor needs to know it and I would want my doctor to do due diligence to be as secure with my information as possible that they're not just so loose that anyone could just hack in there and spread it out to everybody I wouldn't want that. With Apple and all those guys, we still haven't found out what they're going to do. They want us to be beholden to them as possible, I can't answer that question right now because I haven't seen enough of where they're going with this information that they have, they have more and more power so they would have to show me somehow that their interest really is for the greater good."</p> <p>Access: "Maybe if it was something of more consequences. But who's going to look for that. I don't have any of those problems. I'm not rich and I don't have AIDs, luckily I don't matter."</p>	<p>good to. I think it's good to know these people all used it, these are their statistics, this is how well it worked, so they can see if things are starting to go bad or better or I wouldn't be against that, as long as they didn't want the information this person, so they could spam me or interact with me personally but if it's anonymous and if it's helping a greater purpose that's fine if my doctor was doing that but I really don't know."</p> <p>Control: "To a certain extent, luckily I don't have a family like that but if there is some family member that wants to get all in your business about your diseases or you should be able to say no, this is who needs it and this is who doesn't. I'm not a control freak but I would like some say in where it's going."</p>	<p>-If had illnesses would want her dr. to protect</p> <p>-questions why tech companies want this data</p> <p>Access not concerned yet if had issues or was famous</p> <p>-Unaware of uses would be okay with sharing for research if anonymous &amp; no contact (marketing)</p> <p>Control desire to control access to a degree</p>
44	<p>Secondary Use: "I worry but in the grand scheme of things I think it's a better. I got myself tested using 23andMe. I know they are using all the information they have but it's better in 30 years, based on my genes and other symptoms they may be able to cure me. Or they may be able to select demographics accordingly and say okay if you are living in the Arizona area, you have a risk of A. So, if it's used for research purposes, I've got no problems but if it's used for other purposes I do, but of course it is."</p> <p>Awareness: "I know my doctors are not using it, my doctors are not, the laboratories are not, they are not mostly so, I have the FitBit, I have a blood pressure monitor that I use. My 23andMe details are linked into my Healthvault so I will always have that. I did go</p>	<p>Highlights importance of controlling access to records and Healthvault.</p> <p>View consent before secondary use.</p> <p>Access: "I haven't thought too much. But my wife's friend is a nurse and I don't go to that hospital for that reasons."</p> <p>Sec Use: "For research purposes, yes anonymised or generalised into what age group I am in, so providing specific age benefits but for my personal care I don't think that would benefit, it would rather be a hindrance."</p>	<p>-Assumes technology companies do use for other purposes. Sees the power of health data &amp; is okay with use for research but not for other purposes</p> <p>Awareness: health prof do not use. He keeps his own record.</p> <p>Checked privacy policy beforehand</p> <p>Sec use: willing for research anonymised</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	through the privacy policy and I was able to talk to some of the folks at Healthvault and ensure it is okay.”		would benefit his health
45	<p>Collection: “Yeah it’s a cause for concern because they don’t know who I am, the general idea of who I am, that’s a concern with putting the information into technologies.”</p> <p>Secondary Use: “I don’t really think about it, the only thing I’ve considered is research. I never really thought about it being used for any commercial purposes. So that would be a concern for sure, research wise, as long as it’s anonymised it can help I’m fine being a statistic but if it’s individual no unless I give consent.”</p> <p>Control: “I don’t think we have 100% percent control. I get naïve, I assume everybody would use it right but when you start thinking about the fact it’s online, who can view it how can they view it, I think at that point we should be able to have some limitations on it especially when it’s something that’s specific, if I did go to see my health professional for a mental, I’m going there to seek professional help, I don’t want that to go somewhere else. I think it could be the form of consent for who can see my information and how it can and cannot be used.”</p>	<p>Access: “It does concern me, everything that’s electronic has the potential to be, not to say that paper can’t be but I think it’s harder for somebody on the outside to get that information. I don’t think, but I don’t think on a regular basis our employers do reach out for that information but it starts to get a little concerning when it’s electronic.”</p> <p>Awareness: not fully aware, some onus on use see HLOC</p>	<p>Coll: concern as not personal</p> <p>Sec Use: didn’t consider commercial okay with anonymous research. Desire for consent</p> <p>-Access concerned of possibilities with electronic data</p> <p>-control don’t have full control. Due to potential for loss and sensitivity should be control in form of consent for uses and access</p>
46	<p>Coll: “I wouldn’t be concerned with the doctor but I would be if it was a technology. The doctor is face to face, I know who he is and where he is but with technology I don’t know who you are or why you want my information so I would not give it.”</p> <p>Access: “I think the nurse might need to access my information so they can help the doctor, that would not concern me but anybody else I would not be okay. I would not want other people to access my information because they are not health professionals and I don’t</p>	<p>Sec Use: “Yeah that would be concern for me as well because my information is for me. I think it would happen with my health information. I am afraid people will sell my information.</p> <p>Aware: “I don’t know what they do at all. I would like to know but I don’t know now and it make me think the worst.”</p> <p>Control: “I would like that control but I don’t know that it is possible. I don’t have any control now of what they do with my information.”</p>	<p>-Coll no concern with dr. but concern with tech doesn’t disclose</p> <p>-Access just health prof doesn’t trust others to care</p> <p>-Fear of selling data</p> <p>-Desire to be aware lack of awareness causes concern</p> <p>-Desire for control</p>

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	trust them to care for me and I would worry they would share my information.”		
47	<p>Coll: “No. Most of the stuff in my medical history I will be open telling health professionals about. If it’s stuff I volunteer to give technologies, it wouldn’t be a concern because I can choose not to give some stuff and there is some stuff I wouldn’t give them but it’s going through me and I’m deciding but you’re giving them that information and you have to realise you’re giving it away essentially.”</p> <p>Sec Use: “I don’t personally fear it but I really hope they don’t use it for anything else, maybe if it had personally affected someone I know, then I might be more worried but as of now I just hope they don’t do it. I’m not a fan of companies selling information. I want an account with you, but when you give your information your awareness they might share information with someone. At the same time, I’m not giving them anything I deem too personal or sensitive I think it happens all the time with ads.”</p> <p>Control: “I’ve been going through a process of trying to get all of my medical records from a car accident and it’s been so difficult and I wish I had control over my health records. I’m the person making it, it’s about me.</p> <p>Aware: “I would hope with the doctor it would stay where it is. I know they send stats to the government for certain conditions. I would hope they wouldn’t use it or I don’t see the need to use it for anything else. With FitBit, I would imagine they do use it, what for though I don’t know. It would be nice if they were transparent.”</p>	<p>Access: “Insurance companies would definitely be on the list of people I do not want to see my health stuff. I don’t want anyone who is not a medical professional viewing it, because I don’t think someone from a law background can interpret my medical record and why would they want to see it anyway, I don’t think it would be to treat me! Another thing is in the event of a car accident. I don’t want an auto insurance company to be able to see that, there’s somethings those insurance companies don’t need to know if it’s not pertinent to what they’re offering. I think right now they try get it through doctors but I think it will shift towards technology companies when they get more information but if you’re trusting a website that’s not a person, you haven’t built a relationship with them if you’re trusting them with your health information you’re taking that risk. I don’t understand why you would disclose certain things to Fitbit I don’t know the necessity, to disclose health information to companies that offer technology based products.</p>	<p>-Coll health no concern – tech okay as controls disclosure wouldn’t give all data (IBT) lose control with tech once disclose</p> <p>-Sec Use: not concerned hopes doesn’t use-no personal stories -tech limit info because they probably use or sell</p> <p>Disclosing is a risk</p> <p>-Access concern for insurance companies can’t interpret data</p> <p>-Wants access to data and more control</p> <p>-Assumes dr. doesn’t use</p> <p>-Desire for transparency</p>
48	<p><i>health information from you from your health history and they store it. Is that a concern?</i></p> <p>No because from my point of view that means they’re being thorough and those are important things that they need to know in order to like treat you properly. So like</p>		

