Navigating the Privacy-Health Nexus: A Smart Health Monitoring Systems Perspective

Jingjing Zhang

A thesis submitted to

Auckland University of Technology

in fulfilment of the requirements for the degree of

Doctor of Philosophy (PhD)

2025

Management, Technology and Organization Department

Faculty of Business, Economics and Law

Supervisors

Dr Farkhondeh Hassandoust

Professor Allen C. Johnston

Abstract

The digital age has sharpened the clash between health and privacy. Smart health monitoring systems (SHMSs) grant unparalleled health insights to empower individuals and communities, but their intrusive nature of data collection raises concerns for privacy. To delve more deeply into the intricacies of privacy phenomena in the health empowerment context through SHMSs, the present study includes two manuscripts organized as Chapter 2 and Chapter 3. Manuscript 1 aims to provide a comprehensive review of privacy contextualization in SHMSs. It addresses the question of, "*What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMSs context?*". Manuscript 2 employs a mixed-methods approach to explore actual and potential SHMS users through the lens of health empowerment theory. It aims to conduct a value-reflexive examination of health and privacy within the SHMS health empowerment context, addressing another research question of this study: "*How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?"*

Manuscript 1 develops a contextual framework derived from a systematic review of 49 peer-reviewed articles. This framework provides valuable insights for scholars aiming to understand the multifaceted privacy concerns in SHMSs settings. The findings help both healthcare providers and policymakers in pinpointing and addressing potential privacy issues surrounding personal health information when developing and implementing healthcare surveillance systems. Furthermore, the findings highlight existing knowledge gaps and suggest some key future research avenues to achieve a more profound understanding of privacy within the realm of SHMSs.

Manuscript 2 uncovers intricate dynamics between privacy and health priorities in SHMS use, particularly across age groups. The findings suggest that individuals tend to prioritize health over broader ethical and privacy considerations in the context of immediate health concerns, which may challenge the notion of traditional trade-off. However, this tendency varies with age. Non-elderly users (under 65) express greater discomfort with SHMS-related privacy loss compared to their elderly counterparts, hinting at generational shifts in privacy expectations. Furthermore, an interesting disconnect emerges in community health perspectives, where non-elderly users perceive their own health empowerment as inherently linked to the well-being of their communities, while, for elderly users, these concepts seem less intertwined.

The study presents a comprehensive review of privacy contextualization and a nuanced re-evaluation of privacy within SHMSs, recognizing the complex interplay between health and

privacy in the digital world. It is among a number of pioneering papers reporting on the prioritization of health empowerment over privacy concerns in SHMSs. This study also exhibits a notable opportunity to embrace contrarian thinking and explore alternative viewpoints. Theoretically, it contributes to the extension of health empowerment theory, adding to the development of the SHMS health empowerment research model. Practically, it suggests that SHMS practitioners should reassess the dynamics of the relationship between privacy concerns and health empowerment. Emphasizing perceived health benefits at personal and communal levels can be an effective strategy to address the tension between privacy and health empowerment.

Contents

Abstract....1
List of Figures....6
List of Tables....7
Attestation of Authorship....8
Co-Authored Works from This Thesis....9
Declaration of Collaboration....10
Acknowledgements....12
Ethics Approval....14
Chapter 1 Introduction....15
1.1 Research Purpose and Research Questions....20
1.2 Theoretical Background....21
1.2.1 Contextualization of Privacy in SHMSs....21
1.2.2 Theorizing the Imperative of Health Empowerment....21
1.3 Research Philosophy....23
1.3.1 Research Ontology....23
1.3.2 Research Epistemology....24
1.3.3 Research Methodology....24
1.4 Research Contributions and Significance....25
1.5 Organization of the Thesis....26
Preface to Chapter 2....28
Chapter 2 Privacy in Smart Health Monitoring: A Systematic Literature Review (Manuscript 1)....29
2.1 Abstract....29
2.2 Introduction....29
2.3 Addressing the Incomplete Contextualization of Privacy in SHMSs....32
2.3.1 Meta-review of the Extent of SHMS Privacy Review Articles....33
2.4 Review Method....34
2.4.1 Search Strategy....35
2.4.2 Study Selection....36
2.4.3 Data Collection Process and Coding....37
2.5 Findings....38
2.5.1 Overview of the Articles' Characteristics....38
2.5.2 Thematic Analysis....41
2.5.3 Privacy Definitions and Contextualizations....42
2.5.4 Proxies, Antecedents, and Outcomes....43
2.5.5 A Matter of Context....49
2.6 Discussion....51
2.6.1 Implications for Stakeholders and Practice....55
2.6.2 Recommendations for Future Research Avenues....57
2.6.3 Limitations....62

2.7 Conclusion 63
Preface to Chapter 3 64
Chapter 3 Health and Privacy: A Value-reflexive Examination (Manuscript 2) 66
3.1 Abstract 66
3.2 Introduction 66
3.3 The Values of Privacy Relative to Health in HIT Environments 68
3.4 Theorizing the Health Empowerment Imperative 70
3.4.1 Individual and Community Health Empowerment through SHMSs 71
3.5 Mixed Methods Research Design and Results 72
3.5.1 Study 1: Qualitative Study Design 73
3.5.2 Developing and Hypothesizing an SHMS Health Empowerment Model 74
3.5.3 Study 2: Quantitative Study Design 83
3.5.4 Quantitative Results 84
3.5.5 Applicability Check 90
3.6 Discussion 92
3.6.1 Meta Inferences and Theoretical Implications 93
3.6.2 Implications for Research and Practice 96
3.6.3 Limitations and Future Studies 98
3.7 Conclusion 99
Preface to Chapter 4 100
Chapter 4 General Discussion 101
4.1 Key Findings & Contributions 103
4.4.1 Findings and Contributions of Chapter 2 103
4.4.2 Findings and Contributions of Chapter 3 105
4.1 Implications for Research 111
4.2 Implications for Practice 112
4.3 Future Research 114
4.4 Limitations 115
Chapter 5 Conclusion 117
5.1 Review of Research Journey 117
5.2 Overall Research Purpose 118
5.3 Review of Research Question 1 119
5.4 Review of Research Question 2 120
5.5 Submission Status 121
5.6 Concluding Remarks 122
References 124
Appendices 151
Appendix A: Chapter 2 - Review Studies Summary 151
Appendix B: Chapter 2 - Coding Results 153
Appendix C: Chapter 3 - Supplementary Materials 166
Appendix D: Ethics Approval Letters 192
Appendix E: Participant Information Sheet 195
Appendix F: Consent Form 200

Appendix G: Interview Questions (Study 1 in Chapter 3) 202
Appendix H: Online Questionnaire (Study 2 in Chapter 3) 205

List of Figures

Figure 1. 1 Thesis structure....26
Figure 1. 2 The position of Chapter 2 in the thesis....28
Figure 2. 1 Four-phase study selection process guided by the PRISMA flow diagram....37
Figure 2. 2 A contextual framework of privacy in smart health monitoring....42
Figure 2. 3 The position of Chapter 3 in the thesis....64
Figure 3. 1 Roadmap of our developmental, mixed-methods approach....73
Figure 3. 2 SHMS health empowerment model....83
Figure 3. 3 Structural model results....87
Figure 3. 4 The position of Chapter 4 in the thesis....100
Figure 5. 1 Research journey....117
Figure 5. 2 Submission timeline....122

List of Tables

Table 2. 1 Inclusion and exclusion criteria 36
Table 2. 2 Summary of the articles' characteristics 39
Table 2. 3 Extracted antecedents and outcomes of privacy issues 44
Table 3. 1 SHMS privacy concern themes....75
Table 3. 2 Convergent validity testing 85
Table 4. 1 Key findings and contributions of Chapters 2 and 3....109
Appendix Table A. 1 Previous review studies on privacy in the health information technology domain 151
Appendix Table B. 1 Theories used to explain the antecedents....153
Appendix Table B. 2 Theories used to explain the outcomes 155
Appendix Table B. 3 Methods used in the published articles....158
Appendix Table B. 4 Coding of privacy definitions/descriptions 159
Appendix Table B. 5 Coding of privacy proxies....162
Appendix Table B. 6 Surveillance focused as a matter of context 163
Appendix Table B. 7 Stakeholder focused as a matter of context....164
Appendix Table C. 1 Literature review summary of privacy concerns in the smart health monitoring context 166
Appendix Table C. 2 Appropriateness of a developmental mixed-methods design (Adapted from Venkatesh et al. (2016)) 177
Appendix Table C. 3 Interview participants' profiles....180
Appendix Table C. 4 Selected quotes by respondents 181
Appendix Table C. 5 Survey respondents' demographic information....185
Appendix Table C. 6 Measurement items of constructs 186
Appendix Table C. 7 Procedural and statistical remedies....190
Appendix Table C. 8 HTMT values for discriminant validity 191

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Author's Name: Jingjing Zhang

	28 July 2024
Signature	Date

Co-Authored Works from This Thesis

The following list includes all co-author works related to this thesis that are currently undergoing revision for publication.

Manuscript 1: Zhang, J., Hassandoust, F., & Johnston, A. C. Privacy in smart health monitoring: A systematic review and research directions. *Communications of the Association for Information Systems* (Submitted on 5 May 2024 and under 2nd round revision).

Manuscript 2: Zhang, J., Hassandoust, F., & Johnston, A. C. Empowering health, rethinking privacy: A value-reflexive examination of health and privacy in the smart health context. *European Journal of Information Systems* (Submitted on 31 January 2024 and under 2nd round revision).

Below is a list of other submissions for workshops and conferences related to this thesis:

NZISDC2021-Poster: An investigation of privacy and surveillance perceptions of smart health stakeholders on smart health monitoring activities. *New Zealand Information Systems Doctoral Consortium (NZISDC) 2021, Massey University, Auckland.* (Presented on 3 July 2021).

PACIS2022-Short paper: Zhang, J., Hassandoust, F., & Johnston, A. C. An Investigation of Surveillance and Privacy-Protective Data Governance and its Impacts on Smart Health Monitoring Systems Use: A Collaborative Stakeholder Perspective. *Pacific Asia Conference on Information Systems 2022 (Virtual Conference)*. (Submitted on 31 March 2022 and presented on 5 July 2022.)

NZDISDC 2023-Poster: Privacy in Smart Health Monitoring Systems: Review, Conceptualizations, and Future Directions. *NZISDC 2023, University of Canterbury, Christchurch*. (Submitted on 16 June 2023 and presented on 8 July 2023.)

ACIS2023-Full research paper: Zhang, J., Hassandoust, F., & Johnston, A. C. Surveillance and Privacy-protective Data Governance in Smart Health Monitoring Systems. *Australasian Conference on Information Systems 2023, Victoria University of Wellington, Wellington*. (Submitted on 11 August 2023.)

Workshop paper: Zhang, J., Hassandoust, F., & Johnston, A. C. Surveillance and privacy-protective data governance in smart health monitoring systems. *Qualitative Paper Development Workshop 2023, University of Auckland, Auckland.* (Submitted on 31 August 2023.)

Declaration of Collaboration

This thesis contains submitted manuscripts comprising research papers with collaborative authorship. The student is the principal author of these co-authored manuscripts, contributing to the leadership and writing up of the work reported in the manuscripts. With guidance from the primary and secondary supervisors, the student actively participated in the entire process of developing the work reported in the manuscripts as research outputs. The student's contributions encompassed the development of research ideas and research design, crafting the research proposal, collecting and analyzing research data, and writing and revising drafts. The co-authors of these manuscripts are the primary and secondary supervisors. Their contributions mainly included shaping research ideas, conceptualization and design, editing and commenting on drafts, and supervising throughout the drafting and review process. The following tables provide details of the contributions, specifying the extent and nature of each co-author's input to the manuscripts, along with the authors' signed confirmation.

Student and Supervisor Approvals

By signing, the co-authors are confirming that the co-authors' contributions stated in the table(s) below are accurate.

Student Name	Jingjing Zhang	Signature	Date	28 July 2024
Supervisor Name (Co-author 1)	Farkhondeh Hassandoust	Signature	Date	29/07/2024
Supervisor Name (Co-author 2)	Allen C. Johnston	Signature	Date	30/07/2024

Chapter Number:	2
Manuscript Title:	Privacy in smart health monitoring: A systematic review and research directions.
Publication Status:	Submitted for Publication
Reference if published:	Not applicable

AUTHOR SURNAME:	CONTRIBUTION
Zhang	● Conception and design of the manuscripts; ● Acquisition of research data where the acquisition required significant intellectual judgment, planning, design, and input; ● Literature review and analysis (secondary data); ● Drafting and revising the manuscript; ● Corresponding with the journal.
Hassandoust	● Guidance on research ideas and research design; ● Critically reviewing the selection, coding, data analysis, and the manuscript in order to contribute to its quality and interpretation.
Johnston	● Guidance of research ideas and research design; ● Critically reviewing the manuscript in order to contribute to its quality and interpretation.

Chapter Number:	3
Manuscript Title:	Empowering health, rethinking privacy: A value-reflexive examination of health and privacy in the smart health context.
Publication Status:	Submitted for Publication
Reference if published:	Not applicable

AUTHOR SURNAME:	CONTRIBUTION
Zhang	● Conception and design of the manuscripts; ● Acquisition of research data where the acquisition required significant intellectual judgment, planning, design, or input; ● Analysis or interpretation of research data (primary data); ● Drafting the main parts and revising them.
Hassandoust	● Guidance on research ideas, gaps, and research design; ● Contribution of knowledge; ● Guidance and confirmation of data collection, analyses, and interpretations; ● Participation in the initial interview and providing guidance; ● Critically reviewing the manuscript in multiple rounds in order to contribute to its quality and interpretation.
Johnston	● Guidance on research ideas, gaps, and research design; ● Contribution of knowledge; ● Guidance and confirmation of data collection and interpretations; ● Critically reviewing the manuscript in multiple rounds in order to contribute to its quality and interpretation. ● Corresponding with the journal.

Acknowledgements

I would like to express my sincere gratitude to my supervisory team, Dr. Farkhondeh (Ferry) Hassandoust and Professor Allen C. Johnston, for their constant support and invaluable guidance. They have supervised me with a wise approach that has seamlessly integrated professionalism, kindness, passion, and patience. I am blessed to have Ferry as my primary supervisor on my PhD journey. Even before my PhD, she opened a fabulous new academic world for me during my Master's degree studies. Throughout my PhD journey, Ferry has trusted me, encouraged me, and generously shared resources she believed would benefit me – without any reservation. Moreover, Ferry has shown great patience whenever I have encountered difficulties in addressing feedback and meeting the team's requirements.

I would also like to express my heartfelt appreciation to my secondary supervisor, Professor Allen C. Johnston. Allen's professional guidance and insightful advice has made my journey more enjoyable, empowering, and highly productive. From Allen, I have learned how to collaborate humbly with team members. Moreover, he has equipped me with effective communication skills to navigate the broader academic ecosystem. I feel very lucky to have Allen in the team. Both Allen and Ferry have successfully promoted a solid and healthy relationship among team members, going far beyond mere supervision. I am incredibly fortunate to have had such supportive supervisors who have always been willing to make changes for the team. They have adapted their approach to my needs. They have taken the time to understand my perspective and ensure clear communication by either providing further explanation or adjusting their communication style. I will never forget their dedication in using their Christmas and New Year's holidays to help me meet a crucial manuscript deadline.

I would like to thank the staff originally at the Business Information Systems Department. It was unforgettable to have had the assistance of Professor Angsana A. Techatassanasoontorn, who supervised me to successfully completing my PhD proposal in the early stage of the journey. I am also grateful to Associate Professor Harminder Singh, the Deputy Head of the Department of Management, Technology and Organization, who agreed to be an additional supervisor in the role of mentor for my supervisory team, and who has continuously offering support throughout my journey. I would like to acknowledge and thank Professor Bill Doolin and Professor Antonio Diaz Andrade for providing insightful comments on my early PhD proposal and for generously sharing their extensive academic experiences with me. In addition, I would like to express my sincere gratitude to those outside AUT who have reviewed

my PhD proposals and ongoing papers and provided invaluable feedback. In particular, these include Professor Annette Mills, Associate Professor Mary Tate, Professor Michael Myers, and Professor Susanna Ho.

I would like to thank the staff from different departments at AUT, who have all been very kind to me and continuously provided strong and timely support in the journey. These include Dr Eathar Abdul-Ghani and Yvonne Meachen at the Postgraduate Research Office. Without Eathar's support in gaining a Doctoral Scholarship, my PhD journey would never have begun. I would also like to extend my appreciation to Associate Professor Kenneth Hyde in the Marketing and International Business department, who kindly offered me the opportunity to sit in on the Qualitative Research Methods paper in my first year of the journey.

I would like to express my sincere gratitude to all those who provided invaluable support during the data collection process for my PhD project. Many thanks go to Associate Professor Barbara Myers in the Management, Technology and Organization department and Professor Asheq Rahman in the Accounting department for their consultations during the preparation of my ethics applications. Additionally, I am grateful to Erin Moloney from the AUT Ethics Committee for her effective coordination on my ethics approval. I would also like to thank those who generously assisted me in identifying potential participants for this study. This includes individuals from both academia and industry, such as Elieen Song, Jenny Pooley, Dr Karen Day, Melanie Barr, Rachael Backer, Soheila Mohammadyari, and Professor Valery Feigin.

I would like to take an opportunity to thank my fellow PhD students for their sincere assistance throughout the journey. These students include Shikha Shethia, Jalthotage Nishika Jayasinghe, Himanshu Sharma, and Kai Schaedlich. Special thanks to Ludwina Lafaele and Andrea Cu for their ongoing administrative support. Their contributions have also been instrumental in my progress.

The constant support and love of my husband James Gao, my parents, my parents-in-law, and the spiritual community at the Auckland Christian Evangelical Church, have been a pillar of strength throughout this journey. I am incredibly grateful for their presence. It empowered me to begin and complete this challenging project.

I extend my special thanks to Elizabeth Ardley and Alison Warren for their professional and insightful proofreading of this thesis.

Lastly, all glory to the Almighty.

Ethics Approval

The present study involved a two-stage ethics applications process – qualitative and quantitative stages. The ethics application number is 22/156.

For the qualitative stage of Chapter 3, the ethics application was approved by Auckland University of Technology Ethics Committee (AUTEC) on 13 September 2022, and is valid for three years until 13th September 2025. The application for an amendment to extend the recruitment of interview participants in Australia was approved by AUTEC on 2 February 2023.

For the quantitative stage of Chapter 3, the ethics application was approved by AUTEC on 14 September 2023.

The appendices section presents the ethics approval letters (Appendix D), participant information sheet (Appendix E), and consent form document (Appendix F).

Chapter 1 Introduction

Smart health monitoring systems (SHMSs) are a form of health information technology (HIT), utilizing cutting-edge surveillance technologies to monitor changes in individuals' personal vital signs and daily health (Alabdulatif et al., 2019; Almujally et al., 2023). These surveillance technologies encompass devices like blood glucose wearables and electrocardiogram (ECG) monitors, which are crucial for the functionality of SHMSs (Stavropoulos et al., 2020). The global SHMS devices market, valued at USD 190 billion in 2024, is projected to surge to USD 474 billion by 2032 (GlobeNewswire, 2023), showing vast potential of surveillance technologies in smart health monitoring applications.

The substantial growth of SHMSs in recent years can be attributed to the anticipated benefits that include facilitating communication between patients and healthcare providers, streamlining diagnostic and treatment processes, reducing costs associated with professional visits, and improving the quality of personal care (Akmandor & Jha, 2018; Salehi-Amiri et al., 2022). While offering their individual members enhanced management of their health status (Sovacool & Del Rio, 2020), SHMSs also provide vital community-level support for public health research, policy development, and disease prevention strategies, among other benefits (Wolfenden et al., 2019). For example, SHMS projects can strengthen observational studies on chronical illnesses and facilitate interoperability over connected hospitals (Pramanik et al., 2017). As surveillance applications, SHMSs provide interactive contexts for health empowerment among individual community members and health service providers, while shaping the regulatory landscape of health policy and systems on a broader scale (Nelson et al., 2016).

Health empowerment is a dynamic process in which people recognize and engage their personal and social contextual resources, and purposefully participate in improving health with the aim of achieving optimal well-being (Jiang et al., 2022; Shearer, 2007). Health empowerment is regarded as the ability of an individual to control their lives and health experiences at a personal level (Shearer, 2007). For instance, some health wearable devices can enhance health empowerment by encouraging overweight users to actively participate in decision making and increase their exercise output (Mardonova & Choi, 2018). Health empowerment is also a multi-level concept with significance for community psychology in relation to collective groups of individuals (Rappaport, 1987; Swift & Levin, 1987; Zimmerman, 2000). For instance, healthcare service providers collaborate with partners across the community and utilize clinical-trial data (successes and failures) to make breakthrough

scientific discoveries (Groves et al., 2013; Pramanik et al., 2017). With this understanding, community health empowerment in the context of SHMSs can be achieved if members actively engage in collective activities that influence health-related decisions affecting the health status of their community. Based on health empowerment theory (Rissel, 1994), community health empowerment also reflects a raised level of individual health empowerment, where the individual is a 'true member' of an SHMS community.

Despite considerable investments in SHMSs and recognition of their relevant benefits, the actual achievement of health empowerment through SHMSs appears to fall short both at the individual and community-level, including health professionals. In this thesis, I define all individual users and practitioners involved in SHMSs as stakeholders. Multiple global reports (e.g., Accenture.com, 2020; Capterra.com, 2021; Fortune.com, 2023; New Zealand IoT Alliance, 2017) highlight that consumers' privacy concerns about the surveillance technologies embedded in SHMSs are a key reason they avoid using health monitoring applications and sharing their health data with health professionals. According to both media reports and the literature, the use of such surveillance technologies evokes confusion or uncertainty among SHMS consumers and other community-level members about who bears responsibility in the event of the loss of health data, and how the proper protection and usage of this data within the surveillance framework can be guaranteed (Accenture.com, 2020; Duckert & Barkhuus, 2022; Princi & Krämer, 2020). Therefore, while SHMSs provide ambitious health insights that can empower individuals and communities, their intrusive nature through data collection (surveillance) raises concerns about privacy, potentially undermining efforts to achieve health empowerment and instead leading to undesirable consequences. These include low SHMS adoption, limited data sharing, incomplete health insights, regulatory and legal challenges, and widespread distrust of surveillance technologies, all of which can seriously impede the realization of the full benefits of health empowerment (Mata-Cervantes et al., 2016; Matt et al., 2019; Nelson et al., 2016).

For much of human history, both health and privacy have stood as fundamental rights, deeply ingrained in the fabric of human existence (Cohen & Ezer, 2013; Di Iorio et al., 2021). They are distinct rights by nature, valued highly for different reasons, but each inextricably linked to Maslow's hierarchy of needs (Maslow, 1943). Maslow's hierarchy of needs refers to a pyramid of human needs from the most basic to the highest (Maslow, 1943). The hierarchy suggests that people seek to satisfy five sets of needs: physiological needs, safety needs, belongingness needs, esteem needs, and self-actualization needs. For example, health is valued as a physiological necessity associated with meeting our most basic need for survival and well-being against injury and accidents (McLeod, 2007; Shapiro et al., 2019), while privacy is valued

as a safety and security requirement in the higher level of needs associated with meeting our need to not be caused harm (Maslow, 1970; Shen et al., 2021). Privacy is also valued for its ability to help meet our needs for esteem and self-actualization, whereby we are seen positively by others and are able to express ourselves genuinely and freely (Laufer & Wolfe, 1977; Maslow, 1970; McLeod, 2007).

Because of contemporary demands of convenience, personalization, and capitalism (Puntoni et al., 2021; Zuboff, 2015), the needs for health and privacy in the modern digital world have increasingly come into contention, serving as opposing forces where the gain of one requires the loss of the other (Fox, Clohessy, et al., 2021; Hassandoust, Akhlaghpour, et al., 2021; Princi & Krämer, 2020; Schomakers & Ziefle, 2023; Shen et al., 2019). Within the literature, some degree of privacy loss is assumed to be an important determinant for effective health diagnosis and treatment throughout the course of one's life (Gao et al., 2015; Seh et al., 2020). However, the contention between the needs of privacy and health in SHMSs seems to contradict Maslow's hierarchy principle, which states that basic needs must be satisfied before any other needs in a higher level can be satisfied (Maslow, 1943). According to this principle, individual users of SHMSs will raise privacy issues only after their health needs have been adequately addressed by the system; however, in practice, Maslow's hierarchy of needs seems inadequate in explaining the situation.

Privacy is often characterized as multidimensional, elastic, and dynamic, adapting to the nuances of individual life experiences (Smith et al., 2011). Thus, people's beliefs about privacy may vary, and its importance may be rated differently for various reasons and contexts, especially in monitoring situations like SHMSs (Kennedy et al., 2021). In short, privacy is context-dependent (Smith et al., 2011). Contextualization enriches our understanding of the subjects under investigation and unveils alternative interpretations of the phenomena from more insightful perspectives (Zahra et al., 2014). It is a foundational step that sets the stage for a deeper exploration. In the information systems (IS) field, the most commonly cited contexts for privacy are related to technological workplace applications, the use of information by sector, the type of information collected from individuals, and politics (Smith et al., 2011).

Given this background, it is urgent to understand privacy phenomena in the context of SHMSs and to conduct a value-reflexive examination of privacy as it relates to health empowerment in this setting. In this vein, the study aims to synthesize the fragmented views on privacy in SHMSs, offering a comprehensive contextualization of privacy before exploring the privacy issues in relation to individual and community health in SHMS settings. Therefore, my first

research question is: *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMSs context?*

Existing literature on SHMSs often provides a rather fragmented and limited exploration of contextualized privacy. For example, contextualized privacy definitions are often missing or poorly explained, focusing only on one group's view of privacy (e.g., Bhatt & Chakraborty, 2020; Dadhich et al., 2022; Peek et al., 2016; Ravishankar et al., 2015). Weaknesses such as these create contextual ambiguity and weaken researchers' abilities to set their studies' direction, choose theories, and interpret their findings (Dinev et al., 2013). Furthermore, a meta-review of the literature was conducted to re-evaluate the existing review studies for a context-specific exploration of privacy issues in the HIT domain (see Appendix Table A. 1 in Chapter 2), the results indicated that existing review studies on the topics of privacy and smart health are incomplete. For example, in some studies, the review criteria, including transparency and the research agenda, are inadequately provided: establishing criteria such as a search strategy and formulating a research agenda are foundational elements of methodological transparency for maximizing research impact (Paré et al., 2016; G. Wagner et al., 2021). Also, the exploration of contextual privacy was found to be incomplete. For example, only one review paper analyzed privacy definitions in its study context (Shen et al., 2019). A handful of papers reviewed antecedents and outcomes of privacy (e.g., Carver & Mackinnon, 2020). A limited set of papers discussed research agendas (e.g., Shen et al., 2019; Talal et al., 2019; Zaman et al., 2022). Given the importance of contextualized privacy (Nissenbaum, 2004, 2009), this study therefore aims to conduct a robust review on the topic and highlight the deficiencies of the existing literature which fails to provide a full picture of contextualized privacy and its significance in SHMSs (see Chapter 2).

With a stronger understanding of contextualized privacy issues in SHMSs, the study continues by exploring privacy phenomena in the context of SHMSs and conducting a value-reflexive examination of privacy as it relates to health empowerment in this setting (see Chapter 3). According to the findings from the systematic literature review (SLR), privacy in exchange for health has become an accepted assumption when digital technologies are chosen to empower effective health systems and personalized healthcare (e.g., Hassandoust, Johnston, et al., 2021; Tran & Nguyen, 2021) – but should it be? Should we assume privacy loss is acceptable for everyone when balanced against their health or are there aspects of the fundamental right to privacy that persist beyond the promise of better health? Further, does the consideration of individual privacy even matter when the health of an entire community is at stake? So, in the context of empowering health versus concerns for privacy, when we ask, "Which values do we value?" (Zimmer et al., 2023, p. 1), the answer could very well be, "It depends."

Values are defined “as trans-situational goals, varying in importance that serve as guiding principles in the life of a person or group” (Schwartz et al., 2012, p. 664). Values can be understood as "what is important to us in life" (Schwartz, 2012, p. 3), and the trade-off between pertinent and conflicting values is what steers an individual toward pursuing a specific goal (Schwartz, 2012). There is a prevailing belief that an individual's values serve as consistent indicators of their thoughts and behaviors in value-relevant situations (Rohan, 2000). The degree of concern individuals feel about something in life can be explained by the level of importance they attach to values associated with that object.

The values of power, achievement, and hedonism promote individuals’ self-enhancement goals. Threats to these values activate cognitive awareness and affective experience related to such threats (Schwartz et al., 2000). It has been argued that these self-enhancement values are also associated with the violation of personal privacy (Alashoor et al., 2015; Schwartz et al., 2000). Privacy represents a fundamental human right to be free from intrusion by others (Solove, 2002; Tavani, 2007), and includes an individual’s right to restrict (or manage) others’ access to personal data through the use of surveillance (Marx, 2015). In the health sector, privacy concerns reflect an individual’s need for a physiological sense of control, boundaries, and self-protection concerning their health information (Zhu et al., 2022). The antecedents of privacy concerns can be categorized according to their influence on the individual, contextual, or macro-environmental level (Henderson & Snyder, 1999; Li, 2011; Miltgen & Peyrat-Guillard, 2014; Xu, 2019). A summary of studies on privacy concerns in the SHMS context is presented in Appendix Table C. 1. In sum, this literature suggests privacy matters to HIT users, even when weighed against one’s health. The details of findings are presented in the following chapter.

Despite the conventional notions of privacy in mainstream research, a number of studies challenge the traditional assumptions of privacy and health value (e.g., Princi & Krämer, 2020; Zarcadoolas et al., 2013). For example, some researchers argue that privacy concerns are not a barrier preventing participants from using HIT (Zarcadoolas et al., 2013). Therefore, before accepting any conventional understanding as a definitive underlying assumption about how individuals perceive and experience the tension between privacy and health in the SHMS context, it is important to ask the following: *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?*

Empowerment is a complex concept originating from women’s and civil rights movements (Rissel, 1994). Based on this concept of empowerment, empowerment theory links individual well-being with the larger political and social environment, suggesting that people need

opportunities to become active in community decision making to improve their well-being, lives, organizations, and communities (Zimmerman, 2000). Health empowerment theory has developed from empowerment theory and uses the premise of empowerment to explain health promotion in the context of health communities (Rissel, 1994). Health empowerment theory provides a model that includes both individual and community health empowerment (Rissel, 1994): individual health empowerment is a pre-requisite for the next level, i.e., community health empowerment (Rissel, 1994; Swift & Levin, 1987; Torre, 1986). In other words, a combination of both levels is essential before community health empowerment can occur (Rissel, 1994). It is noteworthy that empowerment is a construct considered to be both an outcome and a process (Rissel, 1994). It is an outcome when empowerment is defined by the distinction between levels (Rissel, 1994; Zimmerman, 1990). Empowerment is also a process that simultaneously operates at both levels until community health empowerment is obtained with an increase in the control over resources (Rissel, 1994; Zimmerman, 2000).

1.1 Research Purpose and Research Questions

The meta-review (review of existing literature review articles) findings strongly underscore the need to address the deficiencies of privacy in previous review studies. To derive a more informed interpretation and conclusion regarding privacy concerns related to SHMSs for researchers and other stakeholders (such as practitioners), the present study first aims to provide a more comprehensive, integrative review of privacy contextualization in SHMSs. It includes synthesizing privacy definitions from various perspectives and reviews the antecedents and outcomes of privacy, relevant theories, methodological transparency, research agenda, and other pertinent scopes (see Chapter 2). The study then explores privacy concerns in relation to health empowerment by conducting a value-reflexive examination of health and privacy in the health empowerment context via the use of SHMSs (see Chapter 3). Leveraging health empowerment theory, the present researcher pursues alternative perspectives that may challenge prevailing attitudes or trends but allow for a deeper investigation into the intricacies of privacy phenomena related to SHMSs. This study seeks to explore the complex dynamics, or the ongoing contention between health and privacy values in relation to SHMSs, surfacing inconsistencies and disparities between the study's findings and prevailing thought on the value of privacy in health information technology use like SHMSs.

The research questions (RQs) that emerge from the purpose of this study are as follows:

> **RQ1** (Chapter 2): *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?*

RQ2 (Chapter 3): *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?*

1.2 Theoretical Background

1.2.1 Contextualization of Privacy in SHMSs

Over the past two decades, IS researchers have shifted their focus away from technology development and toward the social context surrounding the design and use of information technologies (Avgerou, 2019; Sidorova et al., 2008). This shift underscores the importance of contextualization in IS research, which involves identifying domains beyond the individual components of a central phenomenon (Renwick & Gleasure, 2021). Researchers have long been encouraged to provide a contextualized definition of their phenomena of interest, as this definition plays a pivotal role in setting the stage for how the phenomena will be examined (Angel & Calo, 2023; Solove, 2002).

Context is important to theory development (Avgerou, 2019). Contextualization in privacy research can be utilized as a powerful sensitizing tool for illuminating the boundary conditions of privacy theories (Xu & Zhang, 2022). In simple terms, contextual richness is an essential way to help link research phenomena and build theory (Zahra, 2007). New theories are emerging which may not have yet received a great deal of attention in new research themes, such as SHMSs. Contextualization helps enrich the existing theoretical perspectives by creating opportunities for their potential integration, and even advancing new theoretical frameworks (Zahra, 2007). Hence, the study approaches contextual richness by examining antecedents and outcomes of privacy in SHMSs, as well as theories and methodologies utilized in the previous literature. Considering their contextual significance, the SLR work pays particular attention to surveillance and stakeholders to provide a complete picture of privacy contextualization within the smart health monitoring context.

1.2.2 Theorizing the Imperative of Health Empowerment

To provide a foundation from which to explore the tension between the values of health and privacy in the SHMS context, while simultaneously engaging with our own value systems, the study looks to health empowerment theory (Rissel, 1994). Health empowerment theory is a derivative of empowerment theory and promotes empowerment as a tool or means by which to achieve the broader goal of better health (Rissel, 1994). As mentioned earlier, this theory suggests a model including both individual and community health empowerment (Rissel, 1994). Applying the definitions proposed by Spreitzer (1995), *individual health empowerment* refers to individuals' perceptions of access to information, support, resources, and

opportunities to learn and grow, enabling individuals to optimize their health and obtain a sense of competency, meaningfulness, self-determination, and impact in their lives. *Community health empowerment* is a group phenomenon that includes a raised level of individual health empowerment, a political action in which individuals have dynamically participated, and the achievement of the redistribution of resources or decision making beneficial to the community in question (Rissel, 1994). Thus, community health empowerment in the context of SHMSs can be achieved if members actively engage in collective activities that influence health-related decisions affecting the SHMS community's health status.

In terms of the challenge of balancing the values of privacy and health empowerment, individuals who are more passionate about gaining broader experiences, sharing their information and knowledge, and acquiring skills, distinguish themselves in the supportive environment of the SHMS community (Rissel, 1994). Through their engagement with SHMSs, individuals not only feel part of the SHMS community and experience personal growth, but also have power as part of that community (Laverack & Wallerstein, 2001; Wolfenden et al., 2019). Despite the parallel advancements in both personal and community levels of empowerment, privacy concerns can deter individuals from engaging with SHMSs, sharing personal health information, and actively participating in health-related initiatives. This is a crucial issue because personal health data is fundamental to the functionality of SHMSs (Nelson et al., 2016).

This study adopts health empowerment theory as an overarching theoretical lens to explain the health versus privacy phenomenon in SHMS contexts. It introduces a fresh perspective on the role of health empowerment theory, guided by the following considerations. First, the term 'theory' is part of a group of words that includes speculation, supposition, guess, conception, conjecture, proposition, hypothesis, explanation, and model (Weick, 1995). There are opportunities to carry theories more flexibly with diverse purposes (Weber, 2012). A theory can serve as a lens through which researchers highlight specific things while filtering out what is seen as irrelevant or noise. Although theories shape what researchers observe—influencing both what they notice and what they overlook (Truex et al., 2006)—this study applies health empowerment theory as a tool to guide the process of understanding complex and often conflicting real-world phenomena (Truex et al., 2006).

Second, health empowerment theory serves as a middle-range theory, offering a framework for explanation. Drawn on the health empowerment framework, the researcher utilizes contextual evidence, including interviews, to contextualize the theory and develop an SHMS health empowerment model (Hassan & Lowry, 2015). Third, IS researchers are recommended

to use theories that allow for exploring a broader, social perspective, rather than the narrow, individualistic perspective that had previously dominated the literature (Weber, 2012). Health empowerment theory goes beyond simply achieving outcomes; it prioritizes the importance knowledge, agency, and control over one's health. Thus, health empowerment theory is well-suited to explain the health value that SHMS users gain in exchange for their privacy, within the context of health empowerment through SHMS usage.

1.3 Research Philosophy

The process of academic research is primarily driven by the philosophical perspectives of the researcher. These perspectives shape the foundational assumptions of various research paradigms and guide the formulation of research questions, as well as the design and analysis of the study (Creswell, 2009). A philosophical paradigm can be seen as a set of fundamental beliefs held by individuals. It represents a worldview that outlines the nature of the world, the individual's place within it, and the range of potential relationships to that world and its components (Guba & Lincoln, 1994). The principles of a post-positivist paradigm focus on the significance of meaning and the generation of new knowledge; they support dedicated social movements, which aim to transform society and advance social justice (Ryan, 2006). Post-positivism asserts that claims about reality must be subjected to the broadest possible critical examination to enable the closest possible understanding of reality (Guba & Lincoln, 1994). The present research follows a post-positivist research paradigm (Creswell & Poth, 2018), because it seeks objective answers to the research questions. The research philosophy can be represented in terms of four elements: ontology, epistemology, methodology, and method.

1.3.1 Research Ontology

Ontology is the branch of philosophy that studies the nature of existence and reality (Creswell & Poth, 2018). It is concerned with how we understand reality. Ontological assumptions can be categorized along a spectrum, with realism at one end and relativism at the other (Crotty, 1998). Among the beliefs of alternative inquiry paradigms, post-positivism represents critical realism, where reality is assumed to exist but to be only imperfectly understood due to the inherent limitations of human intellectual mechanisms and the complex nature of phenomena (Guba & Lincoln, 1994). Critical realism posits that an objective social and natural reality exists that waits to be scientifically discovered and studied (realism), but it also acknowledges that this reality is imperfectly measured and subjectively constructed (relativism) (Guba & Lincoln, 1994; Pickard, 2013). In the present research, privacy phenomena exist in the context of SHMSs. However, following post-positivism's critical realism, this research seeks a more informed interpretation and conclusion on privacy phenomena related to SHMSs. It therefore

explores privacy in relation to health empowerment by conducting a value-reflexive examination in SHMSs.

1.3.2 Research Epistemology

Epistemology refers to the philosophy of knowledge, focusing on the validity of information required for research and the methods by which it can be acquired (Ponterotto, 2005). In simple terms, epistemology focuses on the nature of knowledge or how we come to know and understand things, which is closely linked to ontology and methodology (Krauss, 2005). While ontology deals with the nature of reality, epistemology addresses how we can know that reality (Krauss, 2005). The present research investigates epistemologies by way of assumptions about knowledge. It aims to see the whole picture of privacy issues in relation to health empowerment in SHMSs, striving for objectivity beyond just the facts (Ryan, 2006). The research addresses inconsistencies and disparities between its findings and the prevailing thoughts on the value of privacy in health information technology use. It means to explore whether the findings fit with pre-existing knowledge. Consequently, the epistemology approach in the present research emphasizes critical traditions, suggesting that findings are potentially true but always open to falsification (Ryan, 2006).

1.3.3 Research Methodology

Although the post-positivist paradigm is mostly connected to quantitative research, researchers can use this paradigm when they are undertaking a mixed methods study in order to uncover multiple perspectives (Onghena et al., 2019; Yin, 2017). To address the research questions, the present study mainly employs a sequential two-stage mixed-methods design encompassing both qualitative and quantitative studies (Creswell & Plano Clark, 2018).

This specific design is chosen due to its three methodological advantages. Firstly, a sequential mixed-methods research design has the ability to address various types of questions—whether confirmatory, exploratory, and pseudo-exploratory[1]—within the same study inquiry (Venkatesh et al., 2013). Secondly, it enables a holistic understanding and integrative insights into findings from a combination of qualitative and quantitative aspects, which strikes a balance between depth and breadth (Venkatesh et al., 2013). Thirdly, a mixed-methods design is particularly suitable for exploring new contexts where issues are challenging to explain or describe using existing views (Ågerfalk, 2013).

[1] Pseudo-exploratory questions are designed to elicit responses that could help contextualize the model for testing. (Banasiewicz, 2021).

Because a mixed-methods research design should serve a specific purpose, it is crucial to consider the appropriateness of the selected mixed-methods design (Venkatesh et al., 2016). Mixed-methods designs are categorized by their purpose: developmental, completeness, complementarity, expansion, corroboration/confirmation, compensation, and diversity (Venkatesh et al., 2013). Among these categories, the study follows the developmental purpose, which involves using the findings of a qualitative study to develop a suitable set of constructs, establish relationships among these constructs in the form of a model, and propose a corresponding set of hypotheses. Subsequently, these hypotheses are tested using a quantitative method (Venkatesh et al., 2016). The research design adheres to ethical guidelines, ensuring appropriate handling of ethical considerations such as participants' data privacy protection, voluntary consent, and risk of harm. It received approval from Auckland University of Technology Ethics Committee (AUTEC). Further justification for employing a developmental mixed-methods design can be found in Appendix Table C. 2. It explains the steps of establishing criteria and the requirements of a developmental mixed-methods research design in the present research.

To answer RQ1 and identify directions for future research, an SLR was conducted, focusing on privacy in smart health monitoring studies (see Chapter 2). A literature review helps address broad questions through a holistic review approach, providing a complete picture of the prevalence of research on a focal topic (Grant & Booth, 2009). It is “a form of secondary study that uses a well-defined methodology to identify, analyze, and interpret all available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable” (Kitchenham & Charters, 2007, p. vi). It also ensures accuracy and impartiality in the search and retrieval process while supporting the development of future research guidelines or directions that professionals can use (Fernández-Alemán et al., 2013).

To answer RQ2, an empirical study was conducted. This empirical study included a pre-study component in the mixed-methods design that served to establish the extant perspective of the contention between privacy and health in the context of SHMSs and health empowerment theory. The main body of the empirical study includes both qualitative and quantitative studies. The details of the qualitative (Study 1) and quantitative (Study 2) components of the mixed method approach are described in Chapter 3.

1.4 Research Contributions and Significance

This study addresses the gap in the comprehensive contextualization of privacy in the context of SHMSs. It develops a contextual framework derived from a systematic review of 49 peer-reviewed articles. This framework provides valuable insights for scholars aiming to understand

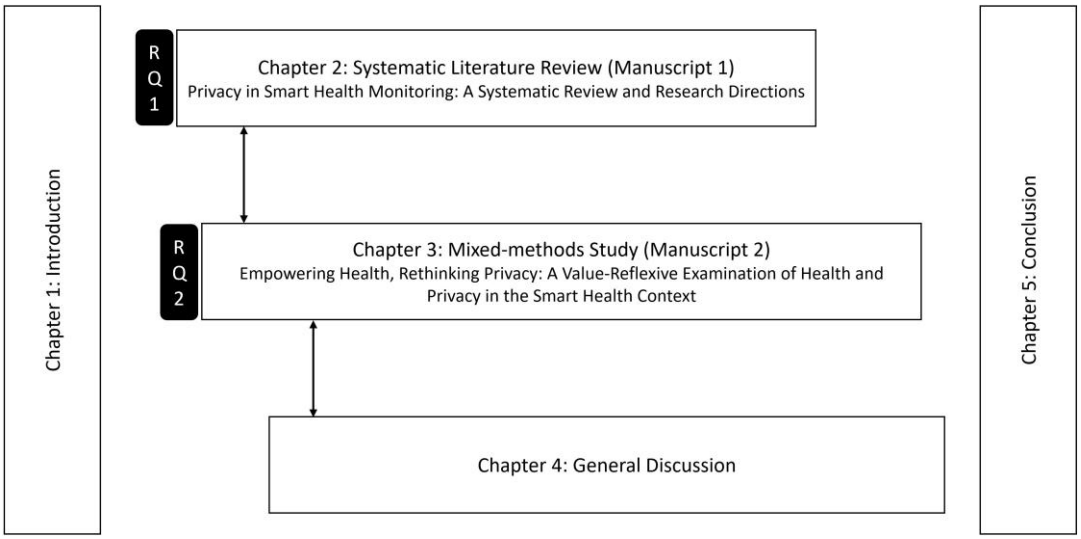
privacy concerns in SHMS settings. The findings highlight existing knowledge gaps and suggest six targeted research avenues to achieve a more profound understanding of privacy within the realm of SHMSs. Based on the findings and the developed framework, a deeper understanding is gained of the intricate interplay of privacy and health values within the digital environments that SHMS users experience. This understanding challenges the conventional notion that privacy concerns uniformly impede health empowerment across one's lifespan. As one of the pioneering papers reporting on the prioritization of health empowerment over privacy concerns in the context of SHMSs, our study offers implications for research and practical applications.