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>that's not why it's really a concern and also that kind of goes to records. It's important to have that information because it's hard to remember that information a second time. So I would rather only be asked for some things once but other things like symptoms I understand them needing to ask again and check on that.</p> <p><i>And then on the other side if it was an app or a technology like Healthvault asking for all that health information, would that be a concern?</i></p> <p>Umm... yeah that's a little stranger. Again I'm more sceptical of that and I trust it less so I guess that's why it would be a little more concerning to me.</p> <p><i>And then if you give health information to your doctor for one purpose, normally to treat you, do you worry about what else it could be used for?</i></p> <p>Umm...I mean I don't really think about that and I guess I should but I don't. I wouldn't really be as worried about people in the doctor's office like having physical access to it but I would be more concerned about their system not being secure and having someone access it from the outside. That would be more of a concern to me I guess that seems more likely to have an impact than like a drastic fallout from some other one random person seeing my health information.</p> <p><i>And then if you gave your information to technology companies, would you be worried about that kind of access?</i></p> <p>Yeah I mean like that's way more concerning because if like, they're like different like with doctors and healthcare systems they know they have all this information which they know they have to keep safe whereas for an app it's not as important. I donna I feel like the fallout for say like Kaiser, that's like my healthcare provider network, say if</p>		

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p>Kaiser got hacked and all like the information from their patients got exposed, that would hit them harder I feel like it would almost hurt their legitimacy more than like an app almost I guess maybe because they have further to fall.</p> <p><i>Okay and then do you ever worry about who might access the health information you give to health professionals or technology companies?</i></p> <p>I think on the doctor side it's a lot less of a concern based on the fact they know they've a lot of restrictions on them protecting health information and it's a really big deal on that side and I feel like it's more concerning on the technology side because for them it's like I donno they could just write something in the terms and conditions that someone could agree to but not realise and like I feel like they would get away with that it's just not going to damage them as much even if it comes to light.</p> <p><i>Are you concerned about errors in your health data?</i></p> <p>Not really. I feel like you have to trust in your doctor to an extent and that he is checking with you for anything unclear.</p> <p><i>Do you feel like you're aware of how your health information is used?</i></p> <p>I feel like I think I'm kind of aware of how a doctor would use it because I know about HIPAA so assuming like they are following that then I do pretty much know like how they're allowed to use it and that compared to like an app where I have way less of an idea of they are allowed to do or would do or in technology in general what that type of information is used for.</p> <p><i>And do you think awareness is important for you in terms of health information?</i></p> <p>Yah. Yah definitely.</p>		

Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
	<p><i>Okay and lastly on that do you feel in control of your health data?</i></p> <p>Ummu...I guess I feel like I have decent control over it and I also would like to have control over it but like I also understand like if there's a point to where my control no longer extends, then there's probably a reason for that. Like with EMTs, you have to consent from someone to take them into your ambulance otherwise its kidnapping but like if they're altered then it's considered implied consent and that's for their own safety and their own benefit. So I kind of understand with health information there's a point where I might not understand why you need it but you need it but like implied consent I would only ever give to a health provider versus a technology yano.</p>		
49	<p>Coll: "No that's not an issue. It should be kept private among the healthcare providers but they should have access, it's really important for healthcare providers to have a holistic picture of your entire health experience. On the technology side, I want it to be like Facebook privacy where I can say you can have access to this information but not this information. Because there are certain things that people should be granted privacy on, because the technology company isn't treating you they are providing storage."</p> <p>Control: "There seems to be a fair amount of control. It is important to have control especially if it's a for-profit corporation that is not the one actually providing the healthcare to you. But even with the healthcare provider if there's something you don't want them to know, I think that's short sighted on behalf of the patient but if you want you should be allowed to control your privacy."</p>	<p>Sec Use: "Yeah I definitely did think twice before I did 23andMe because if I ever want a high profile career then them having access to my genetic records is something which could be a vulnerability. I'm not incredibly terrified about it at the moment. I wasn't concerned enough about it not to do 23andMe but it is something I definitely consider."</p> <p>Access: "I don't worry too much at the moment because I don't think I have too much data. But broadly speaking I think people should worry more because healthcare providers have to take a lot of measures to ensure that only people who really need the data can access the data because it should be only accessed to ensure you get the best medical attention."</p> <p>Aware: "I'm not really aware with my doctor because she just works at a clinic. I think people should be entirely educated about what their rights</p>	<p>-No should be private among health prof but need access</p> <p>-Tech want control over access</p> <p>-Need to have control</p> <p>-Did consider future risk but concern wasn't enough to stop usage (Privacy Calculus)</p> <p>-Access: not concerned at present but should only be necessary access</p> <p>-Should be educated on rights and benefits</p>



Interview Participant	Dominant Concerns	Additional Dimensions	Extracted Meaning
		are, what they should be looking out for and what the benefits of sharing their health data are.”	
50	<p>Coll: “No because that’s just numbers and if it’s stored from a medical standpoint that can change the way they make decisions and diagnosis so I’ll give them as much as they need. For the FitBit I might be a little more hesitant if they’re asking for certain things. I know FitBit they’re not sophisticated enough to need some of these bits of histories or sensitive information but if it’s height and weight and heart rate it doesn’t bother me at all.”</p> <p>Sec Use: “The further use without your knowledge it could be ignorance is bliss where if they are using it and I don’t know, there’s probably not a lot I can do about it but if they’re going to be using it I would want to know about it but as whole I’m not really concerned, as I don’t have a lot of health information that would be out there.”</p> <p>Aware: “Yeah if it’s sitting on a computer I don’t need to know but if someone is going to use or you haven’t come to our office in 5 years we’re going to delete it, basically a substantial event they need to use it or access it for, I want to know.”</p>	<p>Access: “Superficially, it doesn’t keep me up at night, I would like to think that it would be accessed for specific benefit purposes and then it’s of archived and left alone, I would like to think that.”</p> <p>Control: “I don’t think I have any control, because once I give the information it’s there, that’s not like I can say I want you to delete my data. I do think controlling your data is important, if they want to use if they’re going to be like hey we’d like to include this as part of a research project they need to get my permission first, that’s really important, but once they have my data I don’t have control, if anybody wants to access that I have no way of knowing.”</p>	<p>-Coll: relevance of info for health, non-sensitive for tech (IBT)</p> <p>-SU: Not a lot of data but desire for consent</p> <p>Access: Assumes not extra access</p> <p>Control: none but desire for permission</p> <p>Aware: not currently but desire for awareness for uses or deletion</p>

## APPENDIX R: INTERVIEW ANALYSIS PERCEIVED BENEFITS

Interview Participant	EHRs	Mobile health	
1	"I think it would be very beneficial, because your information is there. If someone is going there quite often that the doctor is able to look up and say come here how are your ears nowadays and how is this, isn't it nice than for no other reason that they have it on front of them."	-	-Benefit access to past data improve service
2	Access to data	Challenge and prompts you	-Jawbone can motivate
3	"I think they can be very useful making information available but it would influence my decision."	"I use a FitBit. It's good my only problem is it needs to be charged so much. The only thing I had to enter was my height and weight and age and tell it what arm I wear it on and which arm is my dominant arm. I actually sometimes go walking just to try hit my goal. I don't enter all the diet it's just a lot of hassle and a lot of monitoring."	-EHR: benefit of access would influence adoption -Wearable more active to meet goals but limits use due to effort
4	"There are lots of benefits to them being able to access my information to know I'm allergic to penicillin would mean the hospital wouldn't give me it, I think it would reduce the time I spent repeating information and maybe the length of stay at a hospital. I think the benefits If I knew them all would make me want to but I wouldn't like to be in the dark about other ways the information is used."	"I've used weight management, diet, exercise, pregnancy and menstrual cycle ones before and I'd definitely use them again."	-Access ensure no errors -Benefits would influence her but would want transparency re sec use -Has used a number of apps would use again
5	"How could I say no to the right people being able to access my data. The benefits would have an influence. When they introduce it all the benefits will be pushed towards you and the risks or uses of the information hidden. I'd still think about the	"I had one called my fitness pal. It was for tracking calories and how much exercise I was doing and I deleted it because it was making me feel bad."	-EHRs access- benefits would influence opt in decision but privacy is important -privacy calculus -Apps deleted due to guilt