1.5 Organization of the Thesis

The remainder of this paper is organized into 4 chapters following the guidelines of the Postgraduate Handbook for Format Two. Figure 1. 1 offers a visual representation of the thesis structure for the convenience of readers.

Figure 1. 1

Thesis structure



Chapter 2 addresses RQ1, which is based on the SLR, or Manuscript 1. Chapter 2 first sets the stage for the review by discussing the importance of contextual clarity in IS research and the shortcomings of existing review articles in meeting this need. It then outlines the methodology of the SLR, including article selection and the coding process. Finally, it presents the findings, a discussion of future implications, and concluding remarks.

Chapter 3 addresses RQ2, which is based on the mixed-methods study, or Manuscript 2. Chapter 3 first describes the salient literature that informs current understanding of the values of privacy relative to health in HIT environments. It then describes the theoretical foundation

on which the study explores the contentions surrounding health and privacy that SHMS users experience. The mixed-methods research design is then presented, along with the findings that inform the discussion. Theoretical and practical implications follow.

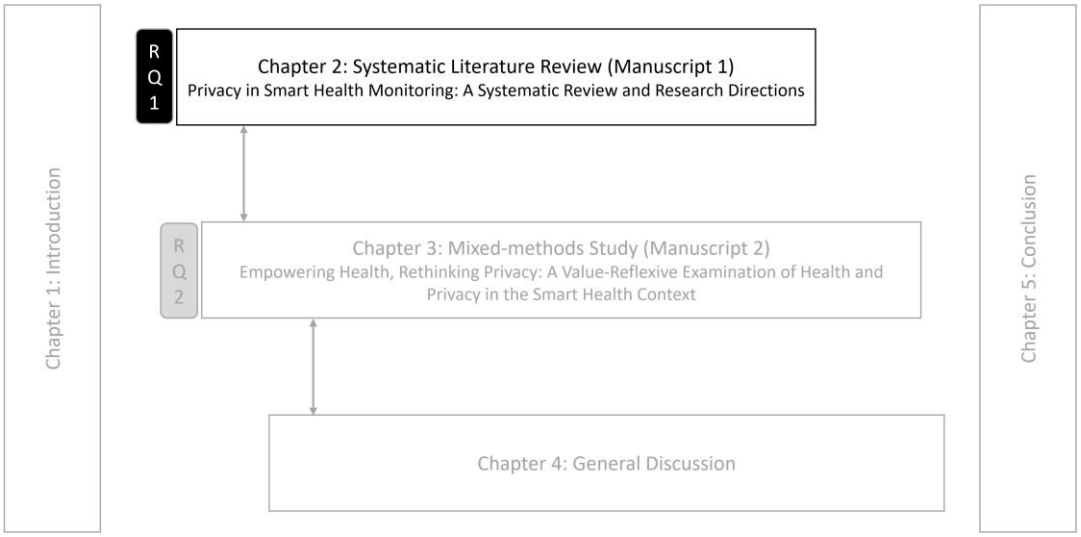
Chapter 4 provides a general discussion based on the findings and contributions of the previous two chapters. Finally, Chapter 5 concludes the study by reviewing the research questions and research purposes, highlighting the contribution and implications of the research, and indicating limitations and future research directions.

Preface to Chapter 2

Chapter 2 aims to answer the first research question (RQ1): *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?* As shown in Figure 1. 2, Chapter 2 includes Manuscript 1, titled '*Privacy in smart health monitoring: A systematic review and research directions*.' Chapter 2 addresses the gap in the comprehensive contextualization of privacy in the context of SHMSs, developing a contextual framework derived from a systematic review of 49 peer-reviewed articles. This framework provides valuable insights for researchers aiming to understand the multifaceted privacy concerns in SHMS settings. The findings from this chapter can help both healthcare providers and policymakers in pinpointing and addressing potential privacy issues surrounding personal health information when developing and implementing healthcare surveillance systems. The findings also highlight existing knowledge gaps and suggest six targeted research avenues to achieve a more profound understanding of privacy within the realm of SHMSs. The remainder of this chapter presents Manuscript 1 based on the findings of RQ1. This manuscript was submitted to the journal of *Communications of the Association for Information Systems*, a peer-reviewed journal ranking A, on 5 May 2024 and is currently undergoing a major revision.

Figure 1. 2

The position of Chapter 2 in the thesis



Chapter 2 Privacy in Smart Health Monitoring: A Systematic Literature Review (Manuscript 1)

2.1 Abstract

Privacy concerns related to surveillance technologies are a primary deterrent for consumers hesitant to share their health data with service providers in smart health monitoring systems (SHMSs). These concerns could impede the adoption and operational success of these systems, resulting in dissatisfaction among both consumers and service providers. Despite its importance, existing literature on SHMSs often provides a rather fragmented and limited exploration of contextualizing privacy, due to the complex nature of surveillance and multi-stakeholder involvement. To address the gap in comprehensively contextualizing privacy within SHMSs, this study develops a contextual framework derived from a systematic review of 49 peer-reviewed articles. This framework provides valuable insights for scholars aiming to understand the multifaceted privacy concerns in SHMS settings. Our findings can help both healthcare providers and policymakers in pinpointing and addressing potential privacy issues of personal health information when developing and implementing healthcare surveillance systems. Furthermore, the findings highlight existing knowledge gaps and suggest six targeted research avenues to achieve a more profound understanding of privacy within the realm of SHMSs.

Keywords: Privacy, Contextualization, Smart Health Monitoring, Stakeholders, Surveillance, Systematic Literature Review.

2.2 Introduction

Smart health monitoring systems (SHMSs) are modern personal health systems that employ real-time surveillance technologies and sensor-based smart health applications to monitor the vital signs and daily health status of their users (Alabdulatif et al., 2019; Almujally et al., 2023). These systems have seen significant growth in recent years due to their anticipated advantages, such as promoting communication between patients and doctors, improving diagnostic and treatment processes, reducing professional visit costs, and enhancing personal care quality (Akmandor & Jha, 2018; Greco et al., 2020). It is estimated that the global SHMS market, valued at USD 172 billion in 2023, will reach USD 474 billion by 2032 (GlobeNewswire, 2023; Market.Us, 2023). Yet, despite significant investments in SHMSs and the advantages they provide, the adoption of SHMSs by both consumers and health professionals continues to

be unsatisfactory for various reasons, such as resistance to change, infrastructure limitations, and a lack of standardization (Osama et al., 2023; Talwar et al., 2023).

Among the cited reasons for the slow adoption of SHMSs, privacy concerns stand out (Arbabi et al., 2022; Essén, 2008; Sovacool & Del Rio, 2020). Multiple global reports (e.g., Accenture.com, 2020; Capterra.com, 2021; Fortune.com, 2023; New Zealand IoT Alliance, 2017) point to consumers' privacy concerns related to the surveillance technologies embedded in SHMSs as the key reason preventing them from using health monitoring applications and sharing their health data with health professionals. These surveillance technologies include devices such as electrocardiogram ECG monitors and blood glucose wearables, which are essential to the efficacy of SHMSs (Rashidi & Mihailidis, 2013; Stavropoulos et al., 2020), but evoke confusion or uncertainty among SHMS consumers about who bears responsibility in the event of the loss of their health data, and how the proper protection and usage of this data within the surveillance framework can be guaranteed (Accenture.com, 2020; Duckert & Barkhuus, 2022; Princi & Krämer, 2020).

For scholars, the juxtaposition of the growth and potential of SHMSs with consumer concerns for privacy represents an intriguing phenomenon to research. However, while investigations into the impact of consumers' privacy concerns on their willingness to adopt and utilize SHMSs may seem appealing, the extant SHMS literature available to inform such work presents a rather limited and fractured perspective on privacy in the context of surveillance and monitoring. Contextualized privacy definitions are either absent or articulated poorly, and despite emphasizing the significance of privacy with respect to the adoption of SHMSs, researchers often encounter challenges in effectively communicating its meaning through clear definitions (e.g., Bhatt & Chakraborty, 2020; Dadhich et al., 2022; Peek et al., 2016; Ravishankar et al., 2015) and limiting the perspective of privacy to a single stakeholder. Unfortunately, weaknesses such as these create contextual ambiguity, which hampers researchers' abilities to set their studies' direction, choose theories, and interpret their findings (Dinev et al., 2013).

Privacy is a multidisciplinary concept (Smith et al., 2011), and privacy researchers in the general field of information systems (IS) have embraced diverse perspectives in defining and investigating various privacy issues for different purposes. For instance, privacy has been defined as a *right* of being alone from a legal perspective (Warren & Brandeis, 1890), as a *commodity* that can be traded for benefits in an economic sense (Campbell & Carlson, 2002; Smith et al., 2011), as a *control* over the acquisition and use of personal information, signifying an individual's ability to manage these aspects (Culnan & Bies, 2003), and as a *state* or

condition that indicates restricted access to personal information (Schoeman, 1984). This plurality of perspectives has served the IS discipline well, but in terms of understanding privacy as a byproduct concern of SHMS surveillance activities, prior researchers do not identify their perspective(s) of interest. As a result, the overall body of literature that informs SHMS privacy research seems incomplete.

Privacy is also a context-dependent concept (Smith et al., 2011). Contexts represent differentiated social spheres serving as organizing principles that shape individual expectations of privacy (Nissenbaum, 2018; Zuboff, 2015). Individuals strive to keep perceived private information private in accordance with the context (Bantan & Shawosh, 2024; Nissenbaum, 2010). SHMSs are complex health contexts due to their use of surveillance technologies and how stakeholders engage with them (Winter & Davidson, 2019). Such systems engage multiple stakeholders based on their interests across various disciplines, multiple levels, and toward multiple data domains (Ribeiro et al., 2019; Talal et al., 2019; Winter & Davidson, 2019). It could be argued that the more stakeholders (e.g., consumers, healthcare providers, government authorities, and smart technology providers) are involved (OECD, 2015; Peek et al., 2016; Swinkels et al., 2018), the more opportunities there are for privacy loss. The diversity of these stakeholders' views and their potential conflicting interests or concerns regarding privacy highlight the complexity of privacy concerns around SHMSs, considering different stakeholders' views could shape the development, implementation, and acceptance of SHMSs (Ismagilova et al., 2020). However, within the literature that has explored the contextual nuances pertaining to SHMS surveillance and stakeholder involvements, limited studies have explored both the perspectives on privacy and the contextual factors (antecedents or outcomes). For example, one study investigated the contextual factor with respect to individual customers' surveillance concerns about data privacy issues (Chadborn et al., 2019). Another study focused on the outcome of privacy on medical practitioners' attitudes toward adopting smart healthcare services (Pan et al., 2019).

Given its critical importance to scholars, we propose a contextual framework for SHMS privacy research that accommodates the diverse perspectives and contextual nuances of privacy in the context of SHMSs. This framework is developed using a systematic review of the IS literature to reveal an existing understanding of privacy that we then contextualize to the unique environment of SHMSs and its multiple stakeholder perspectives. The research question guiding our review process is:

> **RQ:** *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?*

Our framework for SHMS privacy research offers valuable insights to scholars interested in understanding the contextual nuances of privacy in SHMS settings. Additionally, we review a wide range of theories and methods applicable for research in this space. Our findings can also assist both healthcare providers and policymakers in addressing privacy issues surrounding personal health information when developing and implementing healthcare surveillance systems. Furthermore, our findings uncover existing knowledge gaps and identify potential research avenues for future investigation.

The remainder of this paper is organized as follows. We first set the stage for our review by discussing the importance of contextual clarity in IS research and the shortcomings of existing review articles in meeting this need. We then outline our systematic literature review methodology, including article selection and coding process. Finally, we present the findings, discussion of future implications, and concluding remarks.

2.3 Addressing the Incomplete Contextualization of Privacy in SHMSs

Over the past couple of decades, IS researchers have shifted their focus away from technology development and toward the social context surrounding the design and use of information technologies (Avgerou, 2019; Sidorova et al., 2008). This shift underscores the importance of contextualization in IS research, which involves identifying domains beyond the individual components of a central phenomenon (Renwick & Gleasure, 2021). These domains provide conditions that can either constrain or enable the formation of the phenomenon (Avgerou, 2019). Contextualization enriches our understanding of the subjects under investigation and unveils alternative interpretations of the phenomena from more insightful perspectives (Zahra et al., 2014). Ultimately, research remains incomplete unless there is a clear specification of the context for conducting the research and where the findings could be reasonably applicable (Davison & Martinsons, 2016). Contextualization also underscores the scope and boundaries of a concept within a specific research context (Mulligan et al., 2016; Solove, 2006). Knowledge construction stems from individuals experiencing the contextual situations in which their thoughts occur (Dewey, 1958). Beyond a contextualized definition with dynamic characteristics and various conceptual perspectives, contextualizing involves providing further explanations of a research phenomenon, theory, and findings in a given specific context or setting (Ravitch & Carl, 2019). It considers the influence of factors like time, place, culture, and social dynamics on the phenomenon under investigation (Avgerou, 2019; Xu & Zhang, 2022). In essence, contextualization is a foundational step that sets the stage for a deeper exploration.

Researchers have long been encouraged to provide a contextualized definition of their phenomena of interest, recognizing its pivotal role in setting the stage for how the phenomena

will be examined (Angel & Calo, 2023; Solove, 2002). For privacy concerns related to SHMS surveillance, a context-focused definition of privacy will help elucidate any abstract concepts and delineate the unique characteristics of privacy, accommodating a range of perspectives, whether convergent or divergent (Solove, 2002). SHMSs operate within intricate environments spanning various disciplines, values, and interests, and encompassing multiple data domains (Ribeiro et al., 2019; Talal et al., 2019; Winter & Davidson, 2019). To adequately contextualize privacy within SHMSs, it is essential to first develop a definition that incorporates diverse conceptual perspectives from various disciplines and use a broader lens (Locke & Golden-Biddle, 1997; Sandberg & Alvesson, 2011). Hence, to set the stage for our context-specific review of privacy within SHMSs, we begin by examining contextualized definitions of privacy.

The manner in which researchers contextualize privacy significantly influences their ability to predict outcomes and propose solutions (Smith et al., 2011; Solove, 2002). Moreover, context is important to theory development (Avgerou, 2019). Contextualization in privacy research can be utilized as a powerful sensitizing tool for illuminating the boundary conditions of privacy theories (Xu & Zhang, 2022). In simple terms, contextual richness is an essential way to help link research phenomena and build theory (Zahra, 2007). New theories are emerging and might not yet receive as much attention in new research themes, such as SHMSs (Zahra, 2007). Contextualization helps enrich the existing theoretical perspectives by creating opportunities for their potential integration, and even advancing new theoretical frameworks. Hence, we study contextual richness by examining antecedents and outcomes of privacy in SHMSs, as well as theories and methodologies utilized in the previous literature. Considering their contextual significance, our review also gives particular attention to surveillance and stakeholders to provide a complete picture of privacy contextualization within the smart health monitoring context.

2.3.1 Meta-review of the Extent of SHMS Privacy Review Articles

As part of this context-specific exploration, we first re-evaluated the existing review studies on privacy issues in the smart health monitoring context. These review articles were scoped using search terms related to ‘privacy’ and ‘smart health.’ In this meta-review, we identified that the review criteria (transparency and research agenda) were inadequately provided (see Appendix Table A. 1 in Chapter 2). Establishing criteria such as search strategy and formulating a research agenda are foundational elements of methodological transparency. They are essential for the advancement of knowledge in a particular research field and for maximizing research impact (Paré et al., 2016; G. Wagner et al., 2021). These reviews offer a valuable, but

limited avenue for obtaining insights from privacy phenomena in healthcare surveillance contexts.

Based on the synthesis of the existing reviews, the exploration of contextual privacy concerns is found to be incomplete. Only one review paper analyzed the privacy definitions in its study context (Shen et al., 2019), while all of the review papers neglected key perspectives of privacy (right, commodity, control, state). These review papers also lacked exploration of the underlying theoretical models and theories of the reviewed articles. Further, only a few papers reviewed antecedents and outcomes of privacy (Carver & Mackinnon, 2020), and only a limited set of papers discussed research agendas (e.g., Shen et al., 2019; Talal et al., 2019; Zaman et al., 2022). The meta-review findings strongly underscore the need for synthesizing partial perspectives to offer a comprehensive, integrative review, that addresses the above deficiencies in previous review studies, allowing researchers and stakeholders (e.g., practitioners) to derive a more informed interpretation and conclusion on privacy concerns related to SHMSs. The present review aims to rectify these significant shortcomings in the literature by providing a comprehensive review of privacy contextualization in SHMSs. It includes examining privacy definitions from various perspectives and reviewing antecedents and outcomes of privacy, relevant theories, methodological transparency, research agenda, and other pertinent scopes.

2.4 Review Method

A literature review helps address broad questions through a holistic review approach, providing a complete picture of the prevalence of research on a focal topic (Grant & Booth, 2009). It is “a form of secondary study that uses a well-defined methodology to identify, analyze and interpret all available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable” (Kitchenham & Charters, 2007, p. vi). It also ensures accuracy and impartiality in the search and retrieval process while supporting the development of future research guidelines or directions that professionals can use (Fernández-Alemán et al., 2013). To answer the research question posited in this review and identify directions for future research, we conducted a systematic literature review focusing on privacy in smart health monitoring studies. Completing a systematic literature review is an iterative process that depends on the quality and scope of the included studies (Moher et al., 2009). In the following two sections, we explain the search strategy and the process of screening and selecting studies based on the preferred reporting items for systematic review (PRISMA) guidelines (Moher et al., 2009).

2.4.1 Search Strategy

The present study focused on peer-reviewed journal articles and conference papers written in English. Given that the concept of smart health monitoring emerged in early 2000 (Meier et al., 2013; Pan et al., 2019), this study considered articles published between January 2000 and February 2024. The search utilized the databases of Scopus, Science Direct, JSTOR, IEEE Xplore, Emerald Insight, EBSCO-host, ACM Digital Library, and AIS eLibrary. Other sources, including PubMed and OVID, were also used to identify relevant articles. Using keywords aligned with our research question, the search primarily targeted articles related to 'privacy' and 'smart health.' Given the distinctive feature of smart health monitoring technology, we purposefully focused our search on the term 'surveillance.' However, 'surveillance' may be excessively restrictive since many articles can use alternative terms for surveillance such as 'monitor,' 'track,' or 'detect.' Thus, we also searched for 'monitor,' a widely used term, to find as many potential studies as possible. Generally, exclusion criteria for the studies were (1) non-empirical and not peer-reviewed, (2) non-full text, (3) irrelevant to the purpose of the review (e.g., paying limited attention to information privacy in smart health monitoring contexts, (4) technically focused, (5) duplicated, (6) and written in another language. Details of inclusion and exclusion criteria are presented in Table 2. 1.

Table 2. 1

Inclusion and exclusion criteria

	Inclusion criteria	Exclusion criteria
Language	English	Non-English
Full text availability	Full text	Non-full text
Source type	Empirical and peer reviewed	Non-empirical (e.g., review, conceptual, and editorial), book section, PhD thesis and dissertation
Subject area	A focus on privacy issues (mainly or partially) using a non-technical perspective	Less privacy exploration within technical focus
Type of system	Smart health, e.g., wearable healthcare, IoT-based smart homes, healthcare surveillance, etc.	Not smart health, e.g., self-monitoring application
Study setting	Health data	No health data
Participants	Individual users, healthcare professionals, government authorities, smart technology providers	Parties not contributing to the subject area
The findings of the study	Relevance to a better privacy understanding, in terms of definition, factors, or outcomes of privacy in the study setting	No relevant findings regarding a better privacy understanding in the study setting

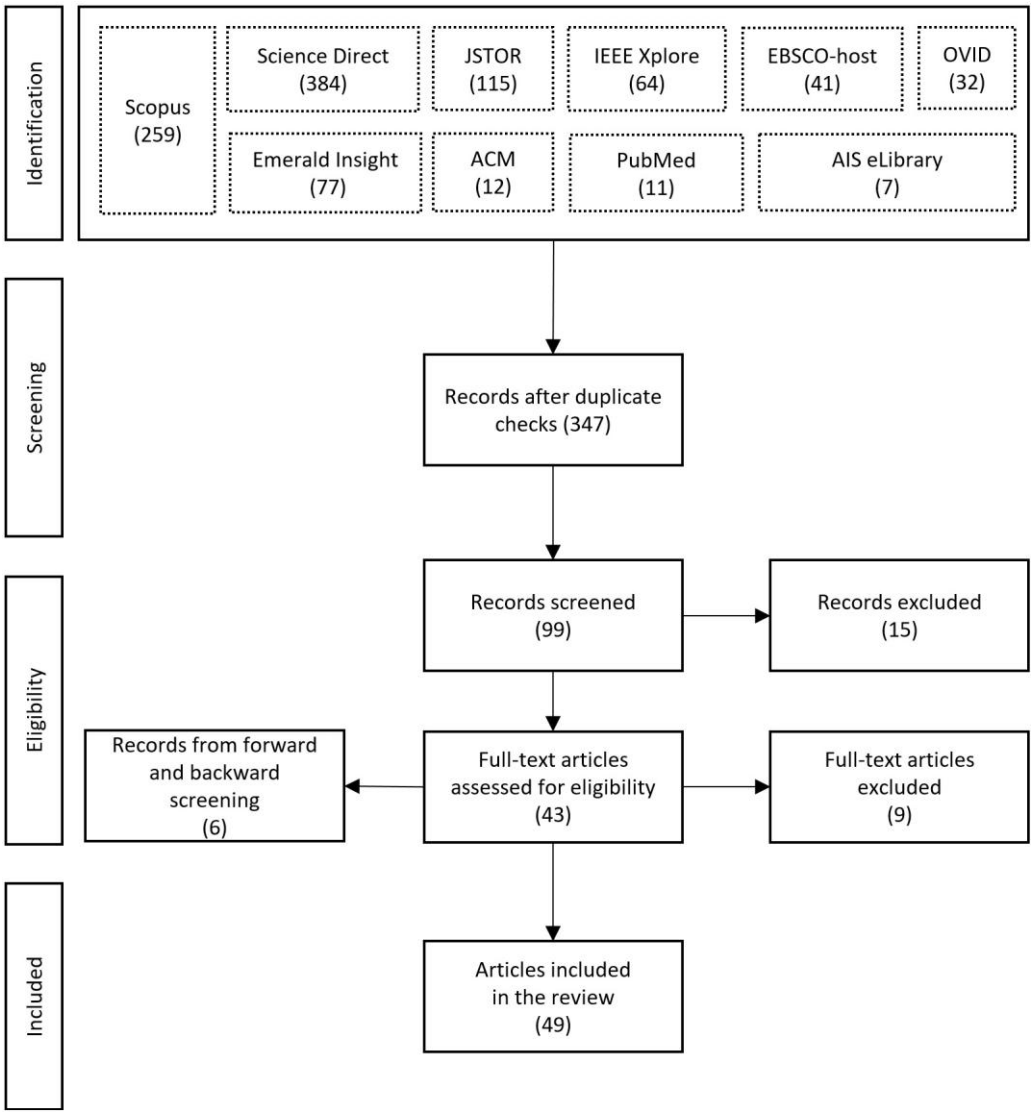
2.4.2 Study Selection

A review reporting guideline is essential in literature reviews as it helps modify the original review protocol and enables changes to be reported as appropriate throughout the process. Moreover, it can be used to mitigate the risk of overlooking any potentially eligible studies. Following the PRISMA guidelines (Moher et al., 2009), we conducted a four-phase process consisting of identification, screening, eligibility, and inclusion, as shown in Figure 2. 1. In the identification process, we initially found 364 records by searching for keywords in the database and 347 records remained after removing duplicates. Screening the title and abstract resulted in a preliminary list of 99 records. However, a few studies were excluded according to the inclusion and exclusion criteria. For instance, studies were removed if they included the search keywords but lacked a clear focus on privacy (e.g., Cristiano et al., 2022b; Grill et al., 2016; Rahman et al., 2022). Studies were also excluded if they only focused on technical aspects – for example, a study focusing on creating a system architecture for a sensor-based smart-health framework that can minimize privacy concerns (Rahman et al., 2022). In addition, articles were excluded if their main focus was not on smart health monitoring, for example, post-Covid public health surveillance (e.g., Seberger & Patil, 2021; Yang, 2022). In the eligibility process, articles in the preliminary list were further assessed with a full-text screen by applying the exclusion criteria, and 43 records were included accordingly. In the last process, six relevant studies were revealed through forward and backward searches of references in the

citations of included articles (Webster & Watson, 2002). A total of 49 records were obtained from a final examination separately conducted by this study's three authors.