Interview Participant	EHRs	Mobile health	
	privacy but I can't say the benefits wouldn't have an impact."		
6	N/A	"They would be they'd have to be fairly large benefits to convince me. Privacy is more important mostly because I'm not too concerned with my health and I'm more cautious of apps and technology in general at the minute so that extends to my health I guess."	-Privacy more important than benefits of technology due to lack of concern with health and mistrust in technology
7	"Efficiency is big. I don't want to have to tell things to my doctor and go to the hospital and answer all the same questions. And the case I referred to earlier if I'm unconscious and can't answer for myself I want them to be able to find out pertinent information about me even my next of kin, just the really necessary information."	-	-EHRs: efficient, in emergency situations
8	"I think there are many benefits. I am a donor I'd want people to know that if I could help other people. I think for people with major allergies and chronic illnesses they can save lives. I think in life or death situations the benefits are more important because it could save lives but there could be fallout regarding breaches of privacy. I think in everyday life privacy is more important. I don't think you can fully outweigh privacy with the benefits because if it's very sensitive information that was breached it can really affect a person I think you have to manage it case by case."	"I think there should be some kind of controls on them for younger people like you're getting into a competition with yourself. I think they should make you want to eat more. Like on MyFitnessPal you can compete with your friends and say she burned so many calories or she lost so much and obviously if its health weight loss it can be an encouraging environment but I think there's definitely a danger of people taking it too far. "	-EHRs: access in emergency can save lives -Benefits more important in an emergency but privacy in everyday life. Hard to weigh as sensitive data -Health apps can promote healthy weight loss but risk of obsession
9	-	"Greater awareness of health and makes people healthier across the board, it would be a lot better for better understanding of conditions instead of periodic visits to a doctor. You'd be able to track over a longer period."	-mHealth: awareness and improved health -EHR: access to data

Interview Participant	EHRs	Mobile health	
10	“Doctors being able to access GP records, I think that’s a great benefit because it’s easier, it would be easier to diagnose and treat the person. For a doctor be able to contact the person that could be brilliant. At the moment, I notice the gap between GP and hospitals, because my mam her records are in one hospital and if she’s ever brought to another hospital it would take some time because there’s a lack of connection between hospitals.”	“I think monitoring your diet in general there can be (benefits), but apart from that not really.”	- mHealth: monitoring diet -EHR: access, diagnosis, communication, current lack of connectivity
11	Benefit of access for ‘right’ reasons	“I think it could be useful for young people you have them dropping dead on a playing field, an app that might say you’re beginning to enter a danger zone, an early warning if you were pushing yourself too hard, that could be very useful. “	- mHealth: health warnings -EHRs: access for benefit of patient
12	“At the moment I am asking the GP for every specialist report. I have them now in paper form so it would be a lot more accessible if you just key in something rather than rifling through papers.”	“It can raise an awareness in yourself if there’s a problem looming, or say you got a cold or something you would dismiss, it might lead you to do something quicker about your health, if you were aware of certain things.”	- mHealth: awareness and proactive towards health -EHRs: benefit of patient access over paper
13	-	-	-
14	“That’s a great idea. So that if for example, you’re playing hockey and you break something, they can get into your records. I’ve had three heart attacks, and so god forbid if I had another one on the Southside, I’d like them to be able to hack into my stuff before I died.”	“I will fill in the information one, because that benefits me or it benefits something who comes across me, if I collapse on the side of the road.”	-EHRs: desire for access in emergency -mHealth: would enter emergency data due to potential lifesaving abilities
15	“The people who need treatment can get it you know, you could prioritise things.”	Beneficial for people who need to monitor	-EHRs: could prioritise treatment -mHealth: benefit if need to track health
16	“There might be less chance of mistakes because they’d have the same information and they’d have your history if you were suffering with something a	“I think they sound very good. If you use them for the sole purpose they’re used for then it’s okay as long as you don’t get obsessed, once you don’t get	-EHRs: access to data less errors, quicker decision making

Interview Participant	EHRs	Mobile health	
	long time and it would probably speed up processes of making decisions to take more blood tests or scans instead of going from one department to another and that doctor from the other department doesn't know anything about you, and I've seen it first hand with me sister and I think it's disgraceful."	obsessed, like the diet ones that could be very dangerous, but if you just use them for the information and to remind you to keep up with your healthy eating I think they be brilliant for that."	-Currently takes too long & doctors aren't informed -mHealth great for reminding to be healthy but risk of obsession
17	-	"Yeah maybe young people or like my daughter when she was pregnant right not going to harm anybody, or doing her diet not going to harm anybody, but personal information no. About health no."	-mHealth: benefit for younger people okay when no data disclosed – no negative outcomes but no disclosure of health data
18	"There could be a lot for it, because you have people who are in accidents on the road and they're brought into hospitals and you've no idea if they're diabetic, and you wouldn't be able to tell them or anything. So it would be a good idea, having the information all in the one package."	"I could see the value if you needed to know health wise how many steps you're using. Well that's the way of the future isn't it."	-EHRs: access to data in emergency situations -mHealth: benefit if needed to be aware – assumption use will grow going forward
19	"I think it would be very quick, the doctor doesn't want everything that belongs to me since I was born to go through. It's the now, dealing with the now pain. They would have so much information, so this woman had a murmur in her heart and now she has difficulty breathing so they can add the bits together and you haven't to go through all the pains and other bits and pieces that have nothing to do with your heart, I do think specific information and maybe it could be done in a way where all the information on your heart would be there and whatever else."	"I'd say that would be good for people with clots or anything like that just to get up. With the sleep, I'd like that now, I'd like that because I'm not a good sleeper."	-EHRs: speed and access to data. But need to not inundate doctor with data -mHealth: useful to get people with conditions moving and tracking sleep
20	"I can see the benefit of sharing information especially in emergencies and possibly reducing gaps in knowledge of a patient's history."	"I thought the FitBit was okay it was interesting for a time but I don't think it gives you any big insights. I use a running app and compete with	-EHRs: access in emergencies and

Interview Participant	EHRs	Mobile health	
		my friends too but not through the app or anything just with screen shots. I find it quite good as a motivator because I'm quite a competitive person. I've also tried lots of the calorie tracking apps but I find they're far too cumbersome."	comprehensive patient files but some reservations -mHealth: FitBit interesting but no real insights. Running and competing -motivating Calorie apps too time consuming.
21	"It sounds quite sensible because I mean in emergency situations where a locum doctor turns up they might not know the gender of the patient not to mind what's wrong with them, so it would be useful just practically to have access to that information on the spot, it would be silly to think that it was sitting in a file in the local surgery and the guy accidentally gets killed because the doctor didn't know they were allergic to penicillin."	"I have no idea why you would want to do that. It just seems to be rather silly, that they're throwing loads of data on to the internet and they're not entirely sure where it's going to go. I'm not entirely keen on doing that which is getting to the hub of the point I suppose. No I've never used a health app and I've no particular desire to."	-EHRs: sensible to have access in emergencies -mHealth: sees no use of mHealth, doesn't agree with disclosing health data – no idea where it goes
22	"Ease of access probably both for medical professionals and patients, if they want their files it's instantaneous. Uniting all healthcare professionals, it's easier to see what the doctor wrote, it could help with diagnosis. I think it could help with education, teaching students about certain conditions and being able to read all their notes. It would probably save money in the long run like paper based systems and mistakes would be less likely to happen. Taking a little bit of the stress out of the patient's hands and giving it to the healthcare professionals because it's up to them then to look at your file. It protects both the patient and the healthcare professional because everything is documented."	-	-EHRs: access for both, diagnosis, education, costs, reduce burden to remember details, documentation protects everyone