Figure 2. 1

Four-phase study selection process guided by the PRISMA flow diagram



2.4.3 Data Collection Process and Coding

Data were extracted into a spreadsheet by the first author and verified by the other two authors. The first author completed the preliminary coding work using the inclusion and exclusion criteria. The other authors reviewed the coding work to ensure all conflicts and discrepancies were resolved. The codes were developed following the research questions. In preparation for addressing our research question, we coded definitions of privacy in smart health monitoring contexts and categorized them in the existing definitional perspectives, i.e., *privacy as a right* (Warren & Brandeis, 1890)*, a commodity to exchange* (Campbell & Carlson, 2002)*, an ability to control* (Culnan & Bies, 2003)*,* and *a state* (Schoeman, 1984). We then

coded privacy proxies, variables for the antecedents and outcomes, and sorted them into several categories by guiding the coding rules and the definitions from the previous literature. New codes for the antecedents and outcomes were developed when the existing categories of codes could not capture them. The results were analyzed based on the following themes: 1) whether the study highlighted surveillance issues; 2) how surveillance was described; 3) which stakeholder(s) was involved in the study; and 4) whether the study investigated more than one stakeholder. Then, the theories and methods used to identify the antecedents and outcomes were also coded.

2.5 Findings

In this section, we provide a general descriptive overview of the reviewed articles' characteristics, as well as our findings related to privacy definitions and contextualization, privacy-related proxies, antecedents, and privacy outcomes present in the reviewed articles. We also highlight key findings of the articles, particularly those concerning surveillance and stakeholder dynamics.

2.5.1 Overview of the Articles' Characteristics

In total, 49 articles on privacy and smart health were included in the review, covering the period from 2006 and 2024, as shown in Table 2. 2. Notably, 41% of these articles were published between 2021 and 2024. Studies in Asia-Pacific and European regions contributed to a significant portion of the published articles, compared to those coming from North America. Smart homes and smart wearables were the most commonly investigated systems. In terms of the study methods, the reviewed literature exhibited a nearly equal distribution between quantitative and qualitative studies. However, only a limited number of studies focused on a mixed-methods approach. Notably, 8 studies investigated multiple groups of stakeholders in relation to group-level analysis.

Table 2. 2

Summary of the articles' characteristics

Variable	Studies	Percentage
Year of publication		
2021-2024	20	41%
2017-2020	23	47%
2006-2016	6	12%
Source type		
Journal article	44	90%
Conference paper	5	10%
Region		
Asia-Pacific	18	37%
Europe	17	35%
North America	8	16%
Multiple countries	6	12%
Type of system		
Smart home	15	31%
Wearable	12	24%
MHealth/eHealth/remote health	11	22%
Smart health	8	16%
IoT	3	6%
Method		
Quantitative	23	47%
Qualitative	21	43%
Mixed methods	5	10%
Participant		
Consumers/patients/residents/users	37	76%
Multiple groups of stakeholders	8	16%
Healthcare providers	4	8%

Theories Used in the Published Articles

Generally, the technology acceptance model (TAM), the unified theory of acceptance and use of technology (UTAUT), and the privacy calculus theory (PCT) proved to be the most popular theories in the literature to explain both the antecedents and outcomes of privacy issues. However, not all the identified antecedents and outcomes were explained by theory. From the theories used to explain antecedents, six theories were applied to analyze the antecedents of privacy issues (see Appendix Table B. 1): the mobile users' information privacy concerns model (MUIPC), PCT, the theory of communicative action, categorization theory, the theory of contextual integrity (CI), and notions of borders. In contrast, theories employed in the outcome literature were more diverse than in the antecedent literature (see Appendix Table B. 2). In particular, multiple theories were found to aim at one outcome – such as the use of PCT and the theory of planned behavior (TPB) to predict subsequent actual behavior surrounding privacy concerns (Princi & Krämer, 2020) and the use of TAM, innovation diffusion theory (IDT), protection motivation theory (PMT), and PCT to explore behavior intention affected by perceived privacy risks (Karahoca et al., 2018). In turn, one theory (or a set of

theories) was used to identify multiple outcomes of privacy issues – for example, the use of TAM to identify outcomes of attitude toward adoption, perceived usefulness, and perceived ease of use (Papa et al., 2020), and the use of PCT and the concept of risk-risk trade-off as a set of theories to identify outcomes of perceived value and application usage (Tran & Nguyen, 2021).

Methods Used in the Published Articles

The reviewed literature was evenly split between quantitative and qualitative studies (see

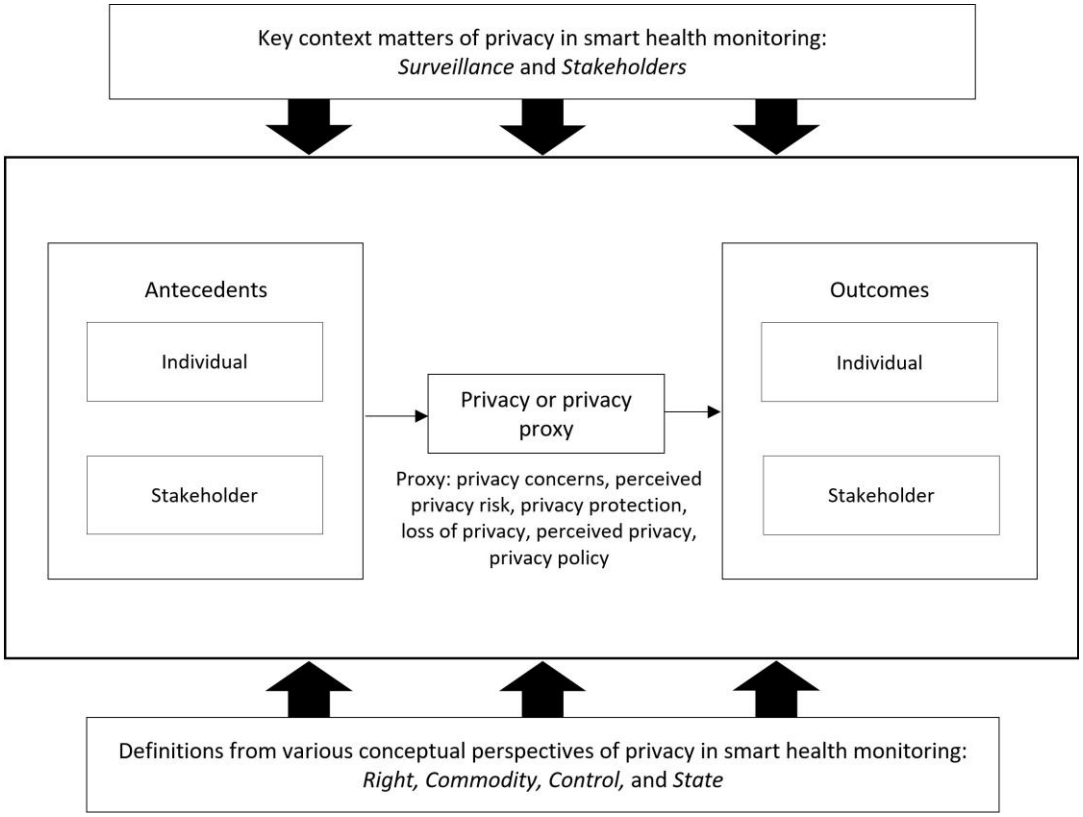
Appendix Table B. ***3***). However, only a small subset of studies employed a mixed methods approach. Almost all the quantitative studies were based on questionnaire survey methods (e.g., Liu & Tao, 2022), while two studies conducted experiments (Princi & Krämer, 2020; Seiferth & Schaarschmidt, 2020). Nearly half of the reviewed qualitative studies adopted the interview approach to address their research questions, while the focus group was the second most popular method used. A few qualitative studies employed the case study method. In addition, longitudinal studies, workshops, jury sessions, and qualitative surveys were other methods that could also be classified into the qualitative method category. In total, only five studies used a mixed-methods design. Mixed-methods research covers various types of purposes such as *developmental*, *diversity*, *completeness*, and so on (Venkatesh et al., 2016). To ensure that the questions from one strand could be used to develop hypotheses to be tested in the next (i.e., developmental purpose), two studies collected qualitative information before conducting quantitative surveys based on the qualitative findings (Cristiano et al., 2022a; Wiegard & Breitner, 2019). In order to obtain divergent views of the same phenomenon (i.e., diversity purpose), two other studies conducted surveys and interviews to analyze the preferences and needs of smart home technologies (Arar et al., 2021; Balta-Ozkan et al., 2013). To ensure a complete picture of a phenomenon (i.e., completeness purpose), one study involved a two-month feasibility assessment based on a questionnaire and interviews at three different time points to assess the initial perspectives of older adults on IoT smart home devices (Choi et al., 2020).

2.5.2 Thematic Analysis

A hybrid model is ideally suited for exploring events that prompt specific changes in outcomes or states. It enables a more comprehensive understanding and explanation within a specific IS field (Burton-Jones et al., 2015; de Guinea & Webster, 2017). Motivated by the notion of hybrid models and the antecedents–privacy concerns–outcomes (APCO) model of information privacy (Smith et al., 2011), we seek to develop a high-level contextual framework to present our synthesis results. The proposed framework is shown in Figure 2. 2. Our framework distinguishes between antecedents of privacy, privacy phenomena, and outcomes of privacy, leveraging a hybrid perspective. We understand that frameworks are typically introduced after the findings and discussions sections, reflecting emerging identifications. However, we present the framework upfront, aligning with the guidance of Suddaby (2006) and Pool et al. (2024). In doing so, the readers can be informed early on about the critical theoretical dimensions and impacts to be presented. In the following sections, our findings are structured and explained in accordance with this contextual framework.

Figure 2. 2

A contextual framework of privacy in smart health monitoring



2.5.3 Privacy Definitions and Contextualizations

Privacy is a multidisciplinary concept rooted in diverse justifications (Smith et al., 2011). Initially, it was framed as "the right to be let alone," acknowledging its legal value (Warren & Brandeis, 1890, p. 193). Economically, privacy is analyzed through cost-benefit lenses and trade-off principles and has been reconceptualized as a *commodity* (Campbell & Carlson, 2002; Smith et al., 2011). In social psychology, privacy in the work of Westin (1967) refers to "the ability of individuals to control the terms under which their personal information is acquired and used" (Culnan & Bies, 2003, p. 326). Philosophically, privacy is seen as a "state or condition" (Schoeman, 1984, p. 199), delineating limited access to personal information, intimacies, thoughts, or body (Schoeman, 1984).

Based on the knowledge above, we extracted the definitions of privacy in the literature from the main perspectives – *right*, *commodity*, *control*, and *state*. Out of 49 studies, only 17 studies (34%) explicitly defined or implicitly described privacy or privacy proxies (see Appendix Table B. 4). Among them, 12 (out of 17, 71%) viewed privacy as a *control*. For example, information privacy was defined as personal control over the unauthorized access, collection, and improper use of personal information in the mHealth application context (Tran & Nguyen, 2021, p. 3). Six studies (out of 17, 35%) viewed privacy as a *state*. For example, privacy risk was

interpreted as the possibility of information abuse, such as information theft and leakage when using mHealth services (Deng et al., 2018). Five studies (out of 17, 30%) were classified into privacy as a *commodity*. These studies employed the trade-off or risk-benefit concept to understand privacy and usage of smart health-related services. For example, the relationship between privacy concerns and the actual behavior of individuals when using an IoT healthcare device was examined from a privacy calculus perspective (Princi & Krämer, 2020). Only one study (out of 17, 6%) defined privacy as a *right* (Fritz et al., 2016). A further study was coded 'N/A' representing 'not applicable,' based on its suggestion that different people rate the importance of privacy differently for a myriad of reasons across a number of circumstances. Therefore, it was difficult to classify this study into any existing conceptual perspectives (Kennedy et al., 2021). Finally, it should be noted that across the studies that provided definitions, many considered using more than one conceptualized perspective to explain privacy. For example, privacy was characterized as both a *control* and a *commodity* in varied smart health contexts (Matt et al., 2019; Princi & Krämer, 2020; Tran & Nguyen, 2021; Wiegard & Breitner, 2019).

2.5.4 Proxies, Antecedents, and Outcomes

Privacy-related Proxies

Before discussing the antecedents and outcomes of privacy issues, we present a summary of the privacy proxies used in the literature. Nearly half of the studies (23 out of 49, 47%) did not use a proxy to investigate privacy (see Appendix Table B. 5). For example, privacy itself was reported as a significant issue when using IoT, among other factors in the healthcare system (Dadhich et al., 2022). Nine studies (out of 49, 18%) used privacy concerns as the proxy of privacy, and 7 studies (out of 49, 14%) used privacy risk (or perceived) as the proxy. In addition, privacy protection (3, out of 49, 6%), perceived risk (3, out of 49, 6%), loss of privacy (2, out of 49, 4%), perceived privacy (1, out of 49, 2%), and privacy policy (1, out of 49, 2%) were other proxies found in the literature. Three studies (out of 49, 6%) 'embedded' the privacy risk topic under the perceived risk variable (del Río-Lanza et al., 2020; Pan et al., 2019; Seiferth & Schaarschmidt, 2020). For instance, participants were asked about the perceived risk in terms of privacy risk, psychological risk, and financial risk (Seiferth & Schaarschmidt, 2020).

Antecedents of Privacy Issues

Our thematic analysis results identified 9 antecedents among 7 studies contributing to privacy issues in smart health monitoring environments, as shown in Table 3. We categorized them

into two categories: *individual* and *stakeholder* by consulting previous studies (Li, 2011; Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011).

Table 2. 3

Extracted antecedents and outcomes of privacy issues

Category	Constructs/Themes	Articles
Antecedents		
Individual	Perceived health information sensitivity	Wiegard and Breitner (2019)
	Surveillance concerns	Chadborn et al. (2019)
	Regulatory expectation	Wiegard and Breitner (2019)
	Individuals' trust in business operators	Shimizu et al. (2022)
	Cultural differences	Kulyk et al. (2020)
	Mobile users' information privacy concerns	Wiegard and Breitner (2019)
Stakeholder	Stakeholders' concerns about surveillance	Beaudin et al. (2006)
	Stakeholders' experience of using mHealth	Pan et al. (2019)
	Implementation of data mechanisms	Burrows et al. (2018)
Outcomes		
Individual	Adoption/use/participation	Alzahrani et al. (2021); Beaudin et al. (2006); Choi and Kim (2024); Fritz et al. (2016); Hassandoust, Johnston, et al. (2021); Sayibu et al. (2022); Tran and Nguyen (2021)
	Continuous use	Burrows et al. (2018); Matt et al. (2019)
	Intention to adopt/use	Arar et al. (2021); Bhatt and Chakraborty (2020); Choi et al. (2020); Dadhich et al. (2022); Deng et al. (2018); Esmaeilzadeh (2023); Karahoca et al. (2018); Li et al. (2021); Liu and Tao (2022); Lu et al. (2021); Mettler and Wulf (2020); Princi and Krämer (2020); Zhang et al. (2019); Zhu et al. (2022)
	Attitude toward adoption	del Río-Lanza et al. (2020); Ghorayeb et al. (2021); Kwiecień et al. (2020); Papa et al. (2020); Shimizu et al. (2022); Shimizu et al. (2021)
	Willingness to disclose/share data	Aljedaani et al. (2023); Kwiecień et al. (2020); Seiferth and Schaarschmidt (2020)

	Trust in smart technology/services	Deng et al. (2018); Liu and Tao (2022)
	Perceived value	Tran and Nguyen (2021); Wiegard and Breitner (2019)
	Perceived usefulness (of smart wearable healthcare)	Papa et al. (2020); Sayibu et al. (2022)
	Perceived ease of use (of smart wearable healthcare)	Papa et al. (2020)
	Feelings of health empowerment	Nelson et al. (2016)
Stakeholder	Attitudes to adopting smart healthcare services	Pan et al. (2019)
	Implementation of smart health services	Peek et al. (2016); Shimizu et al. (2022); Xing et al. (2021)
	Designing smart health systems	Cristiano et al. (2022a); LeBaron et al. (2020); Ravishankar et al. (2015)
	Stakeholders' use of wearable monitoring technology	Runkle et al. (2019)
	Smart home development	Balta-Ozkan et al. (2013); Kennedy et al. (2021); Kim et al. (2018); Suman (2017)

Individual-level antecedents encompass a category of factors primarily concerning the characteristics, attitudes, attributes, and behaviors of individuals regarding specific privacy issues in the smart health technology context (Dinev & Hart, 2004; Li, 2011; Xu, 2019). We found several antecedents relevant to the individual-level category: *perceived health information sensitivity* (Wiegard & Breitner, 2019), *surveillance concerns* (Chadborn et al., 2019), *regulatory expectation* (Wiegard & Breitner, 2019), *individuals' trust in business operators* (Shimizu et al., 2022), and *cultural differences* (Kulyk et al., 2020). Users' information privacy concerns are related to their personal disposition to privacy and have been operationalized as a general concern in previous studies (e.g., Malhotra et al., 2004; Xu, 2019). These studies suggest that individual users with a high degree of information privacy concern are likely to be high on risk beliefs. Likewise, *mobile users' information privacy concerns* was considered as a personal deposition to privacy and coded as an antecedent that directly influences the perceived privacy risks or uncertainties of mobile users in a health information monitoring context (Wiegard & Breitner, 2019). The degree of transparency regarding data collection, processing, and sharing mechanisms within SHMSs significantly influences users' trust and their subsequent privacy concerns (Awad & Krishnan, 2006; Esmaeilzadeh, 2019; Finch & Tene, 2014). This relationship is impacted by users' technological literacy, suggesting that enhancing transparency and educating users about SHMS technologies could mitigate privacy concerns (Esmaeilzadeh, 2019; Someh et al., 2019; Zhang et al., 2017). Thus, we suggest the following proposition:

Proposition 1a. *Technological transparency* can influence individuals' trust and privacy concerns in the context of smart health monitoring.

Individual-level antecedents encompass cultural factors that shape how individuals perceive privacy (Smith et al., 2011). For instance, Dinev et al. (2006) found that in Italy, privacy is often at risk due to the Italian penchant for conversation, which reduces the likelihood of keeping anything confidential, whether it's personal matters or business secrets. Similarly, *cultural differences* could account for differing decisions on whether to submit or share personal information at the individual level (Dinev et al., 2006). In the reviewed studies, cultural differences have been identified as an influential factor in privacy concerns analyzed at the individual level (Kulyk et al., 2020). Researchers have found that people from Southern European countries perceive data disclosure as a personal choice, while people from Eastern European countries feel forced to disclose personal data. Overall, cultural and societal norms toward health information privacy shape SHMS use (Li, 2011; Miltgen & Peyrat-Guillard, 2014). Cross-cultural differences in privacy expectations necessitate tailored SHMS privacy practices that align with local privacy norms and values, indicating a need for context-specific privacy management strategies. Thus, we suggest the following proposition:

Proposition 1b: Contextual privacy norms across cultures can influence individuals' privacy concerns in the context of smart health monitoring.

Stakeholder-level antecedents emphasize the ways in which a specific industry and its stakeholders utilize information, encompassing their actions and attitudes toward safeguarding personal data, which, if compromised, could erode personal privacy (Tallon, 2013). Antecedents in relation to stakeholders have been widely associated with organizational reputation, implementation of privacy policies, informativeness, and the trustworthiness of an organization, among others (Ioannou et al., 2020; Li, 2011; Miltgen & Peyrat-Guillard, 2014). In the existing literature, three stakeholder-level antecedents have been identified: *healthcare providers' concerns about surveillance* (Beaudin et al., 2006), *healthcare providers' experience of using mHealth* (Pan et al., 2019), and *implementation of data mechanisms* (Burrows et al., 2018).