Interview Participant	EHRs	Mobile health	
23	<p>“Oh yeah, definitely. People change GPs quite a bit I never do it but people do, and the transfer of information is never accurate I know from dealing with employees whereas one person with one record makes sense that you have an identifier for me. There are people who play the system, it would eliminate that but it would also eliminate the risk of error.”</p>	<p>“We’ve two sons who are fitness fanatics and they would go that far. I wouldn’t go so far as wearing something although I do see the value of it. It’s not hugely important to me whether I do 5,000 steps or 10,000 steps I’d like to be doing more but it’s not hugely important to me but having the data recorded would be important for younger people definitely because they’re far more aware than I was of health issues and fitness and all of that. I think it has less value for me.”</p>	<p>-EHR: transfer data, no gaming the system, eliminates errors -mHealth: sees value for younger due to health and fitness awareness but not for her as not concerned about health</p>
24	<p>“It would minimise administration in hospitals on the surface that’s a benefit but that’s thousands of jobs. Ease of access and the benefit is consistency of access is very positive, one of the thing that emerges from that is that you’re not depending on the patient to remember or faithfully recount, it would facilitate diagnosis and treatment. But it’s also more vulnerable both to abuse, and to unauthorised access, and to loss, all it takes is you know a power outage and no one has access to anything. One benefit is getting a profile of the health of the country, of a particular demographic, I’m uncomfortable with that like I said before, but I can see the benefit of it. There are benefits to everybody <b>but</b> the benefits to one are often countered by disadvantages to the other so the potential benefits to individual people, access awareness education control, is a disadvantage to corporate business.”</p>	<p>“Fun, it’s interesting to track something of which you’re not particularly aware, and the way that they’re designed is to facilitate access to information that you might not particularly know how to access under normal circumstances so I think that in theory they can be used to educate people and they can be used to allow people to take control of their own health. In practice, I suspect it’s more limiting, and it absolves public and medical bodies of responsibility in a way that I’m not comfortable with that, but I don’t think that’s necessarily an inherent risk I think it’s just the way that economics works at the moment. I think the potential benefits are quite extensive but I think the potential abuses are about co-extensive.”</p>	<p>-EHR: lots of benefits but benefit to one is often a disadvantage to another – vulnerable to misuse -mHealth: fun, tracking, education, HLOC, but puts responsibility to person, makes her uncomfortable -Possible benefits and abuses are extensive</p>
25	<p>“I can email my doctor she can get back to me; the communication benefits exist there. I can see my health records online, well they are they’re behind some sort of security protection but I can see the</p>	<p>“Yeah if you’re training for a marathon or whatever you’d want to know. As you get older you notice these things, my own parents and in laws they need to track cholesterol levels, blood</p>	<p>-Benefit of tracking for fitness or BP etc. but can be done manually</p>

Interview Participant	EHRs	Mobile health	
	details of my last visit. I suppose you could spot a trend if you were, they weigh you so you could keep track. Also if you forgot you can log in, they actually record what they said to you and the prescription.”	sugar levels things like that. So like I can see that benefit, it can be done with a pen and paper, you don’t need an app.”	-EHRs communication access to data for trends or recall
26	“They have access to what they need. Our generation lives in more of a transient environment where they are not likely to set down roots so I want my records to travel with me. I don’t want to have to spend hours on the phone to have a health professional to try get my records here.”	“It shows me that I do not move when I’m at work, and it scares me but it keeps me active to a degree. I haven’t necessarily made life changing decisions based on it but it keeps me more conscious.”	-Shows activity improves movement a bit but not life changing -Need access to data, should travel with patient
27	“It makes it easier for him with less paperwork and that’s obviously good for the environment. It allows him to track my health over time. I think for the patient it makes it quicker because the doctor can access past information so quickly and share information with relevant parties which can help to treat you quicker.”	“There’s lots of benefits but mostly awareness and monitoring over time and giving you a bit of a push I was driven before regarding my exercise I have more confidence in my ability to manage it now. If I had an illness I’d definitely use them, though I’d want to know more about how the information is used, I would like to be informed and have the ability to decide what is used and how and understand how it is protected for peace of mind.”	-Awareness and monitoring exercise -If sick would be beneficial but would want control, awareness of data use -EHRs: easier, access and sharing data – better care
28	“They’re easier for the doctors because all the information gets put in right away and they can access it at any point. If you went to your doctor frequently and had a specific health problem, it would be useful to be able to see everything online and have everything in one spot, that would be really helpful too because sometimes you go to different doctors and you have a certain amount of information with one.”	“They can be really beneficial. I’ve seen a lot of people really love it. It’s gotten them moving and active and they have big competitions with one another so I think depending on the person it can be really beneficial. I just don’t like them for me but if I was really unhealthy and I needed something to motivate me to get back on track, it would be a really good option.”	-Access to data and comprehensive record -Benefit for some people to get active and compete but not for her
29	“It’s much easier to keep track of information, to find information. You could have a connection between doctors and patients. For ASU’s health	“There’s plenty of benefits because <i>awareness</i> of your health is really what motivates people to improve their health. Simply being aware of I’m	-Ease of access, communication



Interview Participant	EHRs	Mobile health	
	services there's a portal where I can check updates cos I went to visit them and they would get back to me on a test online, it saves paper too."	walking this many steps today and I'm burning so many calories doing it, if I were to walk another maybe 1,000 steps I could burn more calories."	-Awareness of health can promote changes
30	"It's always with you and it's easy to access for the hospital too they can just pull it up right there and they don't need to run to the back and get the piece of paper. Healthvault we learned about where we signed up for it and then one of the girls had went to the doctor that week and when she went home they had emailed her like a summary of the visit and we thought that was helpful and handy but kind of weird because they're sending that information via email and it could be intercepted."	"I like using them just to track. I like working out and I like seeing how well I'm doing and I was able to kind of compete with myself so that's kind of fun. We also had Fitbit in the office for a while and it was fun to see who got the most steps and it really pushes you."	-Benefits of access of portable records -Healthvault helpful to give you summary but risky via email -Tracking and competing with self and others
31	"I think anyone who's informed is more educated. If I could see things about my health I would be more educated and I would be able to make better decisions. You know if I was blissful, which is what I am now, I could just take my pills but if I was really educated I could make more informed decisions."	"If people are not technologically savvy you could teach them like my mom is 85 and she has an iPad and if there was something that would say take your pill I could teach her, that would be awesome you know she could integrate something into her iPad. That would be helpful to her and empowerment is huge. She feels very un-empowered by her health situation."	-Access to her EHR could enable informed decisions -Could teach older people and empower them
32	"Better diagnosis, if he sees patterns, I'm only concerned because I'm getting older, I'm concerned about diseases that I'm aware of, there's things that I don't know about, that are not common. Going back in your history we can see you have that."	"Primarily awareness for myself what I'm doing, how I'm treating my body that kind of thing, it provides an overall hey you're eating this much, you're exercising this much, so it helps. It also helps promote me to move more."	-EHR: Better diagnosis linking data -mHealth: awareness and motivation
33	"Historical information can be kept to watch trends in individual patient health, which would be useful. And being able to request electronic records from a doctor office eliminates the sometimes hefty fees being charged for copies of records. It allows the patient to have access to more data themselves."		-EHR: History and access

Interview Participant	EHRs	Mobile health	
34	“Sustainability, we’re not killing trees for paper and then storage and costs. And having that information centrally that can be accessed, I might be on a certain medication but if I’m in a car accident, the hospital would have no clue, so the ability to share that information for emergency care is the best benefit.”	“The fact I’m monitoring it, it makes it easy and fun for me to track things about my health that without it I wouldn’t have done as routinely or frequently.	-Sustainability, storage -Sharing data in emergency -Enables easy, enjoyable, regular monitoring
35	“Yes in a broad category. If we just use demographics, stripped off names and social security and everything else, I think it has HUGE potential to develop drugs and see what works and what doesn’t. But we need to, we need to strip off identifying information at least.”	“Absolutely. I could track how long I jog, heart rates, calories. My daughter lost a bunch of weight using apps. When I quit smoking I did use a little timer to show me how long I’d quit smoking, how much money I’d saved, that lasted about 3 days. I’ve got a short attention span so; I was actually doing it for me not the money or but it was novel.”	-Benefit for research but need to anonymous -Sees benefit of tracking but needs to tie into his reason for use
36	“Absolutely. They make things easier for doctors they are portable and improve the information doctors have to decide on the best course of treatment for the patient. This is beneficial for the patient if they receive faster, better healthcare. Also if patients can access their own records, that would be great for awareness.”	“It will help me to better understand how much activity I do and how well I sleep.”	-EHRs: portable and access to data for diagnosis. Benefits patient with better healthcare and access -Benefits of trackers for awareness
37	At the VA, I don’t know how updated their system is but it’s advantageous over paper records. My sister is a nurse and she even made a mistake once but she caught it, the size of medication they give to a child, that would have killed them. Software could prevent that, the downside would be the doctor and nurses could be complacent but the advantage is you have something which is not human making the decision or notifying you of a mistake and ultimately it is the future and we should be pushing it, while making sure it is safe and secure. Secure is key.”	“It’s beneficial not collecting sensitive data or data that can be misconstrued. I mean just steps, they’re beneficial. Companies are pushing the boundaries on what’s beneficial, they just released the first commercial ECG for consumer. It’s the first FDA approved device which can detect HBO fibrolation and every time they want to expand the device to include more diagnoses they have to get FDA approval.23andMe got approved for a very narrow piece of genetic diagnosis, but before they were offering broad diagnosis. That could lead to many	-Aid in decision making -Future but need to be secure -Benefit of tracking non sensitive data -Pushing boundaries with ECGs and 23andMe risks of misinterpretation, false positives

Interview Participant	EHRs	Mobile health	
		false positives and sending that out over email isn't exactly secure and if you misinterpret that."	
38	"Technology really helped us a lot and by just giving the patient's name we can get to know about all of their medical history. I used to have irregular headaches so they have correlated this with PCOD. They had correlated this that ENT and this gynaecologist so the technology helped both doctors when the information was correlated. If that was not shared, they would be treating me differently I would still be suffering the same."	"If it will create awareness among people and if we teach them how to use them and all it will be easy and they will be in control beforehand, it is better to prevent it. Its within our hands rather than going to the doctor at the end."	-Personal experience of benefit of sharing health data for diagnosis -Benefit of mobile health to track and prevent illness – Views internal HLOC
39	"I think the benefits outweigh the risks but there are risks too. The doctor it makes their lives easier with entering information, having complete information available to them. That benefits patients too in terms of the healthcare they receive."	"Yes, you're able to stay ahead of the curve and watch what's going on and watch for patterns and be able to more proactive in our healthcare. We should be more proactive."	-Benefits outweigh risks – better care (Privacy calculus) -Track and watch patterns in health – need to be proactive HLOC
40	"If he needs to share records, say you go to a doctor and you have something, it's much easier to transfer than copy a bazillion pieces of information and fax it, so they can more readily share information that <i>needs to be shared</i> . I can see my test results and <i>I</i> can see the changes, in a sense that makes me feel more in control because I can see."	"It's that individual taking control of high cholesterol, or high blood pressure or if you're overweight all of those things contribute to deteriorating health. Having those apps helps you monitor them, it's just easier to keep track and say ye I'm on target, I'm doing it yay."	-Ease to share data -Accessing her record makes her feel in control -Monitor health and track goals -HLOC proactive outlook
41	"The research it enables and accessibility to it. Say I just forgot, I can just check and I could easily go to another healthcare provider and to be able to get a second opinion and compare it would be a lot easier. I don't speak their language but I would have the information there and the facts are always the facts."		-Research and access to data empower patient
42	"A couple of times I've had to wait for records to be transferred and that can take a couple of weeks but if you had a database you could type in	"It just makes me more aware of how active I am. I know as a college student I have the potential to lapse into large periods of inactivity so if I can	-EHRs experienced lack of connectivity. Benefit of access

Interview Participant	EHRs	Mobile health	
	someone's number and pull them up. And in hospitals if people had identification and you could pull it up and see this guy had bypass surgery you can't give him this, that could be useful. I know lots of places use them but it's very fragmented."	look down and see I have walked 500 steps today on my day off I should really get outside. It's great to be able to self-check."	-Awareness of activity and encourages activity
43	"I would like to see it on a cloud so if you go into the ER in Budapest, somebody there could be like this has person this, and all that information is there in alerts so people don't have to ask an unconscious person. I wouldn't mind a cloud thing on your cell phone, so people can make decisions, that's very valuable I would want that to happen."	-	-Would like access to files or on phone -Access to data to make decisions
44	History, like I lived in Seattle and they literally had to ship in my X-ray records here, so I would like to have it with me electronically. .	"It gives you awareness for a healthier lifestyle. It is easy enough but you need like a year or two before you reap the benefits. So for example, I just got my H1CP test results, my annual blood test, I got my cholesterol levels, my blood sugar, my vitamin D, everything. I'll get them tested again a year from now, and a year after that so I'll be able to track what direction I'm moving in."	-History and travelling with -Awareness of healthy lifestyle but need time to get benefits
45	"It's easier, if I did go from a doctor to a specialist that information could be sent pretty quickly, there's no lapse, so I think there is a need for it, it's just I think there needs to be a better way to go at it and there needs to be more working around the whole electronic thing, and how things are used and how they can assist me."	"If I have a cold I don't want to go to a doctor for a cold, or because I have allergy issues so determining if it's allergies versus a cold I think that would be useful, or if I wanted to get in better shape if there is something to help me out but I get worried where they show you a range and that's where I'm like maybe I should see a doctor for."	-EHR ease of sharing data – need to work it for patient benefit -If apps could help her but when they give range of diagnoses need to see dr.
46	"Of course because my friend has cancer. The health centre were not sure so they showed his information to other doctors and in California, one very famous doctor checked the case and said it is cancer. So, it really helped him."	-	-EHRs useful as can share data – friend's experience-