In a study by Beaudin et al. (2006) from the perspective of *healthcare providers' concerns about surveillance*, various professionals such as general practitioners, nurses, caregivers, and social workers, who constitute an essential stakeholder group, expressed skepticism toward smart home monitoring due to their perceptions of privacy issues. Healthcare providers are aware that their involvement in health tracking or surveillance activities may evoke privacy concerns among individuals, such as patients fearing judgment from family or clinical

caregivers (Beaudin et al., 2006). Therefore, healthcare providers' concerns about the negative influence of surveillance technologies can be considered a crucial antecedent of privacy issues in SHMSs. Moreover, in a study by Pan et al. (2019), *healthcare providers' experience of using mHealth* (in terms of pleasant usage experience) has been found to negatively impact their perception of privacy risks associated with smart healthcare services, and positively affecting their intention to adopt these services. Additionally, studies have suggested that privacy issues and relevant challenges can result from the failure or lack of meaningful awareness in mechanisms implemented by various stakeholders (Burrows et al., 2018; Jakobi et al., 2019). We coded *implementation of data mechanisms* as another stakeholder-related antecedent because it is a powerful influencer that controls privacy by negotiating existing boundaries and borders (Burrows et al., 2018). The alignment (or misalignment) of privacy expectations among SHMS stakeholders (e.g., users, healthcare providers, technology providers, and regulators) plays a critical role in shaping the ecosystem's privacy landscape (Lyles et al., 2021; Windasari et al., 2021). Misalignments may lead to privacy tensions and breaches, suggesting that a collaborative approach to establishing shared privacy norms and expectations is critical for the success of SHMSs (Lyles et al., 2021). Thus, we suggest the following proposition:

Proposition 2: Stakeholder dynamics and privacy expectation alignment can influence individuals' privacy concerns in the context of smart health monitoring.

Outcomes of Privacy Issues

We identified 15 outcomes among 41 studies (91%), coded in *individual* and *stakeholder* related categories (as shown in Table 3 above).

Individual-related outcomes are the most noticeable impact of privacy issues and refer to individuals' subsequent behaviors and beliefs (Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011). This group of outcomes reflects the impact and relevance of privacy concerns on individual-level attitudes, perceptions, and behaviors in relation to smart health monitoring systems. These factors pertain specially to the outcomes related to the characteristics or actions of individual people rather than broader group outcomes. Many researchers have argued that privacy significantly impacts the adoption (e.g., Beaudin et al., 2006; Fritz et al., 2016) and continuous use of a healthcare-based smart service (e.g., Burrows et al., 2018; Matt et al., 2019). Additionally, instead of examining users' actual behavior when using or adopting a healthcare-based smart service, we found that a large number of studies examined users' intentions to use such services based on the theory of reasoned action (TRA), which suggests that behaviors match actual intentions (Fishbein & Ajzen, 1977; Smith et al., 2011). For instance, a study by Lu et al. (2021) found that perceived privacy risk was negatively related to

the intention to use smart healthcare devices. A few studies focused on the attitude toward adoption, such as accepting smart home technologies (Ghorayeb et al. 2021) and adopting smart wearable healthcare devices (Papa et al., 2020). Individuals' willingness to disclose or share their data was found to be another important outcome affected by the desire to preserve privacy (Kwiecień et al., 2020). Moreover, privacy was shown to have a negative association with individuals' trust in smart technology or services (Deng et al., 2018; Liu & Tao, 2022) and individuals' perception of the value of smart healthcare applications (Wiegard & Breitner, 2019).

We found that perceived privacy assurance, derived from effective privacy protection mechanisms and clear communication of these protections, fundamentally shapes users' engagement with SHMSs by influencing their adoption/use, continuous use, and intention to adopt/use (Bansal et al., 2015; Chalhoub et al., 2024; Xu et al., 2011). When users perceive strong privacy assurances, their trust in smart technologies/services increases, leading to a positive shift in their attitude toward adoption and a greater willingness to disclose/share data (Bansal et al., 2015; Chalhoub et al., 2021). Furthermore, perceived privacy assurances enhance the perceived value and usefulness of smart wearable healthcare technologies, making them more appealing for adoption. This comprehensive impact of perceived privacy assurance on individual-level factors highlights the critical need for SHMS developers and policymakers to prioritize privacy as a core component of technology design and user communication strategies, thereby enhancing user engagement and empowerment in managing their health. Thus, we suggest the following proposition:

Proposition 3: The integral role of perceived privacy assurance can result in shaping user engagement and trust in SHMSs.

Stakeholder-related outcomes refer to outcomes or consequences that are relevant to the key stakeholders involved in the caused privacy issues of the smart health technologies over a broad range, covering economic, social, and environmental aspects from the stakeholders' collective perspective (Ruhlandt, 2018; Valle-Cruz, 2019). In addition to *individuals* (e.g., patients and users), the key stakeholders of smart health monitoring systems often include *healthcare providers*, *smart technology providers*, and *government authorities* (OECD, 2015; Peek et al., 2016; Swinkels et al., 2018). According to our review results, stakeholder-related (non-individual stakeholders) outcomes in the context of smart health monitoring include *stakeholders' attitudes to adopting smart healthcare services* (Pan et al., 2019), *implementation of smart health services* (e.g., Peek et al., 2016), *designing smart health systems* (e.g., Cristiano et al., 2022a), *stakeholders' use of wearable monitoring technology*

(e.g., Runkle et al., 2019), and the overall *smart home development* driven by multiple stakeholders (e.g., Kennedy et al., 2021).

Effective stakeholder collaboration in the design, implementation, and promotion of SHMSs acts as a critical catalyst for overcoming privacy concerns, fostering innovation, and enhancing the adoption and continuous use of these technologies (Thiebes et al., 2023; Ullah et al., 2021). Integration of diverse stakeholder perspectives – including those of healthcare providers, technology developers, users, and regulatory bodies – into the development and governance of SHMSs leads to more privacy-centric designs and policies (Miyachi & Mackey, 2021; Ullah et al., 2021). Such collaborative efforts result in smart health services and wearable technologies that are not only more aligned with end-user privacy expectations but also with the operational and ethical standards of healthcare providers and the regulatory frameworks of government authorities (Renwick & Gleasure, 2021). This integrated approach facilitates the creation of SHMSs that are perceived as more trustworthy and valuable by all stakeholders, thereby improving attitudes toward adoption, enabling smoother implementation processes, promoting more innovative system designs, and ultimately driving the development of smart homes and healthcare environments that are both technologically advanced and privacy-respecting. Therefore, we suggest the following proposition:

Proposition 4: Stakeholder collaboration can be a catalyst for privacy-centric SHMS innovation and adoption.

2.5.5 A Matter of Context

Privacy is a context-dependent phenomenon. The term ‘context’ means the surroundings associated with phenomena existing in the environment external to individuals, most often requiring different levels of analysis (Cappelli, 1991; Mowday & Sutton, 1993; Smith et al., 2011). In IS research, the most commonly cited contexts for privacy are related to *technological applications*, *the use of information by sector*, *the type of information* collected from individuals, and *the political context* (Smith et al., 2011). Given that the type of information is well acknowledged in the smart health monitoring context and political contexts can be emotionally charged through the presentation of authors’ beliefs in different causes (Smith et al., 2011), our review work emphasizes surveillance and stakeholder matters to compile a full picture of privacy contextualization in the smart health monitoring context.

Surveillance involves any gathering and processing of personal data in order to manage or influence those whose data have been collected (Fox, Clohessy, et al., 2021). To review the extent to which the effectiveness of surveillance technologies was addressed in the included

studies, we extracted the keywords describing the surveillance phenomenon and synthesized these into three groups – *Highlight*, *Mention*, and *Not mention* (see Appendix Table B. 6). Most studies came under the *Highlight* group, which strongly suggested the perception of a surveillance or monitoring phenomenon in the evaluation of privacy in a smart healthcare context. For example, Choi et al. (2020) investigated the effect of potential privacy risks deterring individual users from choosing different types of monitoring devices. Studies in the *Mention* group only briefly referred to surveillance issues and provided no explanations or discussions. For example, some researchers mentioned constant monitoring as a kind of surveillance with several negative implications (Kim et al., 2018). Studies in the *Not mention* group did not consider or discuss surveillance issues at all. Among the identified keywords, *monitoring* (e.g., (Chadborn et al., 2019; Choi et al., 2020) and *tracking* (e.g., (Beaudin et al., 2006; Li et al., 2021) had widespread use in the majority of studies when referring to surveillance issues. A few studies used *intrusiveness* (e.g., (Etemad-Sajadi & Dos Santos, 2019) and *intervention* (e.g., (Fritz et al., 2016; Shimizu et al., 2022) to explain the negative feelings related to monitoring or surveillance activities. Notably, some studies also explored the surveillance effectiveness of different monitoring devices – the *video camera* was ranked first with the highest negative effect (Arar et al., 2021; Balta-Ozkan et al., 2013).

Stakeholders are defined as any group or individual "who can affect or is affected by the organization's purpose" (Freeman et al., 2010, p. 93). The key stakeholders of smart health monitoring systems often include *individuals* (e.g., patients and customers), *healthcare providers*, *smart technology providers*, and *government authorities* (OECD, 2015; Peek et al., 2016; Swinkels et al., 2018). Stakeholders play a key role in the implementation of privacy protection concerning smart services. In this study, stakeholder context was reviewed according to 1) whether a study investigated multiple stakeholders, and 2) which stakeholder(s) was included. A limited number of studies explored privacy issues in the context of multiple stakeholders (e.g., Peek et al., 2016), compared to a distinct group of studies focusing on one single stakeholder (either an individual user or healthcare professional), as shown in Appendix Table B. 7. In multi-stakeholders studies, privacy was reported as not a large concern for some groups of stakeholders (e.g., older adults or rest home managers) but much more important to other groups of stakeholders (e.g., technology developers) (Alzahrani et al., 2021). This means that different stakeholders may have different beliefs regarding privacy concerns. The importance of multi-stakeholders was also highlighted and discussed in some single stakeholder-focused studies from the perspective of individuals (Chadborn et al., 2019; Chen et al., 2021; del Río-Lanza et al., 2020; Hunter et al., 2020; Ravishankar et al., 2015; Suman, 2017). For instance, individual stakeholders were identified as being frequently

ignored by organizations due to the divergence of goals between individuals and other stakeholders (Chadborn et al., 2019).

2.6 Discussion

In this section, we present our discussion on privacy definitions and contextualizations, antecedents and outcomes, along with the implications and limitations of our research by leveraging the contextual framework in Figure 2 as our guiding structure. Furthermore, our discussion extends to encompass the diverse theories, methodologies, and contextual nuances that collectively paint a comprehensive portrait of privacy contextualization within the existing scholarly landscape.

Privacy definitions and contextualizations: The review findings reveal that privacy definitions were insufficiently expressed or incorporated by privacy and smart health monitoring studies. While some studies discussed different perspectives of privacy such as viewing it as a *right*, *commodity*, *control*, and *state* (see Appendix Table B. 4), a consistent and sufficient definition of privacy from these diverse conceptual perspectives was generally underdeveloped. We identified three implications for future researchers to consider. First, clarifying the contextualized definition of privacy from one or multiple perspectives can enrich our understanding of privacy within multidisciplinary environments like smart health monitoring. This clarification will aid researchers in delineating the focus of their studies and selecting appropriate theoretical frameworks and theories. For instance, if the study focuses on viewing privacy as a *commodity* or something of value, trade-off theories like privacy calculus can be employed (e.g., Matt et al., 2019; A. Wagner et al., 2021). In light of the *state* perspective, theories like Balance theory can be utilized to explore if a state is either balanced or imbalanced toward a triadic-relationship system of privacy, consumer, and health insurance providers. Second, a chosen perspective can facilitate researchers in adopting existing measurement items from other studies which also use the same perspective. For example, Princi and Krämer (2020) employed measurement items from Smith et al. (1996) as both studies hold a *control* perspective on privacy. Third, privacy is not a one-size-fits-all concept: it changes based on the situation and individuals' experiences, especially in complex systems like smart health monitoring (Pang et al., 2020; Solove, 2007). Privacy is multidimensional and varies with context, which is ever-changing due to the various life experience of individuals (Altman, 1977; Laufer & Wolfe, 1977; Xu et al., 2011). Though this complexity can make defining privacy challenging, it is both fundamental and essential for advancing research in this field as it helps to support knowledge accumulation and progress in the smart health monitoring area (Gruber, 1995). Thus, combining different perspectives helps liberate our

understanding of privacy across different disciplines and levels in complex environments like SHMSs. For example, Matt et al. (2019) explored how people's control over their data affects their willingness to use health monitoring devices, and then looked at the cost-benefit aspect of privacy and functionality in continuous usage. Several additional instances (i.e., Princi & Krämer, 2020; Tran & Nguyen, 2021; Wiegard & Breitner, 2019) in the reviewed literature showcased the integration of multiple perspectives to comprehend the privacy phenomena.

Proxies, antecedents, and outcomes: The review findings suggest that proxies, antecedents, and outcomes related to privacy in smart health monitoring are lacking and underdeveloped. This highlights the need for further exploration of privacy and its interplay with other concepts through a measurable framework. Given the difficulty of measuring privacy, a great deal of empirical privacy research in the social sciences has relied on a privacy-related proxy as the central construct to measure privacy and explore its relationships with the antecedents and outcomes of that proxy (Smith et al., 2011). A proxy is highly recommended because measuring relationships depend on people's perceptions and cognitions rather than their rational assessments. Several researchers highlighted the importance of examining privacy beyond privacy concerns, as privacy concerns may have a negative connotation and do not straightforwardly represent privacy (Dinev et al., 2013; Fox, van der Werff, et al., 2021). Moreover, privacy can be investigated by involving more than one proxy. For instance, Wiegard and Breitner (2019) studied the relationship between mobile users' information privacy concerns and perceived privacy risks. In sum, there is a need for a more precise measurement of privacy that should be carefully matched with the research context to further advance the literature (Stewart & Segars, 2002).

Antecedents are factors that influence the shaping of privacy issues (Ozdemir et al., 2017; Xu et al., 2011). A lack of knowledge of influential factors could result in an incomplete understanding of the privacy issue, hampering the delivery of appropriate privacy protection in smart health monitoring. Several antecedents were explored in the reviewed literature in terms of different levels (individual and stakeholder). However, the majority of the explorations were at the individual level but with very little antecedent analysis at the stakeholder or other levels. Privacy is of growing concern when involving multiple stakeholders (Smith et al., 2011). The introduction of smart healthcare services can often generate resistance from service providers (e.g., clinicians) when adopting the services (Pan et al., 2019). Thus, antecedents should be studied deeply from the stakeholder perspective (Smith et al., 2011). Moreover, despite the identification of *cultural differences* (Kulyk et al., 2020) as an important societal-level antecedent, our review analysis found that the antecedents from other levels such as societal, environmental, cross-cultural, or national levels, were seldom

explored. Due to their significant impact on individuals' information privacy, the antecedents from these under-researched levels should be effectively addressed in future empirical studies. Furthermore, our review findings indicate that a large fund of knowledge has been gained from considering individual users' perceptions of privacy issues. However, a small number of stakeholder-level studies also evaluated perceptions of individuals who offered healthcare professional service through smart devices (e.g., Pan et al., 2019). Interestingly, perceptions of customers' privacy risks were also shown to exist among other stakeholders who sought to limit individuals' use of smart health monitoring applications (Galanxhi-Janaqi & Nah, 2004). For example, a perception of privacy-related risk was found to negatively impact doctors' personal attitudes toward using smart healthcare services, which could eventually affect the implementation of the service (Pan et al., 2019). Thus, privacy researchers should be cautious as focusing solely on the perceptions of individual customers may introduce bias and overlook the perspectives and experiences of other individuals (aside from customers), consequently failing to identify group-level privacy issues (Bélanger & Crossler, 2011).

Outcomes have been frequently linked to a specific privacy phenomenon in the reviewed studies. Indeed, without considering the outcomes, it is difficult to determine how important dealing with privacy truly is (Phelps et al., 2001). Smart health monitoring systems strive to generate co-created outcomes of value for both the individual users and the community at large (Janamian et al., 2016; Ramaswamy & Ozcan, 2014). Regarding the outcomes for individual users, the results of the reviewed literature showed a great interest in measuring intentions or attitudes toward the usage or adoption of smart health systems while neglecting actual behaviors. Although the theory of reasoned action (TRA) suggests that behaviors will match actual intentions, it should be cautioned that the relationship between privacy and stated intentions does not always reflect actual behaviors (Smith et al., 2011). Future studies could target actual behaviors and thoroughly investigate contextual factors that may predict those behaviors (Plangger & Montecchi, 2020).

Moreover, smart health monitoring systems involve collaborative healthcare service communities (Alabdulatif et al., 2019; Deloitte, 2019), in which stakeholders who work together using shared health data generate value for individual customers and share this value among stakeholders (Vargo et al., 2008; Winter & Davidson, 2019). It is important to explore the behavioral outcomes at the stakeholder level, for example, stakeholders' attitudes (e.g., Pan et al., 2019) and their use of smart health systems (e.g., Runkle et al., 2019). Additionally, exploring organizational and regulatory outcomes is essential for organizations and policymakers to effectively manage privacy issues in SHMSs (Manyika et al., 2011; Winter & Davidson, 2022). For example, understanding how privacy influences practices fosters trust

between organizations and users (Esmaeilzadeh, 2019; Liu & Tao, 2022). This enables organizations to identify innovation opportunities and develop new products, services, and processes that prioritize privacy and security (Xu, 2019). Companies that demonstrate a strong commitment to privacy can gain a competitive advantage by attracting privacy-conscious customers and partners (Smith et al., 2011). By emphasizing the regulatory outcomes influenced by privacy concerns, companies can ensure compliance with relevant laws and regulations, avoiding costly penalties and legal actions (Esmaeilzadeh, 2019). On the other hand, policymakers rely on research and evidence to inform the development of laws and regulations related to privacy and data protection (Solove, 2006; Someh et al., 2019).

Theories: Overall, the reviewed literature exhibits a significant deficiency in the application of theory. However, this absence of relevant theories raises questions about the validity and value of the research (Sutton & Staw, 1995). A theory is a linguistic device used to parsimoniously organize and clearly communicate concepts in a complex empirical world (Bacharach, 1989). It helps explain underlying processes and provides an understanding of the systematic reasons for a specific occurrence or non-occurrence (Sutton & Staw, 1995). Therefore, it is important to use an appropriate theory or (theories) to solidify the research motivations and assumptions when examining privacy-related constructs. Prior studies have commonly employed theoretical frameworks like TAM, UTAUT, and UTAUT 2 to understand how people adopt and use health information technologies. However, these models have faced criticism for being overly simplistic and limited. They concentrate solely on individuals' perceptions and intentions to use technologies, lacking specificity to the health domain (Lee et al., 2003; Shachak et al., 2019). Some researchers have also argued that the contributions of those frameworks to knowledge in this area have reached a plateau (Rouidi et al., 2022; Shachak et al., 2019). Moreover, the review of the research found that one of the key barriers to the successful implementation of digital health devices is both their low level of acceptance and resistance by healthcare professionals (Cilliers & Flowerday, 2014; Pan et al., 2019; Rouidi et al., 2022).

Methods: The application of a mixed-methods design was quite limited in the literature. However, this method provides an opportunity to develop fresh theoretical perspectives by combining the strengths of qualitative and quantitative methods (Venkatesh et al., 2016). Moreover, a mixed methods design is particularly useful because it helps provide a holistic understanding of a phenomenon at an early research stage (Venkatesh et al., 2013). The nature of the healthcare context frequently changes and involves contextually relevant challenges (such as the technological complexity associated with users) (Califf et al., 2020).

Thus, using the mixed-methods design is appropriate to better explore the underlying layers of privacy issues in healthcare-related domains (Califf et al., 2020; Fox & James, 2021).

Context matters: Context matters are dynamic forces and factors embedded within an entity and have been used as important predictors to measure a proposed relationship in an entity (Edwards & Steins, 1999; Shah & Ward, 2003; Shalley et al., 2004). Since these forces span multiple levels that are not relevant to a user (or a user group) (Kaplan et al., 2010; Shalley et al., 2004), several attempts were made by privacy researchers to distinguish contextual factors from other sets of factors (such as individual factors and macro factors) (Li, 2014; Miltgen & Peyrat-Guillard, 2014; Ozdemir et al., 2017). Surveillance was also an important theme in the literature review, with many studies highlighting the influence of surveillance in the smart health system. However, research on influencing factors stemming from surveillance has yet to be developed. The range of topics explored in the literature review was narrow and straightforward. For example, a large number of studies focused on the participants' acceptance of a surveillance device installed in their homes. Researchers who focus on surveillance as a matter of context should employ a measurable predictor to more deeply understand how privacy is affected by surveillance. Regarding stakeholders, only a small portion of the research in the reviewed literature focused on entities beyond individual users. The resistance of healthcare professionals to smart health systems due to their privacy concerns could be a key barrier to the successful implementation of digital health (Pan et al., 2019). Smart health monitoring can be seen as a dynamic community relying on multi stakeholders. Thus, unlike personal devices, the success of a smart health service hinges on the cooperation of multiple stakeholders, not merely on individuals' usage. It is recommended to shift research attention to the stakeholder level by evaluating contextual factors related to the context of collaborative stakeholders.

2.6.1 Implications for Stakeholders and Practice

Implementing privacy protection in smart monitoring services is challenging due to the intricate network of stakeholders and their diverse protection mechanisms. The participation of various stakeholders has been found to provoke privacy issues among individuals, serving as a significant antecedent factor and outcome of privacy. This review has emphasized four key stakeholders of smart health monitoring systems.

Individuals: Individuals include any end-users of smart health applications. In the dynamic environment of smart health monitoring, where collaboration among stakeholders is paramount, it is crucial for individual users to recognize themselves not only as beneficiaries but also as vital stakeholders, given their active involvement. Individuals' perceptions of

privacy and surveillance concerns are found to block them from using health monitoring technologies and sharing their health data with other stakeholders in smart health monitoring systems. However, individuals should understand the duality of privacy and surveillance in smart health monitoring applications. Smart health monitoring systems and surveillance technologies are forming new contexts of health data flow. In complex environments like this, multiple stakeholders naturally interact and collaborate across different disciplines and levels, working across various data domains to ensure individuals receive healthcare benefits. Hence, individuals should acknowledge the dual nature of privacy and surveillance in smart health monitoring systems and actively engage in smart health monitoring services in order to empower their health through the system.

Healthcare providers: Stakeholders in this category refer to clinicians such as doctors and nurses, caregivers, volunteers, and emergency personnel, among others, and involve healthcare facilities ranging from hospitals and health systems, ambulatory surgery centers, long-term care facilities, home health agencies, ancillary providers, to community group homes. The adoption of smart health monitoring technologies can offer advantages to healthcare providers, including enhanced operational efficiency, cost reductions in patient care delivery, improved quality measurement, and expanded reporting capabilities. However, concerns about privacy and associated challenges may arise if healthcare providers encounter difficulties in implementing effective data governance mechanisms or if there is a lack of meaningful awareness among this group of stakeholders. Data governance in healthcare services has been given significant prominence in recent years, based on its aim to maximize the value of data assets and manage data-related risks in the system. Since data governance can diffuse tension in terms of privacy and data sharing, mitigate risks, and balance interests within the multidisciplinary contexts of data sharing, healthcare providers should develop data governance mechanisms for their privacy activities.