Interview Participant	EHRs	Mobile health	
47	“Well your visits can be cut shorter as a patient because you don’t have to go through the whole chart thing again and it benefits doctors because they can see the information and can accurately diagnose people.”	“It’s nice being able to see how active I am every day. I am a competitive person so it’s nice to be able to compete with friends. I try to be an active person so it made me more aware and made me think why not take the stairs and make little changes throughout the day.”	-Shorter time for patient access and diagnosis for dr. -monitor activity, compete with friends, and make small changes
48	“I have shadowed a few doctors and every single person says this is the worst part of our job. They don’t like inputting and coding information but I know it makes communication between departments infinitely faster. I have my dentist and eye doctor in my network so that’s much easier they all know who I am its one system. It’s a lot faster and its better care because they all know that I’m allergic to whatever.”	“It’s easier to track what you’re doing. With my watch it makes running more efficient because I don’t have to plan out a whole route before I go, I can just see this loop is about 3 miles so it makes it easier and more efficient and less planning needs to go into it.”	-Improves communication -All health prof. have access to her data -Wearable makes running easier and more efficient
49	“I think there are multiple benefits. One of the most important ones is cost effectiveness. Others are ease of access especially with sharing of information and the third, it allows for easier corrections of errors because there’s always a risk of errors in records. So it increases the accuracy of the information.”	“It allows you to quantify your information and see patterns over time, but it also allows you see if you’re meeting your goals. It just provides a metric I guess so you can see how you’re doing, rather than how you <i>feel</i> you’re doing.”	-EHRs: cost, access, accuracy -Quantify data and track if you’re meeting goals
50	“Absolutely, because different doctors can have access and make notes which would be a little more live in terms of the updating, whereas if you’re always going through a paper chart, you might miss something important. I think digital records would be very useful and it would be easier to track access, and if there’s a summary they need to send me it would be easier to generate a summary.”	“Of course because we over estimate how physically active we are so it would be helpful, you’ve done 5,000 steps that’s half of what you’re supposed to get, if you’re not a regular exerciser that information would be helpful to set goals but there has to be a way to change behaviours because someone who is not a regular exerciser can track the steps, until there’s a way for them to step up a goal, it’s just information with no purpose.”	-EHR: Improves access file is more live, don’t miss detail Can track access -Awareness but need to be able to change behaviour otherwise data is useless

## APPENDIX S: INTERVIEW ANALYSIS: ADOPTION INTENTIONS

Interview Participant	EHRs	Mobile health	Extracted Meaning
1	Would be willing to opt in.	No. Goes to gym for workout but doesn't see need for apps	-EHRs would opt in -Apps -no – irrelevant to her
2	Would like to see it come in.	“Oh yes, I found Jawbone is a challenge. You feed it back into their website, and they're probably using it, which they do because they send you little bits of, it says yesterday you took 3,000 steps you really should be taking 5,000 steps you know, so it puts it up to you, it never recommends products, it never does that, it does do the thing it would be good if you eat this kind of food which is okay you know, so I find that acceptable.”	-Would use Jawbone again believes data only used for prompts
3	“Before I decided I would like to see how it plays out and how it is implemented but probably would allow it ye. I would like a European wide one where I could fill my prescription anywhere in Europe. I wouldn't trust our government to implement it correctly though.”	“I'll continue with the FitBit. The apple HealthKit I want to fill in my emergency details in that. I'd want them to tie in better. I don't know if I'll get more dedicated to the FitBit it is a lot of effort.”	-EHR: probably but would want to see how its implemented -Will continue and plans to try app but not sure if will become more dedicated
4	“I don't know probably yes, like if I was rushed to A&E and I had an allergy if the hospital had the notes it would definitely be beneficial but I'd need to know more before saying definitely yes”	“I'd use them if I needed to, if I had a chronic illness like diabetes it would be great to keep track of my glucose levels and I could show my doctor if I wanted or share with him. I've used weight management, diet, exercise, pregnancy and menstrual cycle ones before and I'd definitely use them again...if I was older I think ones to remind you to take your tablets be great...but I think I'd only use ones recommended by my doctor like or a name I've heard of.”	-EHR probably yes due to benefit but would need info -Would try apps if met a need she had. -Has tried many -Prefer dr. recommendation or familiar company
5	“I suppose as long as it was kind of privatised in the way it was laid out like I wouldn't even want	“I think the fitness one is good to keep track if you're going to be learning from it but not if	-Fitness useful if learning but risk of obsession

Interview Participant	EHRs	Mobile health	Extracted Meaning
	diabetic written beside my name. I'd want some sort of code systems like for chronic illness so if you accessed me you wouldn't automatically get every single detail about my health, like if it was like that XXXXX, Diabetic, I would say absolutely no, but if it was well done and only information that was needed, so I could go on myself and see ye that's okay I'm happy with healthcare professionals seeing that. I wouldn't like access to everything so I could self-diagnose or to find out my bloods are back and I should visit doctor"	you're going to be obsessing over it. I prick my blood but I don't know if there's an app for that again maybe there is but I haven't come across it."	-Would use one for diabetes -EHR would require limited details only necessary data, control to check but not full access
6	"Probably yes but it comes down to hierarchy I wouldn't want my chiropractor to see everything my doctor can see, there might be some other information in the file that would be relevant to him and I wouldn't mind him seeing that. If there was a way I could say my chiropractor could access this and my GP can see it all."	"I would use the sleep tracker app I wouldn't have a problem using something like that. If there was a good app I trust, no actually maybe I wouldn't be dedicated enough to track my health."	-EHRs desire to control access on granular level -Would use sleep app little data disclosed but not detailed app may not be interested enough
7	"Very likely for efficiency I would like education beforehand and control though. If you can see a tangible side to it, then I'd consider it but on the other side of that if there's a risk I would be less likely. Privacy is important, again it depends like in some health situations the benefits could be greater than health fitness apps but the drawbacks are definitely very real and very concerning like you don't know where it's going."	"I'd use some but more so the information based ones, the exercise one's you can control. It's nice to be able to enter information to track your health but have they commercial motivations. They would have more merits if they were more open about where it was going and gave you a choice. My fitness data isn't too sensitive but I'd want to know more about the company before using it. The less third parties involved the better if you ask me – you just don't know where the information is going."	-EHRs: efficient but need for control and education privacy more important in some cases -mHealth: would use apps with control and non-sensitive data. Commercial motives
8	"I would include mine I would query the safety and privacy of the system before deciding. But if I was taking into hospital and they knew I had no appendix so they then knew the pain in my	"I would use pregnancy apps again I think. They all told me different things so I used a few and didn't enter much to them or didn't take it as gospel. I use a pill tracker now to remind me to	-Would use apps with caution and minimal data disclosure

Interview Participant	EHRs	Mobile health	Extracted Meaning
	stomach was not my appendix it would be helpful. I think it's hard to repeat or tell all the symptoms or history you have and sometimes you don't know what the serious points are and seeing it all together might help them diagnose quicker but I would query the safety and uses of my data."	take my pill so that's good. Menstrual cycle I used to use that but I wasn't great at it. I'd still use exercise ones in phases."	EHRs: yes, due to benefits of access and comprehensive but would query privacy and sec use
9	"I think I would be happy enough, because I'm from the South Side of Dublin so if something happened I would be rushed to Beaumont, they should be able to see whatever could affect my treatment. They should have some register they can access. It's probably very hard to win over people when they're giving away data like that but once it's clarified that this is going on a central database then I think it's okay, I think generally people won't disclose something unless it's to a doctor they might go online but if it's something serious they will go to the doctor, and there should be a central database and once it's consented to it should be okay."	"No. I play football now but unless it came in with the club I don't think I would use it. There's nothing stopping me I suppose if I was playing at a very top level I would try get every inch out but I play at lower level so it wouldn't bother me too much so it's just motivation I suppose."	-EHR: would opt-in -Should have central database -Difficult to win people over due to data sensitivity -People tend to go to the dr. but once they're informed and can consent -Health no intention due to no motivation/need -If was playing at higher level
10	Yes "I'd like access to the information and some control."	"No I wouldn't use anything like that. Diet app is one thing but nothing for real health stuff. I would be too paranoid about my health, say I had a blood pressure tracker I'd be constantly checking it. I would be worried. It would stress me out."	-Diet apps okay but no to 'real' health data as would cause stress -EHR consent with access and control
11	"A personal identification number held on a central system whether you go to a hospital in Dublin or in Galway that record is there, but restricted access to genuine medical professionals only in <b>your</b> interest, but the problem is people with ulterior motives, may hijack data for their particular purposes and sometimes they're to the detriment of the individual. There has to be checks and balances and safeguards but there's probably	"I'm just too busy to bother. It doesn't concern me. The only thing is, if someone is wearing these things and it somehow connected to a database, whoever is monitoring that are they able to identify you, as in who you are, and where you live and that and then target you in terms of ads, and are you able to stop it and unsubscribe, I don't know?"	-EHRs: would like a central system. Need for safeguards but always risks -mHealth: no intention due to lack of interest/time. Concern about lack of anonymity and secondary use



Interview Participant	EHRs	Mobile health	Extracted Meaning
	going to be occasional lapses of security. I'm in favour of all of these developments but with the right safeguards.		
12	"I would be very interested in using it for my own benefit, my own information. I would need to know more obviously."	"I would if they were available. If the doctor recommended it, I'd give it a try at least."	-EHRs: interested in accessing own data -mHealth: would try
13	"Patients, if they're not medically trained they may misread that information, and if they are going to have access to it they need to be spoken to about what it means. It might frighten them and with some people it might even do them damage because they'd be frightened."	"Yes because I've lost three stone. I'm really trying to improve my lifestyle, because I'm at an age where you can run into health problems so I'm trying to do something about it. If it was a recognised site, like the Mayo or a reputable place I wouldn't be opposed to using"	-mHealth: would try as trying to be proactive (HLOC) -Reputable organisation -Pro EHRs but patients could misconstrue data & cause
14	Willing to opt-in. "I don't give a damn who knows what about me medically because I think it's in my best interest that they do and you would have to rely on their professional etiquette as that they're not going to divulge anything sensitive."	"I wouldn't use them for myself."	-mHealth: checks steps infrequently & will fill in medical ID. Would not use wearables -EHRs: opt-in – need data trust they won't disclose
15	"I suppose its contradicting some of the things I've said but it sounds valuable yeah. As long as it was private not everyone can just see like Facebook or something like that."	"No, no. It's too much detail, technology has it's uses but I think you can be obsessed by it, how useful is it? I think they're valuable for people who need them, not particularly for me."	-EHRs: sees value, desire for restricted, controlled access -mHealth: No intention due to no need or health issues
16	"I think that would be very good."	"I'm not too familiar with them I wouldn't know how to do them but I probably would, if I was shown how it to get them up and all. I'd love to see how many steps I take. It's only if it's a certain ailment I would mind (disclosing data). Different types of information I mind yeah. Oh I'd be very wary of other information."	-mHealth: not familiar with apps but would try steps – would need help -Okay with sharing steps but no to other health data -EHRs: positive and beneficial
17	"Not a lover, I wouldn't be interested in that at all now. First of all, I think that there's nothing like the spoken word for a person to say and if there's going to be notes there they going to be more	No	-EHRs: no, reduce doctor patient interaction -mHealth: no intention to adopt

Interview Participant	EHRs	Mobile health	Extracted Meaning
	interested in what's on the screen that the person, and you know what you feel not the screen."		
18	Good idea	"I might if I thought it would help. I'd have to be shown how to use it."	-mHealth: would use if had a need & was shown
19	"I think it would be useful. I would like the little thing you plug into your computer and it's all there, that that's yours and you could bring that with, that's yours and that goes in your safe at home and if you had a heart attack your family could go and bring in your little key so it's yours. I think it's your privacy and yet it's there and it's not cluttering up."	"I wouldn't mind. I would use it, if I had one."	-EHRs: yes. desire for access to data. Suggests USB key -mHealth: would use step apps and trackers
20	"I would have some reservations. I wouldn't want doctors to automatically have access. It should be limited to what they need and only when they're treating with overrides in emergencies. I would like access, that would be good for reminding me after appointments and to look back over time. I could also spot some mistakes and follow up. My main reservation would be having all that information in one place, there would be huge interest from pharmaceutical companies, insurance companies, employers and even government to try access this information and I think that would really undermine the integrity. It should be for improving health only. I think a lot would depend on how the system was implemented too. I would want assurances it would be safe, would serve its purpose but no more. I think educating citizens would be very important and shouldn't be an afterthought but because of the possible benefits I would strongly consider giving my permission. I would want to be included but I wouldn't want to suffer as a result."	"I like my running app and I'm comfortable with the level of detail. I don't use all features I don't compete through the app, I don't share it on Facebook, I haven't given them real data. Other apps, I might try some non-invasive ones but I've no plans. I wouldn't try those all in one apps like Apple's one though. I wouldn't want to give all of that information to the tech lads. I don't use the Health thing on the iPhone and disabled the step tracking. It's very cheeky for them to automatically assume you want to track when you haven't given permission. They just put that on with a software update. They say include medication and allergy information for doctors to access in an emergency but why would a doctor check that, it's just a way to get that information by making you think it could really benefit you and maybe save your life. Nice try Apple but no not for me."	-EHRs: limited access for detail & time, patient access for errors and informing. Only used for health purposes. Education important & security. -mHealth: comfortable using apps with limited tracking, falsified data, and limited use of features. Will not use Apple Health – they just want data. Didn't ask for consent -No plans to try other apps but would consider non-invasive apps -IBT

Interview Participant	EHRs	Mobile health	Extracted Meaning
21	"It sounds like a very good idea but, it would really be a terribly tempting for health insurance companies to try hack into, or they might just get it sold to them."	"No. I don't even turn geolocation on my phone. No I've never used a health app and I've no particular desire to"	-mHealth: no intention -EHRs: useful but tempting for insurance companies to hack or buy
22	"Yeah."	"I wouldn't mind them having my steps and p what I eat that would be fine. Maybe like my mental health I wouldn't use it. If I was taking loads of meds and my blood pressure results or something like that maybe not"	-mHealth: okay with diet and steps but not mental or medication -IBT -EHR: would consent
23	Yeah definitely	"I do use the Fitness thing, for steps I occasionally check am I doing my 10,000 steps a day but I just out of curiosity. But I wouldn't go that far, it's not as valuable for me."	-EHRs: would consent -mHealth: checks steps occasionally wouldn't use tracker – no value for her
24	Yes, with limited access	"No. But only partly out of data or privacy concerns, it's mostly because I'm not sufficiently efficient, I'm not good at tracking things in general, but apart from just being too lazy, I would have some data concerns I in terms of security and in terms of what it might be used for, marketing."	-Wouldn't use any new apps due to forgetfulness and concern for secondary use and security -EHR yes but limited access and has concerns
25	N/A -doctor uses EHRs	"I probably will end up using health apps if I'm honest but I can't see myself using wearables. I won't be buying an Apple watch I can say that with certainty, I'm not really a gadget man. I would have a personal issue with sharing my health information with some with a database basically."	-Would use apps but not trackers as does not want to share health data with technology
26	"I'm not sure because but I'd be happy if he did I would want him to have access to whatever he needs access to, he seems like a good guy."	"It's attached to me so it's staying. It's interesting. It depends on what they're marketing, if it was a blood pressure monitor maybe. I have high blood pressure before so if I was really concerned about it I might look at something like that."	-Continue to use FitBit would use others if was worried about a condition -Wouldn't use PHR -Unsure about dr. use but would be happy – needs info