Smart technology providers: Smart technology providers often encompass developers, vendors, and suppliers who focus on providing and maintaining smart health devices, service apps, and smart health monitoring service platforms by means of various information and communication technologies (ICTs), including sensing and surveillance. These technology providers are at the forefront in introducing surveillance technologies in smart health monitoring applications. Privacy issues have been demonstrated to influence the design, strategies, and development of functionalities within smart health systems when considered from a design thinking lens. There is a significant amount of literature on privacy-focused technologies in smart health monitoring applications. However, there is relatively little research that delves into the negative impacts of privacy concerns on smart technology

providers. Therefore, it is imperative for smart technology providers to have a thorough understanding of the privacy concerns associated with their technologies due to the key considerations discussed below. Technology providers have an ethical responsibility to protect the privacy and confidentiality of users' health data. Adhering to privacy regulations and laws is crucial for smart technology providers to avoid legal repercussions. Mishandling of privacy issues can lead to negative publicity and damage the reputation of developers and providers. By prioritizing privacy and implementing robust data protection measures, they can protect the brand reputation of technology providers.

Government authorities: Governmental authorities include government agencies, policy makers, and legislators that help achieve better data governance among stakeholders. Only a few of the reviewed studies investigated the efforts of government authorities regarding the privacy issues of smart health monitoring. However, antecedents, including individual-level *regulatory expectation* and *trust in business operators* and stakeholder-level *health tracking data mechanisms*, are all associated with the active involvement of government authorities. Moreover, smart health initiatives, like the development of smart homes, are intricately linked with the overarching objective of smart city development pursued by local government authorities. Therefore, it is imperative for government bodies to prioritize the management of individuals' privacy concerns by enhancing regulatory frameworks and fostering collaboration with other stakeholders involved in these systems.

2.6.2 Recommendations for Future Research Avenues

Based on the review of the existing literature, our study provides six research avenues along with a number of research questions for future research.

Avenue 1 – Contextualized definition: Clarifying the contextual and dynamic nature of privacy through a clarified definition is a pragmatic approach for accurately grasping and analyzing privacy issues (Solove, 2002; Xu & Bélanger, 2013; Zhang et al., 2017). A definition is essential as it serves as a foundational principle for facilitating transparent communication and fostering a coherent understanding of privacy (Dinev et al., 2013). Without a precise and consistent understanding, there is a risk of fragmented and ambiguous interpretations of privacy (Dinev et al., 2013). Despite its importance, the definition of privacy within the context of smart health monitoring remains underdeveloped in the literature. To fulfil the contextualized definition of privacy, researchers could answer the following research questions:

1. Privacy holds diverse interpretations. How do researchers define it pragmatically?
2. How has privacy been characterized in SHMSs?

Avenue 2 – Multi-level analysis: In general, multi-level research involves exploring phenomena at different levels of analysis, including individuals, groups, organizations, and communities (Blakely & Woodward, 2000; Smith et al., 2011). The community level, in particular, has garnered significant attention due to the advancements in remotely delivered virtual healthcare ecosystems (Schiavone et al., 2021). Multi-level research is essential for mapping a complete picture of privacy conceptualization and crucial for the mechanisms and reasons behind the occurrence of the privacy phenomenon (Ancona et al., 2001). The debate surrounding privacy conceptualization is fueled by complexity across various levels (Mulligan et al., 2016). However, our review shows that the existing literature has provided insufficient analysis across various levels regarding the antecedents and outcomes of privacy phenomena in smart health monitoring contexts. analysis Rather than solely focusing on individuals' perceptions, researchers can utilize our proposed framework to broaden their investigation at multiple levels in their forthcoming empirical studies. To conduct a multi-level analysis, researchers could explore the following research questions:

1. How do individual characteristics, organizational practices, stakeholder dynamics, and societal influences interact to shape privacy conceptualizations in the context of smart health monitoring technologies?
2. What are the key factors at the individual, organizational, stakeholder, societal, and technological levels that contribute to enhancing user acceptance of privacy features in SHMSs?

Avenue 3 – Methods of analysis: Future researchers are encouraged to use a mixed-methods design rather than using a single method in order to comprehensively investigate the privacy dynamic in the context of smart health monitoring. They are advised to explicitly delineate and/or recognize the purposes of their mixed-methods design, which could help readers better grasp the goals and outcomes of their mixed methods research papers (Venkatesh et al., 2013). To achieve this, it is critical to be aware of the exact nature of mixed-methods designs and the wide range of purposes for using a mixed-methods approach (Venkatesh et al., 2013; Venkatesh et al., 2016). Several purposes (i.e., *developmental*, *diversity,* and *completeness*) appeared in the reviewed literature. Other purposes and examples (such as *complementarity*, *expansion*, *corroboration/confirmation*, and *compensation*) can be found in the work of Venkatesh et al. (2013). In addition, meta-inferences are narratives, theoretical statements, or a story inferred from an integration of findings from qualitative and quantitative and strands of mixed methods research. Meta-inferences are considered important components of mixed-methods research (Venkatesh et al., 2013). It is hard to define a research program as truly being mixed-methods research unless it provides combining

findings from both qualitative and quantitative studies (Venkatesh et al., 2013). Thus, researchers using mixed-methods designs should offer an explicit discussion of meta-inferences. There are further potential research questions to explore as presented below:

1. How do ethnographic studies illuminate the nuances of privacy concerns in relation to smart health monitoring technologies, and how can these insights inform the development of more robust privacy policies and practices?
2. What do rich qualitative interviews with stakeholders tell us about the organizational policies, procedures, and cultural norms surrounding privacy issues in the context of SHMSs?
3. To what extent do methodological biases in sample selection impact the validity and generalizability of research on privacy issues in SHMSs, and what strategies can be employed to mitigate these biases?

Avenue 4 – Stakeholder analysis: Future studies can concentrate on analyzing multi-stakeholder engagement, delving into the stakeholders' ecosystem for privacy protection management in smart health monitoring. True cooperation among stakeholders was argued to be far from reality in terms of users' active participation in advanced health systems (Suman, 2017). Individuals do not feel encouraged to use smart health devices (or services) to share health data because of their surveillance and privacy concerns stemming from inadequate cooperation amongst stakeholders. Researchers are recommended to deepen stakeholder-specific investigations in response to an insufficient analysis of stakeholders in the literature. The investigation should also provide a clear description of the categories or types of stakeholders involved in the context. An investigation of multiple stakeholders would help to mitigate health data privacy concerns and allow users to regain control (Chadborn et al., 2019). Possible research questions include the following:

1. How do the diverse values and objectives of stakeholders in SHMSs contribute to the effectiveness of implementing data privacy mechanisms?
2. How can value co-creation strategies be employed within the stakeholder ecosystem of SHMSs to address privacy concerns and enhance user engagement and empowerment?

Avenue 5 – Contributing to the IS theories: A theory is viewed as a system that logically connects its key components through propositions or hypotheses (Bacharach, 1989). It serves to elucidate the relationships between phenomena by emphasizing causal connections and determining the sequencing and timing of such phenomena (Sutton & Staw, 1995). The significance of theory in IS lies in its ability to explain the what, why, and/or how of

phenomena (Mueller & Urbach, 2017). However, our review findings reveal a significant dearth in the application of theory, with an overreliance on TAM- or UTAUT-related models. Despite their prevalence, TAM and its related models have faced criticism for oversimplifying the system usage context and adopting a narrow viewpoint (Shachak et al., 2019). Given the intricate nature of privacy issues within smart health contexts, this oversimplification has become more pronounced. To contribute to IS theories and overcome the limitations of the current literature, future researchers could derive significant value from incorporating more influential theories and embracing a broader perspective that effectively addresses the complexity of smart health contexts. Rather than prescribing specific theories, we encourage scholars to consider theoretical pluralism and adopt theories that go beyond offering simple causal explanations. That is, scholars can consider dynamic and longitudinal perspectives using process theories/models and stage theories. In the IS field, process theories focus on the dynamic and temporal aspects of phenomena, which explain how specific outcomes are gained through a series of actions or events (Markus & Robey, 1988). For instance, health empowerment theory emphasizes the ongoing process through which individuals gain control over their health and health-related activities in a broader sense, i.e., a professional community (Rissel, 1994; Spreitzer, 1995). It involves a series of activities and interactions that result in greater health empowerment within the community. Diffusion of innovations theory highlights that diffusion is the process by which an innovation is transmitted through specific channels over time among the members of a social system (Rogers, 2003; Sahin, 2006). Moreover, as suggested in the work of Li (2012), integrating multiple theories in a study can yield more fruitful insights into privacy and related behaviors. Furthermore, it is essential for researchers to establish connections among the theories when constructing an integrated theoretical framework (Li, 2012). For example, the privacy calculus theory is commonly employed as a central approach to analyzing individuals' behavior before incorporating other theories. While these different theories are used to interpret how the privacy calculus is processed, the general findings support the central role of the privacy calculus (Laufer & Wolfe, 1977; Li, 2012). Potential research questions are as follows:

1. How do individuals make decisions to disclose health data in SHMSs: thinking beyond privacy trade-off?
    a. How do psychological, socio-cultural, and technological factors collectively influence individuals' decisions to disclose health data in SHMSs?
    b. What alternative theoretical frameworks can better explain these influences beyond the traditional privacy trade-off model?

2. How can customer-perceived value be reshaped in SHMSs from a multidimensional development theory perspective?
    a. In the context of SHMSs, how are different dimensions of customer-perceived value – comprising utility, trust, personalization, and privacy concerns – interrelated?
    b. How can multidisciplinary theoretical perspectives enhance our understanding of these relationships to improve user engagement and system design?

Avenue 6 – Investigating less-explored aspects of emerging themes from this review:
Researchers are encouraged to focus on the influencing factors arising from lesser-explored aspects of emerging themes, such as barriers to surveillance and difficulties in involving new stakeholders with new business plans, as well as the profound impact of emotional responses such as stress, anxiety, and discomfort stemming from privacy concerns (De Moya & Pallud, 2020; Degirmenci, 2020; Zhang et al., 2022). The use of surveillance or monitoring devices (or services) without appropriate privacy protection mechanisms in the system is very likely to stimulate competing demands for privacy and data sharing when individuals use smart health monitoring systems, which can result in individuals' unwillingness to employ smart health devices or services (Pirzada et al., 2021; Prati et al., 2019; Westin, 2003). Although surveillance was recognized as an important theme in the reviewed literature, only a few studies explored surveillance-related contextual factors. Likewise, health insurance providers are emerging as stakeholders interested in subsidizing the purchase of wearable devices and implementing bonus programs. However, involving new stakeholders may heighten the complexity of privacy management. It is crucial to analyze the characteristics of these new stakeholders and their contextually relevant challenges in addressing the privacy concerns of individual customers.

Moreover, our findings reveal a notable disparity in the distribution of studies, with a substantial contribution from Asia-Pacific and European regions, while insights from North America remain relatively limited. Despite this, numerous reports highlight a concerning prevalence of privacy breaches associated with SHMSs in North America (e.g.,CNBC.com, 2022; Thelancet.com, 2023). This raises questions about whether North America might exhibit a greater tolerance for privacy breaches in SHMSs compared to European regions, prompting an investigation into how these variations in cultural and regulatory contexts impact privacy perceptions and management strategies. Is this disparity potentially influenced by variations in regulatory frameworks and cultural perspectives? In respect to these less-explored aspects, there are a number of possible research questions of interest for future researchers:

1. How can inappropriate traceability and monitoring affect individuals' willingness to share data in the context of smart health monitoring?

2. How do perceived privacy risks influence the use of reward-based SHMSs?
3. Does North America exhibit a greater tolerance for privacy breaches in SHMSs compared to European regions?

In sum, this section has discussed several promising avenues for future research. Each avenue highlights unique perspectives and research questions based on a contextualized definition, multi-level analysis, methods of analysis, stakeholder analysis, contribution to the IS theories, and investigation of less-explored aspects of emerging themes.

Future researchers are encouraged to combine multiple avenues to gain a richer understanding of the specific privacy issues surrounding a particular SHMS research topic. Manuscript 2 exemplifies the effective integration of multiple research avenues, demonstrating how future researchers can incorporate these approaches into their studies. Manuscript 2 shows that SHMSs grant unparalleled health insights to empower individuals and communities, but their intrusive nature of data collection raises privacy concerns. Against this backdrop, Manuscript 2 delves more deeply into the factors influencing privacy concerns in the use of SHMSs while examining the intricate dynamics between privacy and health priorities in SHMS use. Motivated by Avenue 5, this manuscript embraces a broader and contrarian view beyond the privacy trade-off perspective. It adopts health empowerment theory that considers dynamic, multi-level, and longitudinal perspectives. Motivated by Avenue 3, Manuscript 2 also highlights the importance of a mixed-methods approach for better understanding the privacy dynamic in the context of smart health monitoring. Additionally, Manuscript 2 focuses on less-explored aspects of technological challenges associated with the surveillance-based nature of SHMSs, which is motivated by Avenue 6. Motivated by Avenue 2, this manuscript uses a multi-level analysis to explore how the factors interact and influence privacy concerns at different levels, such as individual, family and community health levels, in relation to SHMSs.

2.6.3 Limitations

Our review has some limitations. First, despite our broad search terms for surveillance, it is possible that some critical articles and concepts were missed since previous researchers may have used alternative terms to surveillance, monitor, track, or detect to describe the surveillance situation. Second, a number of reviewed articles used various terms for smart health monitoring systems, such as eHealth, remote health, connected health, or smart home which may have caused inconsistencies in the article inclusion. Third, the review aimed only at key stakeholders – individuals, healthcare providers, smart technology providers, and government authorities. Future literature reviews could include more novel stakeholders, for

example, insurance service providers, which may be essential in smart health monitoring systems.

2.7 Conclusion

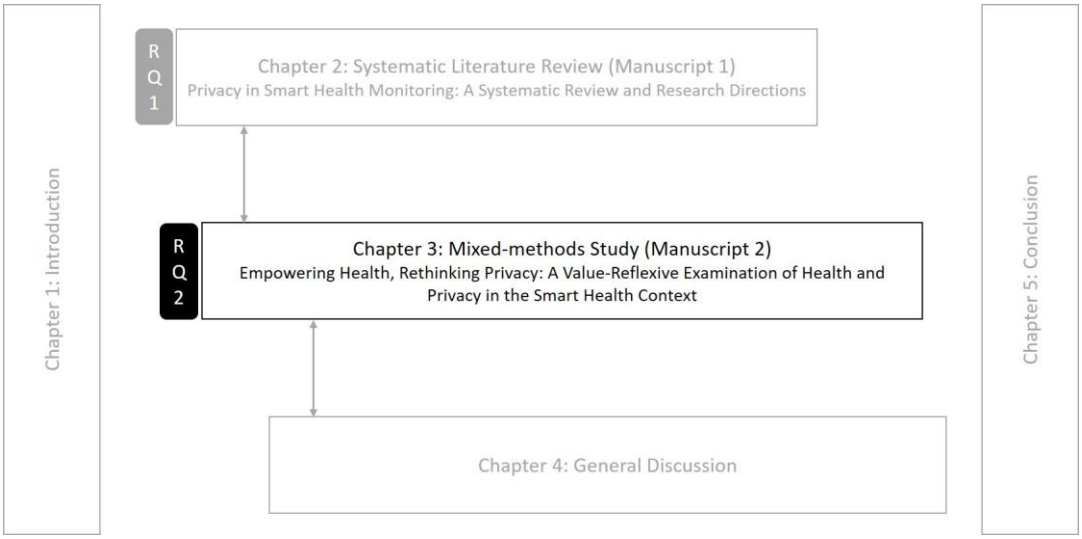
We addressed the gap in the existing literature concerning the incomplete contextualization of privacy in SHMSs and answered our research question. Initially, we emphasized the importance of contextual clarity in privacy research within SHMS contexts and highlighted the deficiencies of previous review articles in meeting this requirement. Through a systematic literature review encompassing 49 articles, we proposed a contextual framework for SHMS privacy research, synthesizing partial perspectives to offer a comprehensive understanding of the current state of contextualized privacy in these systems. Our framework offers valuable insights for scholars seeking to grasp the nuanced aspects of privacy in SHMS settings. Furthermore, we examined the theories and methods utilized in current SHMS research, advocating for scholars to consider multiple theoretical perspectives and adopt mixed-methods approaches. Our findings can assist healthcare providers and policymakers in identifying potential privacy issues related to personal health information when collaborating on the development and implementation of healthcare surveillance systems. Additionally, our research identified existing knowledge gaps and outlined six potential research avenues to achieve a thorough understanding of privacy in SHMSs.

Preface to Chapter 3

Based on the findings from Chapter 2 and existing literature, Chapter 3 aims to answer the second research question (RQ2): *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?* As shown in Figure 2. 3, Chapter 3 includes Manuscript 2 titled 'Empowering Health, Rethinking Privacy: A Value-Reflexive Examination of Health and Privacy in the Smart Health Context'. The SLR work of Chapter 2 uncovered the reality of privacy phenomena studied in the reviewed literature. It offers critical contributions to the entire thesis. For instance, it provides a contextual framework for a comprehensive understanding of privacy in SHMSs. It highlights the multi-level analysis as an important research avenue for researchers on privacy in SHMS contexts, which motivated the investigation in both individual and community-level health empowerments rather than focusing solely on the individual level. Moreover, it supports the importance of deriving significant value from incorporating theories that can better capture the intricate dynamics of smart health environments.

Figure 2. 3

The position of Chapter 3 in the thesis



The insights from Chapter 2 pave the way for Chapter 3, which further explores privacy concerns in relation to health empowerment in SHMSs. Drawn on health empowerment theory, Chapter 3 involves a sequential two-stage mixed-methods design encompassing both qualitative and quantitative studies. The findings show that health concerns trump broader ethical and privacy considerations. Faced with illness, individuals prioritize their well-being above all else; however, age significantly modulates this equation. Non-elderly users (under 65) express greater discomfort with SHMS-related privacy loss compared to their elderly

counterparts, hinting at generational shifts in privacy expectations. Furthermore, an interesting disconnect emerges in community health perspectives, where non-elderly users perceive their own health empowerment as inherently linked to the well-being of their communities, while, for elderly users, these concepts seem less intertwined. The findings of Chapter 3 challenge the notion of a universal trade-off and unveils intricate dynamics between privacy and health priorities in SHMS use, particularly across age groups. Chapter 3 pursues alternative perspectives that may challenge prevailing attitudes or trends but allow to discover deeper on the intricacies of privacy phenomena within SHMSs. It contributes to addressing the contention between health and privacy values in SHMSs, surfacing inconsistencies and disparities between our exploration's findings and the prevailing thoughts on the value of privacy in health information technology use like SHMSs.

Chapter 3 Health and Privacy: A Value-reflexive Examination (Manuscript 2)

3.1 Abstract

The digital age has sharpened the clash between health and privacy. Smart health monitoring systems (SHMSs) grant unparalleled health insights to empower individuals and communities, but their intrusive nature of data collection raises concerns for privacy. Challenging the notion of a universal trade-off, this study unveils intricate dynamics between privacy and health priorities in SHMS use, particularly across age groups. Through a mixed-methods exploration of actual and potential SHMS users, we discovered that in the context of immediate health concerns, individuals may prioritize health over broader ethical and privacy considerations. Faced with illness, individuals may prioritize their well-being above all else; however, this tendency varies with age. Non-elderly users (under 65) express greater discomfort with SHMS-related privacy loss compared to their elderly counterparts, hinting at generational shifts in privacy expectations. Furthermore, an interesting disconnect emerges in community health perspectives, where non-elderly users perceive their own health empowerment as inherently linked to the well-being of their communities, while, for elderly users, these concepts seem less intertwined. These findings challenge the prevailing assumption that health empowerment through SHMSs necessarily entails universal privacy sacrifices. Our study invites a nuanced re-evaluation of privacy within SHMSs, recognizing the complex interplay between health and privacy in the digital world. Given the study's limitations, further research is warranted to substantiate these findings and explore their implications more deeply.

Keywords: Health empowerment; privacy; smart health technology; contrarian thought; value-reflexive.

3.2 Introduction

For much of human history, health and privacy have been among the many inalienable rights of humans (Cohen & Ezer, 2013; Di Iorio et al., 2021). They are distinct rights by nature, valued highly for different reasons, but each inextricably linked to Maslow's hierarchy of needs (Maslow, 2013; Shapiro et al., 2019; Zimmerman, 2000). For example, health is valued as a physiological necessity associated with meeting our most basic need for survival and well-being against injury and accidents (McLeod, 2007; Shapiro et al., 2019), while privacy is valued as a safety and security requirement associated with meeting our need to not be caused harm (Maslow, 1970; Shen et al., 2021). Privacy is also valued for its ability to help meet our needs

for esteem and self-actualization, whereby we are seen positively by others and able to express ourselves genuinely and freely (Laufer & Wolfe, 1977; Maslow, 1970; McLeod, 2007).

In the modern digital world, because of contemporary demands of convenience, personalization, and capitalism (Puntoni et al., 2021; Zuboff, 2015), health and privacy have increasingly come into contention, serving as opposing forces where the gain of one requires the loss of the other (Agaku et al., 2014; Fox, Clohessy, et al., 2021; Mechanic & Meyer, 2000; Nelson et al., 2016; Niknejad et al., 2022; Seh et al., 2020; Srivastava et al., 2022). Within this literature, some degree of privacy loss is assumed to be an important determinant for effective health diagnosis and treatment throughout the course of one's life (Agaku et al., 2014; Ali & Dang, 2022; Gao et al., 2015; Hassandoust, Akhlaghpour, et al., 2021; Seh et al., 2020). Privacy in exchange for health has become an accepted and somewhat obfuscated underlying assumption of digital technologies that empower effective health systems and personalized healthcare; but should it be? Should we assume privacy loss is acceptable for everyone when balanced against their health or are there aspects of the fundamental right to privacy that persist beyond the promise of better health? Further, does the consideration of individual privacy even matter when the health of an entire community is at stake? So, in the context of empowering health versus concerns for privacy, when we ask, "Which values do we value?" (Zimmer et al., 2023, p. 1), the answer could very well be, "It depends."