Interview Participant	EHRs	Mobile health	Extracted Meaning
27	N/A -doctor uses EHRs	"I will continue to use MyFitnessPal for now I like it. It keeps me aware and helps me manage "my diet in terms of ensuring my body gets the proteins and fats it needs. I will continue to monitor my exercise too because it keeps me focused to ensure I hit the goals I need to."	-Will continue to use app as helps monitor food and goals
28	Not sure if doctor currently uses. But it would be very helpful.	"No I don't like the apps or the FitBit. I feel like I put too much time into it and it doesn't really do much for me. I've tried them before, it's just not my thing. I'd rather exercise for myself rather than to reach a goal. It lasts longer too if you're doing it for yourself."	-Unsure if dr. uses EHRs -No intention to adopt apps as doesn't like -tried before but likes to be healthy for herself
29	N/A – doctor uses EHRs	"If I had a smartphone, I probably would, I like the idea of the sleep app. I don't know about the calorie ones where you have to input all that you eat because that would get tiring and annoying but one that measures heartbeat and mood if that were to exist although it probably wouldn't be reliable, I would want it to be reliable if I were to use it."	-If had smartphone might try sleep apps but automatic tracking not entering data -Interest in heart devices but would require reliability
30	N/A	Will continue to use trackers	-Use for tracking and competing
31	Doctor uses but no access- She would like access	"The hardest thing for me, if it's a company that is trusting. so I don't know if FitBit really is trusting but like start-up companies. It could be a 22-year-old kid who doesn't know anything about data or about health but are companies you want to trust but if it has medical research behind it you hope it's validated and that it's got safeguards that's the biggest thing. Maybe it comes through the insurance company or banner medical then you hope it has those safeguards."	-Hardest thing is determining trustworthiness of data handling, and advice offered

Interview Participant	EHRs	Mobile health	Extracted Meaning
32	-	“Probably. I would probably try something a little more advanced, something that monitors my heart rate and that kind of thing”	-Would use something more advanced e.g. heart rate monitor
33	“Not by choice, but often those decisions are made without including the patient. I think my doctor uses some kind of system. Not too sure on details but he didn’t inform me when he moved from paper.”	“No, I do not plan to use any of those technologies myself. As I said I try to limit my risk so I wouldn’t actively put health data on a phone or laptop and give it to a tech company. No. “	-Wouldn’t willingly enter EHR but lack of control -No intention to use mHealth due to risk
34	-	Uses Fitbit	
35	Need for anonymity and education on how information could be used	“The time to track it all sitting in a restaurant trying to type it in, there’s no way. And my privacy concerns. I just don’t want them to use my stuff. But my biggest thing would be how it fits my needs best. I would look at what I could use. I probably wouldn’t even look at privacy, it’s more of an afterthought but still important.”	-EHRs conditions anonymity & education -Barriers time and privacy -When deciding looks mostly for his needs – privacy an afterthought
36	“Yes. I would like proof of the security protocol in place that would reduce any concerns. I would like knowledge of who can access the data that would also be a comfort. I would like to have a say in this access to my record especially with third parties or my family. Any other uses of the information for marketing I would like to be informed beforehand.”	“Yes, I would like to purchase a FITBIT. They are quite expensive but I think I would like it and it would help me with healthy behaviours.”	-Willing to opt in -Conditions security awareness, access awareness and control for access & use -Plans to purchase FitBit. Expensive but will help change behaviours
37	-	“I do want to try a FitBit. I’m waiting for prices to drop.”	-Intention to try FitBit when cheaper – non-sensitive
38	[Doctor already uses EHRs]	“My mom was very much motivated and she took it. It makes us feel good, it motivates us to do more and more. So yeah I would use it again. I will search for health apps to have a proper diet and I heard about this it is a sleep pattern app so I think these apps help us take care of our health.”	-Would use tracker as motivating -Plans to use sleep app
39	N/A	“Yeah probably some health apps for tracking my conditions, that could help.	-Intention to use apps to help manage health – privacy calculus

Interview Participant	EHRs	Mobile health	Extracted Meaning
40	N/A Doctor uses EHRs	Doesn't use. Expensive at present	-Would consider but no plans
41	N/A Doctor uses EHRs	<p>"Yes. I consented to it and whatever I provided at the time I am okay with and I didn't give it more than my date of birth and my gender. Although since they track when I'm awake and sleep and move, I'm sure they can easily track my location which I didn't think about at the time of signing up.</p> <p>I use another app, to track my cycle, I'm sure I would use any app that I needed. But then again only if I was comfortable with the information I provided, I would never give detailed personal health issues to a faceless app."</p>	<p>-Will continue Jawbone use as happy with data disclosed</p> <p>-Didn't consider tracking</p> <p>-Other apps would need to be comfortable disclosing data wouldn't provide detailed health data (IBT)</p>
42	"I'm pretty sure he has files in filing cabinets. He uses a computer but it's not linked to anything I don't think and there's definitely a lot of paper usage. I think that (an EHR) would be fantastic."	"I will continue to use the FitBit, I like it. Knowing me I probably will get into pregnancy apps eventually when I go down that road. Or I know they've got that pacifier for kids that reads their temperature and stuff and that's pretty cool cos your baby can't tell you. I could definitely see myself using things like that."	<p>-EHR would opt in.</p> <p>-Continue to use FitBit</p> <p>-Future would use for children's health as very useful</p>
43	-	"Yeah, if they were cheaper and sometimes my husband and I laugh about how many steps we took on the S health and we have fun, mostly out of curiosity but I don't have much stuff on me so it may be that I don't like anything on me personally, would I have it in my phone, sure why not. "	-Intermittent use of health app curiosity but wouldn't wear wearable
44	"At some point you have to trust your doctor because they have more information than you do and you can have doctors that will misuse it but you always have the right to switch to a different doctor	"Yes. For example, I know that if I go to a doctor I can show them history on what my sugar levels have been for the last four years. It's not every day or every month but it gives you a general trend of what it has been so typically it may differ from one person to another."	<p>-Need to trust doctor</p> <p>- Awareness can track personally and share with dr. as symptoms differ from person to person</p>

Interview Participant	EHRs	Mobile health	Extracted Meaning
45	N/A	“Nothing’s really bothering me to the point where I feel like I need to yet, I may not be in the best shape but I do take pretty good care of myself I do watch what I eat. I’m going to have kids so I think that’s the point where I start looking at it more. Would use but I would lie or not give information.”	-Currently no need or push to use mhealth -would withhold or falsify data
46	N/A	“I like the one I use because I always forget to record my health but I should pay more time but it is not easy to remember so I don’t think I will be able to do more. I would if I had more time. My friend she records her health information and she always encourage me to try but I always forget.”	-Will continue use of menstrual tracker -Should take more time but forgetful – friend encourages her to try health apps
47	N/A	“FitBit, I’ll probably go back to that. A lot of the health apps are annoying to use. It’s hard to know what the good ones are.”	-Will use FitBit -Difficult to identify good health apps
48	N/A	“My watch tracks running distance so I like that. It’s not hooked to an app though. I use it whenever I run. The only one I can think of is PACT. My friend told me about it. Basically you can set goals and you have to either check in or take a picture of it and if you make your goal then you can make money, its super cool.”	-Dr. uses EHRs. -Will try health app
49	N/A	“I have definitely considered using them. I don’t do cardio exercise so it wouldn’t be worth the investment but if I ever start exercising I would definitely be interested in getting one. And devices that track your heart rate and blood pressure. I think that data is extremely powerful, the more data you have the better generally. I mean, it can be abused but I see data as a tool. I do sometimes	-Would use if exercised -Interest in other devices - data is a powerful tool there is risk of misuse -privacy calculus

Interview Participant	EHRs	Mobile health	Extracted Meaning
		use the Apple Health to track how many steps I've taken."	
50	-	"It comes down to is it going to be beneficial for the time investment, because there's a bunch of nutrition apps and activity trackers but for me personally I don't think that's going to change my behaviours, collecting data just for the purpose of collecting data is not an interest of mine so it needs to be able to actually help me do something different, that's why the Jawbone started to lose its appeal because it didn't change anything. I would use it for entertainment purposes rather than behaviour changing. I dabble with them and some are easier to use, the health app that comes with the iPhone is pointless because I haven't figured out how to go back and look at a really detailed trend of steps, a tiny graph doesn't help."	-Aware of number of health solutions but don't change behaviour -Doesn't track for sake of information