Against this backdrop, this study explores the complex dynamics, or the ongoing contention between health and privacy values as it persists in the SHMSs of today and surface inconsistencies and disparities between the findings of our exploration and the prevailing thoughts on the value of privacy in health information technology (HIT) use. SHMSs are a form of HIT that employ advanced surveillance technologies to monitor changes in individuals' personal vital signs and daily health (Alabdulatif et al., 2019; Ray et al., 2020; Winter & Davidson, 2019). The continuous monitoring and personalized feedback offered by SHMSs empower both individuals and communities, as they provide their users a better understanding of their health status (Sovacool & Del Rio, 2020), while also providing community-level support for public health research, policy development, and disease prevention strategies (Wolfenden et al., 2019). In doing so, however, they problematize values associated with privacy (Essén, 2008; Maher et al., 2019), as ethical dilemmas arise due to the potential intrusion into individuals' basic human rights and the erosion of their privacy relative to the good of the whole. As such, it's not clear if the assumptions of individual privacy values that underpin extant HIT research are applicable in the SHMS context or are in need of revision.

Leveraging health empowerment theory and following a mixed-methods research design involving 377 actual and potential users of SHMSs, we find that, when people face health issues or immediate concerns for their health, they prioritize these problems over the broader issues of ethics, equity, and privacy. we also find support for the notion that the relative value of privacy to health does not hold steady through one's lifetime, nor for health interests beyond oneself. Specifically, concerns for privacy loss from SHMS use is a significant health empowerment determinant for non-elderly users (less than 65 years old), but not for elderly users. Moreover, non-elderly SHMS users attribute the health empowerment of their communities to their individual health empowerment, while elderly users seem to disconnect the two. These are two important findings from our research that are not consistent with the assumptions of privacy versus health that have underpinned our current expectations of HIT use in the digital world and indicates a departure from conventional wisdom and underscores the complexity of the privacy-health empowerment dynamics.

In the sections that follow, we first describe the salient literature that informs our current understanding of the values of privacy relative to health in HIT environments. We then describe the theoretical foundation upon which we are able to explore the health and privacy value contention SHMS users experience. We then describe the mixed-methods research design and the findings that inform our discussion. Theoretical and practical implications follow.

3.3 The Values of Privacy Relative to Health in HIT Environments

Values are defined "as trans-situational goals, varying in importance that serve as guiding principles in the life of a person or group" (Schwartz et al., 2012, p. 664). Values can be understood as "what is important to us in life" (Schwartz, 2012, p. 3), and the trade-off between pertinent and conflicting values is what steers an individual toward pursuing a specific goal (Schwartz, 2012). While individual values are organized into a cohesive system that influences and elucidates individuals' attitudes and behaviors (Schwartz et al., 2012), certain values are compatible with each other, while others may be contradictory (Schwartz et al., 2012).

Usually, values are abstract, giving rise to a broad constellation of related attitudes and behaviors. Core values are pervasive and commonly internalized from a young age (Aronson, 2004). There is a prevailing belief that an individual's values serve as consistent indicators of their thoughts and behaviors in value-relevant situations (Rohan, 2000). The degree of concern individuals feel about something in life can be explained by the level of importance they attach to values associated with that object.

The values of power, achievement, and hedonism promote individuals' self-enhancement goals. Threats to these values activate cognitive awareness and affective experience related to such threats (Schwartz et al., 2000). It has been argued that these self-enhancement values are also associated with the violation of personal privacy (Alashoor et al., 2015; Schwartz et al., 2000). Privacy is considered to be a fundamental human right to be free from intrusion by others (Solove, 2002; Tavani, 2007), involving an individual who restricts (or manages) access to personal data through the same surveillance means (Marx, 2015). In the IS field, the most commonly cited contexts for privacy are related to technological workplace applications, the use of information by sector, the type of information collected from individuals, and politics (Smith et al., 2011).

Research in the HIT context has contributed to this discussion (Shen et al., 2019), showing that, due to the intensive usage of surveillance and monitoring technologies, HITs impose various negative effects on the privacy of their users (Essén, 2008; Maher et al., 2019). These effects include being seen and traced without knowledge or permission (Burrows et al., 2018; Gupta et al., 2021; Perez & Zeadally, 2021), risks of sensitive health data sharing and losing control over lifestyle choices (Hassandoust, Johnston, et al., 2021; Wiegard & Breitner, 2019), and a post-adoption feeling of lack of control over personal information inconsistent with actual privacy risks (Zhang et al., 2019).

Despite the conventional notions in mainstream research, few perspectives challenged the traditional assumptions of privacy and health value (e.g., Princi & Krämer, 2020; Zarcadoolas et al., 2013). For example, researchers argue that privacy concerns are not a barrier preventing participants from using electronic health information tools (Zarcadoolas et al., 2013).

In the HIT context, *privacy concerns* refer to individuals' concerns for the protection of their personal health information and medical facilities' use of it (Kuo et al., 2014). According to the existing literature, the antecedents of these concerns can be categorized according to their individual, contextual, or macro-environmental level influence (Henderson & Snyder, 1999; Li, 2011; Miltgen & Peyrat-Guillard, 2014; Xu, 2019). The antecedents of privacy concerns at the individual level include personality, knowledge and experience, as well as various other psychological factors and demographic characteristics (Li, 2011; Smith et al., 2011; Xu, 2019), while antecedents at the contextual level include traceability (Beaudin et al., 2006; Chadborn et al., 2019), security (Alraja, 2022; Hsu et al., 2013), fairness/equity (Li, 2012; A. Wagner et al., 2021), information sensitivity, ethical considerations (Gupta et al., 2021; Kaplan, 2016; Li et al., 2023; Pirzada et al., 2021), and the importance of organizational transparency (Xu, 2019). Finally, legislation and regulatory structure (Wiegard & Breitner, 2019; Xu, 2019), cultural

values (Kulyk et al., 2020; Li, 2011; Yun et al., 2019), and social norms are three macro-environmental factors that have been argued to be effective predictors of privacy concerns related to HIT use.

In summary, this literature would suggest privacy matters to HIT users, even when weighed against one's health. But before this knowledge can serve as an ironclad underlying assumption of how individuals perceive and experience the tension between privacy and health in the SHMS context, we believe a more nuanced exploration is required: one that takes a contrarian view of the assumption and differentiates among and between individuals and their community empowerment interests.

3.4 Theorizing the Health Empowerment Imperative

To provide a foundation from which to explore the tension between the values of health and privacy in the SHMS context, while simultaneously engaging with our own value systems, we look to health empowerment theory. Health empowerment theory is a derivative of empowerment theory and promotes empowerment as a tool or means by which to achieve the broader goal of better health (Rissel, 1994). It transcends the achievement of outcomes, rather, it embraces the notions of prioritizing knowledge, agency, and control over one's health. For these reasons, the study explores the contention between health and privacy values that persist in the perception of SHMSs from the perspective of prioritizing health empowerment over the general values of health and privacy.

Empowerment is a complex concept originating from the women's and civil rights movements (Rissel, 1994). It is often promoted as an idea of enhancing individuals' possibility to control their lives and health experiences at an individual level (Shearer, 2007), but empowerment is also a multi-level construct significant for community psychology in relation to collective groups of individuals (Rappaport, 1987; Swift & Levin, 1987; Zimmerman, 2000). Based on this concept of empowerment, empowerment theory links individual well-being with the larger political and social environment, suggesting that people need opportunities to become active in community decision making to improve their well-being, lives, organizations, and communities (Zimmerman, 2000).

Health empowerment theory uses the premise of empowerment to explain health promotion in the context of health communities. The theory suggests a model including both individual and community health empowerment (Rissel, 1994). Applying the definitions proposed by Spreitzer (1995), *individual health empowerment* refers to individuals' perceptions of access to information, support, resources, and opportunities to learn and grow, enabling individuals to

optimize their health and obtain a sense of competency, meaningfulness, self-determination, and impact on their lives. *Community health empowerment* is a group phenomenon that includes a raised level of individual health empowerment, a political action in which individuals have dynamically participated, and the achievement of some redistribution of resources or decision making beneficial to the community in question (Rissel, 1994). As highlighted in the study by Israel et al. (1994), "an empowered community has the ability to influence decisions and changes in the larger social system" (p. 5).

Previous studies (e.g., Swift & Levin, 1987; Torre, 1986) suggested that individual health empowerment is a pre-requisite for the next level of empowerment. A combination of both levels is essential before community health empowerment can occur. Moreover, according to Rissel (1994), empowerment is considered to be both an outcome and a process. It is an outcome when empowerment is defined by the distinction between levels. Meanwhile, empowerment is a process that simultaneously operates at both levels until reaching community health empowerment with an increase in the control over resources.

3.4.1 Individual and Community Health Empowerment through SHMSs

In the context of SHMS, according to health empowerment theory (Rissel, 1994), community health empowerment can be achieved if members actively engage in collective activities that influence health-related decisions affecting the SHMS community health status. In other words, community health empowerment reflects a raised level of individual health empowerment, where the individual is a 'true member' of an SHMS community. The study applies health empowerment theory as an overarching theoretical lens in our research context, because it is suitable for explaining the health value SHMS users gain in exchange for their privacy. Privacy concerns reflect an individual's physiological sense of control, boundary, and self-protection about their health information (Zhu et al., 2022). In contrast, the value of the empowered individual health in SHMSs is based on a sense of competency, meaningfulness, self-determination, and positive impact on their lives (Kim & Gupta, 2014; Spence Laschinger et al., 2010).

Following the challenge of balancing values of privacy and health empowerment, individuals who are more passionate about gaining broader experiences, sharing their information and knowledge, and acquiring skills distinguish themselves in the supportive environment of the SHMS community (Rissel, 1994). Through their engagement with SHMS, they are not only feeling as if they are a part of an SHMS community and growing personally, but that they have power as part of that community (Laverack & Wallerstein, 2001; Wolfenden et al., 2019). Despite the parallel advancements in both personal and community levels, there is a potential

deterrent effect of privacy concerns on individuals' willingness to engage with SHMS, share personal health information, and actively participate in health-related initiatives, given that personal health data forms the foundation for the functionalities in SHMS (Nelson et al., 2016).

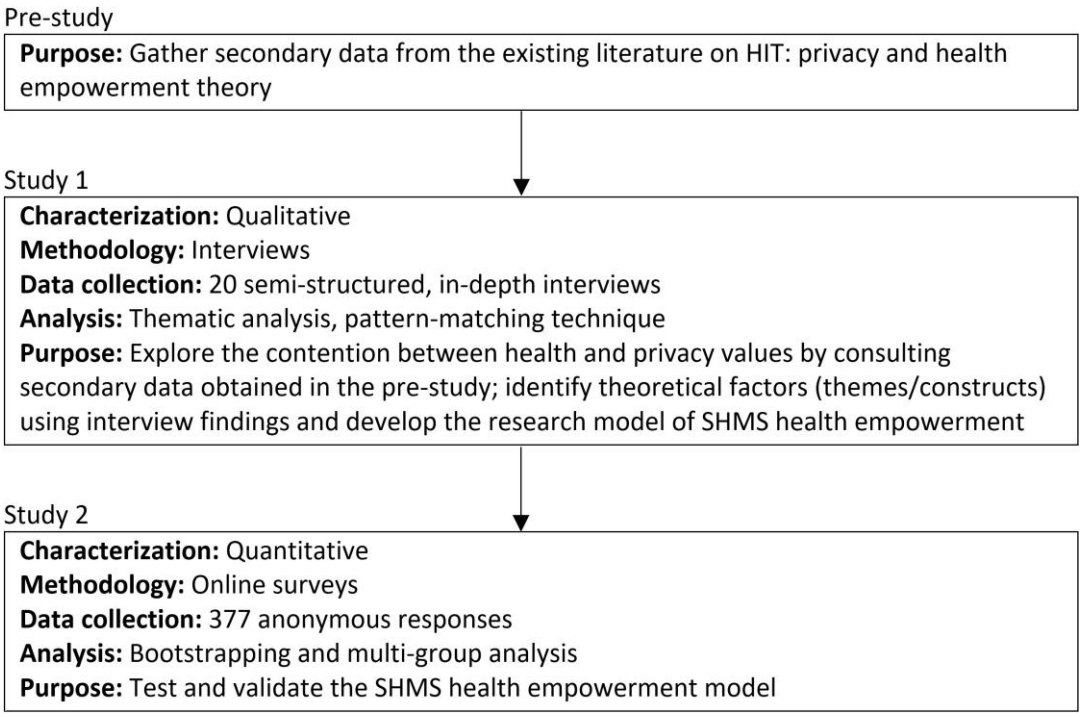
3.5 Mixed Methods Research Design and Results

The present research follows a post-positivist research paradigm to uncover multiple perspectives (Creswell & Poth, 2018). It employs a sequential two-stage mixed-methods design encompassing both qualitative and quantitative studies (Creswell & Plano Clark, 2018). This specific design is chosen due to its three methodological advantages. Firstly, a sequential mixed-methods research design has the ability to address exploratory questions within the same study inquiry (Venkatesh et al., 2013). Secondly, it enables a holistic understanding and integrative insights of findings from a combination of qualitative and quantitative aspects, which strikes a balance between depth and breadth (Venkatesh et al., 2013). Thirdly, a mixed-methods design is particularly suitable for exploring new contexts where issues are difficult to explain or describe using existing views (Ågerfalk, 2013).

Because a mixed-methods research design should serve a specific purpose, it is crucial to consider the appropriateness of the selected mixed-methods design (Venkatesh et al., 2016). Mixed-methods designs are categorized by their purpose: developmental, completeness, complementarity, expansion, corroboration/confirmation, compensation, and diversity (Venkatesh et al., 2013). Among these categories, we follow the developmental purpose, which involves using the findings of a qualitative study to develop a suitable set of constructs, establish relationships among these constructs in the form of a model, and propose a corresponding set of hypotheses. Subsequently, these hypotheses are tested using a quantitative method (Venkatesh et al., 2016). Figure 3. 1 presents a roadmap of our mixed-methods research design.

Figure 3. 1

Roadmap of our developmental, mixed-methods approach



As shown in Figure 3. 1, we included a pre-study component in our mixed-methods design that served to establish the extant perspective of the contention between privacy and health in SHMSs and health empowerment theory. The details of the qualitative (Study 1) and quantitative (Study 2) components of our mixed method approach are described next.

3.5.1 Study 1: Qualitative Study Design

Study 1 adopts an explorative research approach (Creswell & Poth, 2018), employing qualitative interviews with 20 individual participants, based on specific SHMSs ranging from some clinical trials to surveillance-based monitoring products available in the local market, e.g., glucose monitors and wearable bio-stickers. The purpose of these interviews is to identify key theoretical considerations and contextual factors for managing privacy concerns in relation to individual and community health empowerment, and then use those insights to formulate a research model and associated set of hypotheses. The interviews were pseudo-exploratory to help contextualize the model for testing. They were semi-structured, and based on an interview guide (Taylor et al., 2016). The interview questions were mainly derived from the literature, including insights into data governance mechanisms (Abraham et al., 2019), and tailored to the smart health context. The interview participant profiles can be found in Appendix Table C. 3. The participants varied in their familiarity with SHMSs. Some were healthcare and government professionals with a greater awareness of relevant legislation, while others were end-users, including five categorized as laypeople. These lay participants are

identified as "Not familiar" (see Appendix Table C. 3), to distinguish their perspectives from those of professionals. Incorporating viewpoints from both laypeople and experienced end-users is beneficial, as it captures a more diverse range of perspectives (Langley et al., 2018), thereby enhancing the applicability of the SHMS model in promoting health empowerment. It also helps address the concern about the alignment between interview participants and survey participants.

The interview protocol was structured in three main sections: 1) gathering demographic information, 2) exploring antecedent factors influencing privacy concerns in SHMS contexts, and 3) delving into the connection (or contention) between privacy and the promotion of health well-being at both individual and community levels in relation to SHMS. The interview questions are listed in Appendix G. The interviews were audio-recorded and fully transcribed for coding purposes. The analysis of the interview transcripts was completed by two researchers using Nvivo v12 software.

The interview transcripts were analyzed using thematic analysis to identify important patterns and themes in the datasets of data governance mechanisms in terms of privacy. Thematic analysis is a technique widely used to identify, analyze, and report patterns or themes from qualitative data (Braun & Clarke, 2006). Using this technique, we executed several main steps, including reading the transcripts, generating initial codes, identifying the themes, defining themes, and reporting themes (Braun & Clarke, 2006). Moreover, we adopted a flexible pattern-matching technique to identify more promising themes for later theorizing. A flexible pattern-matching technique enables the interaction of inductive and deductive components while combining rigor with high flexibility (Bouncken et al., 2021). For example, with a deductive interaction, we combined two factors of cultural diversity and religious difference into one factor as *cultural and religious differences*.

3.5.2 Developing and Hypothesizing an SHMS Health Empowerment Model

In the following section, we showcase a selection of quotes considered to be the most informative and explicit insights relating to the factors from the interviews. The quotes are integrated into insights spanning a full model of individual and community level health empowerment, henceforth referred to as an SHMS health empowerment model. Appendix Table C. 4 presents the selected quotes by participants on the key constructs and relationships.

Based on the interview results, we identified seven antecedent factors impacting individuals' privacy concerns with SHMSs. These factors include *legislative protection*, *transparency*, *cultural and religious differences, ethical considerations*, *fairness/equity, traceability*, and

security, which can be integrated into three value-based themes, i.e., regulatory and sociocultural, ethical, and technological (see Table 3. 1).

Table 3. 1

SHMS privacy concern themes

Themes	Factors of privacy concerns
Regulatory and sociocultural	Legislative protection
	Transparency
	Cultural and religious differences
Ethical	Ethical considerations
	Equity/fairness
Technological	Traceability
	Security

Regulatory and sociocultural theme in relation to privacy concerns

The findings reveal three factors in relation to regulatory and sociocultural privacy concerns in SHMSs: *legislative protection*, *transparency*, and *cultural and religious differences*. In general, *legislative protection* of data privacy refers to the right to information, provisions prohibiting or restricting the use of mechanisms of data governance, rules on IT-security-legislation, and provisions supporting the use of mechanisms (Weber, 2010). In healthcare settings, it has been reported that robust legislative protection addresses privacy concerns, reduces skepticism toward technical innovations, and enhances their perceived value (Gasser et al., 2020; Li et al., 2016; Nguyen et al., 2022; Princi & Krämer, 2020). In line with this literature, all the interviewees highlighted the importance of legislative protection for the effective management of privacy issues in SHMSs. For example, a participant (*participant#5*) who was a caregiver from the healthcare industry stated, "*I am very familiar with the existing privacy acts and codes …[because] we were repeatedly mentioned all those acts when we have nursing courses.*" Although some other participants were not familiar with those acts and codes, they nevertheless mentioned the importance of legislative protection. A typical quote (*participant#3*) was: "*I'm not as familiar as I should be…I guess in New Zealand where generally people are pretty well protected it's an area that's really difficult to make sure it's well covered in law.*"

Transparency refers to ensuring everything is visible, denoting one's openness or open communication to pursue trustworthiness (Kim et al., 2014). Since transparency is defined as openness of information, transparency and openness could be used in an interchangeable way (Zhang et al., 2020). In healthcare system contexts, transparency ensures that system operations are visible and understandable. It includes clearly communicating the system's

capabilities, such as accuracy, limitations, potential errors, and recognized biases (Khanna & Srivastava, 2020). Transparency has been found to be positively associated with customers' privacy concerns in various IS contexts (e.g., Bargh et al., 2017; Xu, 2019). Additionally, the relationship between privacy and transparency is treated as a trade-off (Bargh et al., 2017). A statement from an individual working in a government health authority (*participant#2*) was made as "*You [government health authorities] can also be very clear in your privacy-related materials about what the information will be used for…so people who really wanted to know what's going on [can] go and read the full document…but for the relatively small number of people that could read that code and understand it, they could go there and confirm that*." Another participant who was a nurse of a healthcare provider stated, "*I have to let him [the patient] know what I'm going to do first and then talk to the person about what the reason is for having this test. And then the beginning is to understand that, well, if there are elderly people who have Alzheimer's, they will also call with the family and communicate with them first, then, I know what to do next*" (*participant#6*).

Cultural and religious differences influence people's attitudes and behaviors when they are involved in using healthcare monitoring devices (Karadag et al., 2019). Different cultural and religious backgrounds contribute to varying interpretations and perspectives on privacy-related matters (Smith et al., 2011; Sovacool & Del Rio, 2020). The literature indicates that cultural and religious factors play a significant role in shaping privacy concerns across different countries (e.g., Choi & Kim, 2024; Martin & Nissenbaum, 2016). Similarly, most interviewees emphasized the importance of cultural and religious matters related to privacy concerns. One participant (*participant#10*), an SHMS project manager from the healthcare industry, claimed, "*We would get feedback from one of our cultural advisory groups before we go into these projects. We are just making sure that we're not completely missing the issue [since] the device could be linked with some ethical considerations*." It should be noted that over-highlighting of cultural and religious differences may negatively influence the fairness and equity aspects during the implementation of data protection mechanisms (Kordzadeh & Ghasemaghaei, 2022; Ministry of Health New Zealand, 1998). An interviewee who was a technical manager from a technology company (*participant#8*) pointed out, "*New Zealand has to respect to Māori*[2] *culture, we need to obey to Māori data protection rights…but we don't bother about Indian or Asian or Chinese data rights at all … Asian differences or any other differences are not that much valued and we only talked about Māori data sovereignty*." Since *legislative*

[2] Māori culture is the cultural practices, beliefs, and customs of the indigenous Māori people of New Zealand. (Harding et al., 2011).

protection, *transparency*, as well as *cultural and religious differences* are three important factors assumed to affect privacy concerns in SHMSs, we posit the following hypotheses:

H1: *Legislative protection* is negatively associated with *privacy concerns* in relation to SHMS.

H2: *Transparency* is negatively associated with *privacy concerns* in relation to SHMS.

H3: *Cultural and religious differences* are positively associated with *privacy concerns* in relation to SHMS.

Ethical theme in relation to privacy concerns

The topic of data ethics strives for a universal declaration of human rights: No one shall be subjected to torture or to cruel, inhuman, or degrading treatment or punishment (Sharkey & Sharkey, 2012). Based on our findings, we observed the importance of ethics in healthcare. Data ethicists place emphasis on values such as moral dilemmas, fairness, and trust (Jones et al., 2018). Those values are closely linked to the evaluation of ethical behaviors (Wagner & Sanders, 2001). Thus, we define data ethics as an umbrella in this study that allows all ethics-related topics (e.g., fairness/equity) to be involved in the discussion. The interview results show *ethical considerations* and *equity/fairness* are two salient factors that touch on privacy concerns and enhance individuals' data protection in a health monitoring system.

The factor of *ethical considerations* focuses on managing ethical concerns such as a loss of personal liberty, an increase in the feelings of objectification and loss of control, and deception and infantilization (Sharkey & Sharkey, 2012). Ethical considerations, in conjunction with consent and privacy issues, have been extensively discussed, underscoring their crucial role in protecting personal health information (e.g., Kennedy et al., 2021; Lee et al., 2016; Sarathy & Robertson, 2003). Ethical considerations also gained remarkable attention in the interview results. One interviewee (*participant#2*), who was working in a government health authority, indicated, "*We are interested in the ethical space and we would call this social license, it's not so much what can you [we] do purely legally, but what would people expect you [us] to do and what is kind of good behavior and…trying not to do things that people wouldn't expect or might not be happy with, even if technically you [we] could do them legally*." The participants understood that surveillance technologies have to be used to access and monitor health data, but these technologies may increase ethical issues as well. Another participant (*participant#10*) noted, "*Our sticking [monitoring] device could be linked with the usage of tracking devices in prison…but those are ankle bracelets right? We need to make sure a device, well, it's not a device, it was a way to capture people's vitals by using the camera on users'*

phones…[therefore] we should be more careful about ethical when we recruited patient volunteers."

The *equity/fairness* factor emphasizes the absence of avoidable or remediable differences between groups of people (Schaefer & Ballantyne, 2022). Health information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances (The Ministry of Health New Zealand, 2017). The literature suggests that fairness aspects have a positive impact on privacy protection belief (e.g., Li et al., 2011; A. Wagner et al., 2021). As said by one interviewee (*participant#1*) from a government authority, *"[Equity is] one of four main dimensions together with clinical safety, privacy, and security in terms of data protection scope in the healthcare sector*." It is noteworthy that, throughout the interviews, there was a frequent blending or conflation of ethical concerns, and equity/fairness in the discussions. Similarly, previous literature argues that several concepts, including ethics, anonymity, confidentiality, secrecy, security, overlap and can easily be confused with the concept of privacy (Smith et al., 2011). Given the aforementioned findings from interviews and existing literature, where privacy has been investigated in the HIT literature from multiple ethical theoretical perspectives (e.g., Gupta et al., 2021; Pirzada et al., 2021), we posit the following hypotheses:

H4: *Ethical considerations* are negatively associated with *privacy concerns* in relation to SHMS.

H5: *Equity/fairness* is negatively associated with *privacy concerns* in relation to SHMS.

Technological theme in relation to privacy concerns

Advanced technology, with its increased capabilities in communication, computation, retrieval, and storage, has redefined the concepts of personal information privacy and the right to privacy (Hathaliya & Tanwar, 2020; Henderson & Snyder, 1999). Under the technological capability theme, the factors of traceability and security have been argued to pose privacy concerns. *Traceability* aids in examining the interconnectedness between the devices and the associated data owners in SHMSs (Lomotey et al., 2017). The interconnected nature of data collection and data sharing, enabled by traceability, allows for the accountability of health services to be tracked. At the same time, it heightens vulnerability to privacy leaks and security threats (Butpheng et al., 2020). This dual aspect of traceability inherently intensifies the tension between the need for traceability and privacy protection requirements (Ganascia, 2011; Yang, 2022). The interview findings reflected these dual aspects. Most participants recognized that SHMSs are largely associated with e-discovery practices or surveillance means to realize access development and continuous monitoring. A participant (*participant#10*)

informed the researchers, *"To be able to use that device within New Zealand, we have to switch off the voice recognition part, but there were questions such as can I be listened or can I be tracked*." On the other hand, it is noteworthy to learn that traceability can contribute to the enhancement of health data protection practices. Another participant (*participant#4*) thought, "*They [traceability] will be able to monitor improper data transfer processes… this [traceability] can avoid or detect unauthorized behaviors and increases data protection ability of the system*."

Security is defined as a condition that results from the maintenance and establishment of protective measures that safeguard a state of inviolability from influences or hostile acts (Al Ameen et al., 2012). Security management includes the execution of risk assessments, the setup of data security roles, and the definition of data security policies, standards, and procedures (Abraham et al., 2019). It is a constant topic that has been proven to be significantly interrelated with privacy protection activities in healthcare systems. There has been a limited number of researches examining the relationship between security and privacy (e.g., Casaló Luis et al., 2007; Hsu et al., 2013). More commonly, security and privacy have been treated as intertwined components. For example, Arpaci et al. (2015) hypothesize that perceived security and privacy will positively influence attitudes toward the educational use of cloud services. Despite the limited research, security is identified as another important factor under the technological theme in our findings. One participant (*participant#2*) reminded the researchers of the importance of distinguishing between privacy and security, saying, "*Privacy is much more about individual control of identifiable information and security is much more about the mechanisms that you use in relation to the web and IT systems to stop people getting in from the outside or stop people from the inside who shouldn't see information from seeing it*." Based on the interview findings, privacy and security are considered highly correlated areas in SHMS settings, where personal data is often required to be shared and communicated among various service providers. For example, a participant (*participant#3*) commented, "*In the past, people have asked me for my password at the hospital and I've always been a bit hesitant…now in order to give my clinicians access…I have to go online and basically share my password with them, [however], the provider should make a better means of password protection."* Since both traceability and security are important in promoting awareness and appreciation of SHMS participation, and they have been tightly linked to health information privacy protection activities, we posit the following hypotheses:

H6: *Traceability* is negatively associated with *privacy concerns* in relation to SHMS.

H7: *Security* is negatively associated with *privacy concerns* in relation to SHMS.

Privacy concerns and individual health empowerment

Our findings underscored the significance of individual health empowerment within a smart health monitoring environment. Within SHMSs, *individual health empowerment* can be described as a psychological evolution coupled with an enhanced sense of better control over one's personal health conditions, stemming from both experiential learning and the support received while engaging with SHMS devices (Nelson et al., 2016). It is an increased intrinsic motivation reflecting how individuals see their engagement with specific tasks in terms of four valued cognitions, i.e., meaning, competence, self-determination, and impact (Kim & Gupta, 2014; Nelson et al., 2016; Spreitzer, 1995). Our interview findings align with this perspective. For instance, one interviewee (*participant#3*) articulated, "*I am sure the system means a lot to me because of its ability to offer knowledge further enhanced my confidence. Being able to view the daily data [glucose records] provided me with a consistent measure of my health condition, giving me a sense of safety and strength*."

Few studies suggest that perceived privacy influences health empowerment of individual users (e.g., Liu et al., 2021; Nelson et al., 2016). However, the literature demonstrates the linkage between privacy and each dimension of individual health empowerment. For instance, privacy has been recognized to negatively associated with competence of user, a dimension of individual health empowerment. When users fear that interacting with an SHMS might expose their sensitive health data, they may refrain from exploring its functionalities, limiting their ability to develop the necessary skills and confidence to use it optimally privacy (Li, 2018). Privacy can also influence self-determination of user, another dimension of individual health empowerment, relating to the extent to which users feel in control of their health-related decisions. If users perceive that their data is being used without their explicit consent or that they lack control over privacy settings, they may feel disempowered (Helm & Seubert, 2020). This can lead to disengagement from digital health solutions, ultimately limiting their ability to take proactive steps in managing their health (Kreitmair, 2024).

The interviews data reveals a potential association between individuals' privacy concerns of using SHMS and their personal health empowerment related to the use and control over personal health information. For example, one (*participant#10*) mentioned that "*People may feel empowered after using the system as they can feel more in control over their health information."* Another person (*participant#3*) stated, *"There can be no movement along the journey towards self-empowerment unless they [we] feel confident that their [our] data is going to be protected and respected and they [we] can be confident their [our] data is not going to be used for any reason*." Regardless of the privacy paradox phenomenon that likely

exists between privacy attitude and behavior (Acquisti, 2004; Kokolakis, 2017; Smith et al., 2011), both existing literature and the interview findings reveal privacy concerns as an important factor that influences individual health empowerment in digital health contexts. Thus, we posit the following hypothesis:

H8: *Privacy concerns* are negatively associated with *individual health empowerment in the SHMS context.*

Individual and community health empowerments

According to health empowerment theory, *community health empowerment* has been recognized as a raised level of individual health empowerment (Rissel, 1994). It represents a group of members with actual control over resources, from which they obtain a high level of psychological empowerment (Israel et al., 1994; Rissel, 1994). Community health empowerment focuses on the ability to use power to solve health and well-being issues. It means that individuals have an increased influence on health-related decisions within the SHMS community (Kapondera et al., 2019; Laverack, 2001; Rissel, 1994). The interview data was in line with this understanding and offered detailed explanations, emphasizing that community health empowerment is an outcome of individual health empowerment. One participant (*participant#15*) was quoted as saying, "*The system can increase our ability to participate in our health data management, in particular it allows us to coordinate with other people including other individuals that is definitely a great opportunity to empower the overall community members including me.*" Community health empowerment is a critical outcome to the overall community development as it allows a shift of focus from the individual to collective actions in communities (Rissel, 1994). Our interview results support this viewpoint, as evidenced in statements such as, *"By participating and interacting in the system, users are able to influence service providers and the service quality of the system that must benefit the overall community health status"* (*participant#13*). Both existing literature and interview data emphasize the importance of community health empowerment and suggest its relationship with individual health empowerment. Thus, we posit the following hypotheses:

H9: *Individual health empowerment* is positively associated with *community health empowerment*.

Trust in SHMS

Trust occurs when a party believes that the other party has characteristics advantageous to its own interest (Chang & Fang, 2013; McKnight & Chervany, 2001). It is associated with many themes such as the motivation, credibility, transparency, and responsibility of a system

(Mittelstadt, 2017). The existing literature indicates that trust not only promotes a sense of individual empowerment but also facilitates community empowerment within healthcare collaborative environments (Minheere et al., 2023; Wakefield et al., 2006). From the individual perspective, one interviewee (*participant#9*) mentioned that trust is important for the acceptance of SHMS, saying, "*Everybody has to be able to trust a service system and its new technology before being willing to try it*." It reflects a common sentiment found in the interview results. Another interviewee (*participant#7*) remarked, "*Overall, trust is an extremely important thing. It can even have a direct impact on the health index of the elderly*." From the community perspective, one participant (*participant#1)* who was from the government health authority stressed, "*Trust is often regarded as a relational basis that can influence the entire population health development*." Thus, we posit two hypotheses as follows:

H10: *Trust* in SHMS is positively associated with *individual health empowerment*.

H11: *Trust* in SHMS is positively associated with *community health empowerment*.

Informed by existing literature and our interview discoveries, various personal and social factors have also been recognized in shaping health empowerment at both the individual and community levels (Ali & Dang, 2022; Chan et al., 2021; Morley & Floridi, 2019; Swift & Levin, 1987). These factors include age (Forsyth, 2020; Shearer, 2007; Zimmerman, 2000), gender (van Uden-Kraan et al., 2009), education (Anderson et al., 2019; Seibert et al., 2011), health literacy skills (Morley & Floridi, 2019), income (Shearer, 2007; Xu, 2019), traumatic experience (Zimmerman, 2000), and racial/ethnic background (Zimmerman, 2000). As such, we posit two hypotheses as follows:

H12: Personal and social factors are significantly related to individual health empowerment.

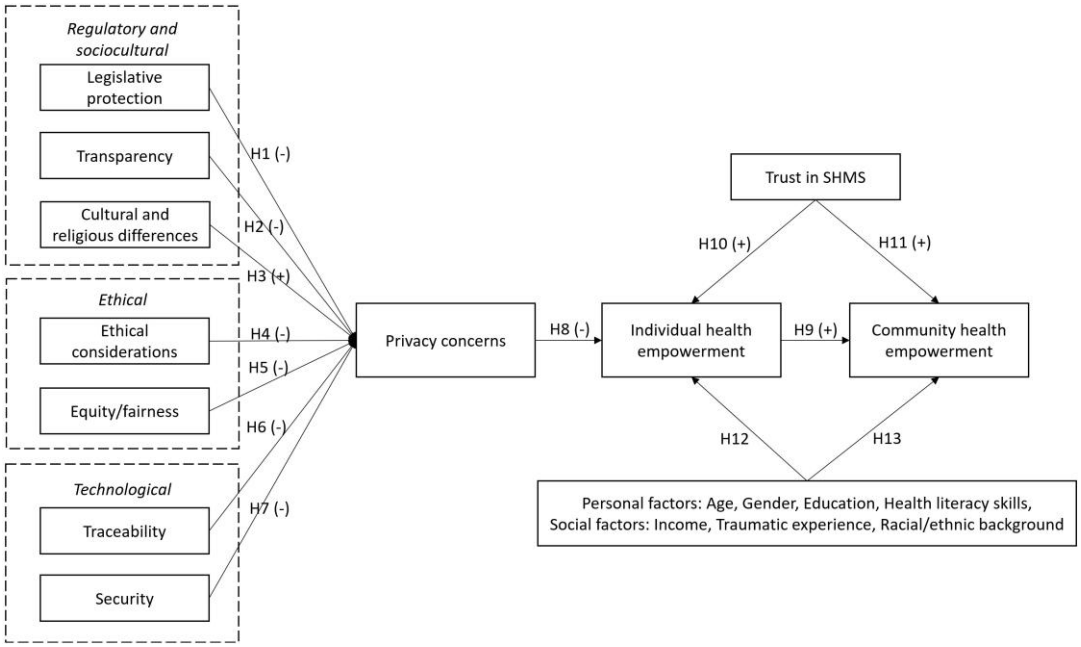
H13: Personal and social factors are significantly related to community health empowerment.

Based on the existing literature, qualitative findings, and the proposed hypotheses, we develop an SHMS empowerment model as shown in Figure 3. 2. The SHMS health empowerment model offers a testable representation of the assumptions of individual privacy values that underpin extant HIT research. In this model, privacy concerns are considered an important psychological condition, influenced by a group of contextual factors, including the regulatory, ethical, and technological aspects of SHMS use. In turn, individual health empowerment is an outcome influenced by privacy concerns, while community health empowerment is posited as an ultimate outcome of individual health empowerment.

Moreover, these two levels of empowerment are also considered to be influenced by *trust*, personal factors (i.e., *age, gender, education* and *health literacy skills*), and social factors (i.e., *income*, *traumatic experience*, and *racial/ethnic background*).

Figure 3. 2

SHMS health empowerment model



3.5.3 Study 2: Quantitative Study Design

Based on the mixed-methods design, we use Study 2 to empirically test the SHMS health empowerment model among individuals who are using or interested in using SHMS. We established an online questionnaire survey webpage on the Qualtrics platform. The questionnaire details can be found in Appendix H. We launched the link of the created webpage and managed the distribution and participant recruitment using a professional agency, Prolific. The sample characteristics of prescreen participants on Prolific platform included individuals whose primary language is English and who live in Australia, New Zealand, and the USA. Moreover, participants under 18 years old or those who answered NO to a filter question regarding their understanding of a smart health monitoring system (SHMS) were excluded. Based on a statistical power analysis using G Power v3.1 software, a sample size of 208 is suggested to be appropriate for the complete model (Faul et al., 2007). Overall, 377 valid responses were received after removing the incomplete and unqualified responses. The demographic information of the survey participants is summarized in Appendix Table C. 5.

The hypothesis-related measurement items were developed from sources tested in previous research. We used a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) to measure the key constructs of the model. All the constructs of the model are first-

order reflective constructs, except individual health empowerment, which is a reflective second-order construct, with four reflective first-order factors—competence of user, meaning of system usage, self-determination of user, and impact of system usage. The measurement items are presented in Appendix Table C. 6, with a comparison to the original items. For instance, to better align with the context of the current study, the wording of LEGP1 regarding the legislative protection construct was revised to: "I think the existing laws in my country are sufficient to protect my health data privacy," compared to the original, which stated: 'The existing laws in my country are sufficient to protect consumers' online privacy.' Additionally, several original items were not adapted due to their lack of relevance, such as the original item for the construct of ethical considerations, "Does not criticize subordinates without good reason," which was excluded.

The measurement and structural models were tested using Partial Least Squares-Structural Equation Modelling (PLS-SEM) SmartPLS v4 software. PLS-SEM is a causal-predictive approach to SEM that emphasizes prediction in assessing statistical models, where structures are developed to provide causal explanations (Hair et al., 2019). PLS-SEM is suitable for exploratory research (Benitez et al., 2020) and has been commonly applied in quantitative research to assess the relationship between variables in a privacy-related healthcare context (Dadhich et al., 2022; Hassandoust, Akhlaghpour, et al., 2021; Liu & Tao, 2022). Given these reasons, PLS-SEM was chosen for testing our complex framework.

Survey designs frequently suffer from common method bias (CMB). Common method bias is defined as the "variance that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al., 2003, p. 879). To offset CMB concerns in our study, we consulted procedural guidance and statistical tests by MacKenzie et al. (2011). The test results indicate that CMB is not a significant concern for this research. The procedural guidance and statistical tests are summarized in Appendix Table C. 7. Further, a pre-test of the questionnaire was run among 50 participants to fine tune the survey in order to improve the logical validity and reliability of the questions.

3.5.4 Quantitative Results

Measurement model assessment

Using PLS-SEM, we assessed the reliability and validity of the measurement model through several criteria, including indicator reliability, internal consistency, convergent validity, and discriminant validity of the instrument items (Chin, 2009). As shown in Table 3. 2, indicator reliability (loadings > 0.7), internal consistency reliability ($\alpha > 0.7$, CR > 0.7), and convergent

validity (average variance extracted or AVE > 0.5) were all confirmed to be satisfactory, except for CURE3, ETCO1, ETCO2, PRIV3, COME1, COME5, TRUS1 and TRUS2, which have been dropped from the model. To test the discriminant validity of the constructs, we followed HeteroTrait-MonoTrait (HTMT) criteria (Hair et al., 2023). HTMT values greater than 0.9 indicate the lack of discriminant validity between conceptually similar constructs. Based on the findings shown in Appendix Table C. 8, all HTMT values between the constructs were below 0.9 and in line with the requirement. The four first-order dimensions—competence of user, meaning of system usage, self-determination of user, and impact of system usage—serve as reflective indicators of the second-order construct, individual health empowerment. The calculated AVEs of the first-order constructs were greater than 0.50.

Table 3. 2

Convergent validity testing

Construct	Item	Std. loading of each item	Cronbach's alpha	Average variance extracted (AVE)
Legislative protection	LEGP1	0.914	0.863	0.785
	LEGP2	0.859		
	LEGP3	0.884		
Transparency	TRAN1	0.782	0.831	0.735
	TRAN2	0.916		
	TRAN3	0.869		
Cultural and religious differences	CURE1	0.915	0.837	0.757
	CURE2	0.933		
	CURE4	0.749		
Ethical considerations	ETCO3	0.879	0.841	0.758
	ETCO4	0.896		
	ETCO5	0.836		
Equity/Fairness	EQFA1	0.853	0.920	0.758
	EQFA2	0.899		
	EQFA3	0.910		
	EQFA4	0.843		
	EQFA5	0.847		
Security	SECU1	0.919	0.909	0.847
	SECU2	0.936		
	SECU3	0.905		
Privacy concerns	PRIV1	0.927	0.901	0.834
	PRIV2	0.884		
	PRIV4	0.928		
Individual health empowerment - Competence of user	COMP1	0.792	0.855	0.778
	COMP2	0.923		
	COMP3	0.924		
	MEAN1	0.837	0.858	0.779

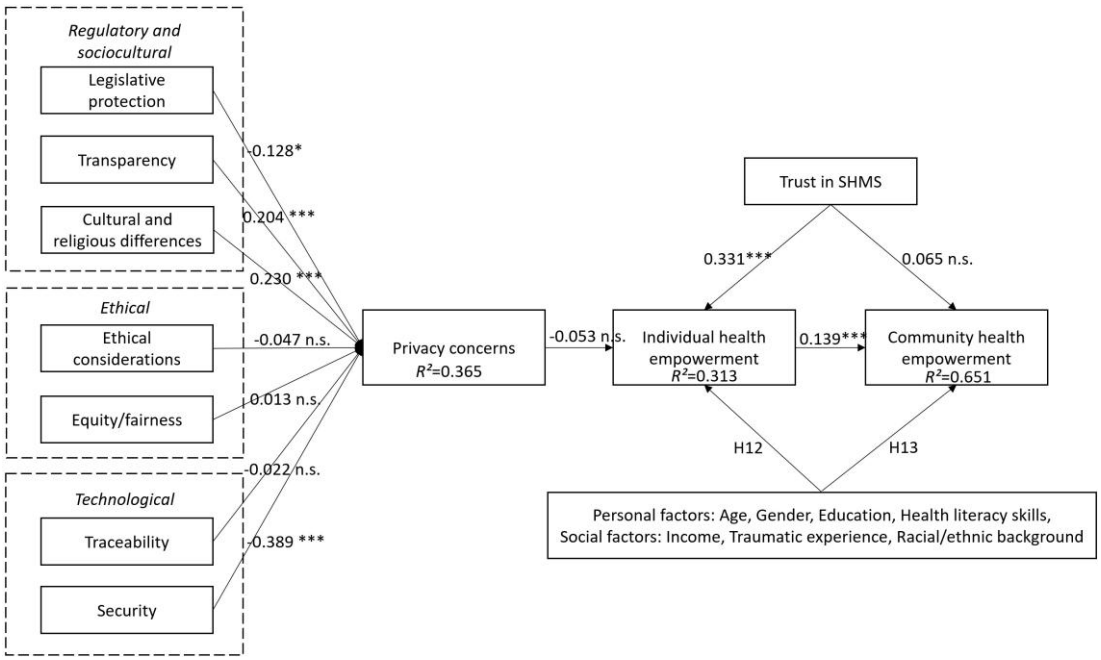
Individual health empowerment- - Meaning of system usage	MEAN2	0.900		
	MEAN3	0.909		
Individual health empowerment- - Self-determination of user	SELD1	0.846	0.847	0.767
	SELD2	0.911		
	SELD3	0.868		
Individual health empowerment- - Impact of system usage	IMPA1	0.856	0.794	0.711
	IMPA2	0.895		
	IMPA3	0.773		
Community health Empowerment	COME2	0.918	0.823	0.739
	COME3	0.726		
	COME4	0.920		
Trust	TRUS3	0.823	0.715	0.771
	TRUS4	0.930		

Structural model assessment

After confirming the adequacy of the measurement model, the next step of Study 2 involves a structural model assessment. This assessment entails evaluating collinearity among the exogenous constructs (Hair et al., 2019). The Variance Inflation Factor (VIF) test was performed for confirming collinearity among the constructs and revealed that the majority of the values were satisfactory, except for the PRIV3 item value in the construct of privacy concerns, which was then dropped. We ran bootstrapping with 5000 subsamples at a 5% significance value to test the path coefficients' statistical significance (Hair et al., 2019). The results of this assessment are shown in Figure 3. 3.

Figure 3. 3

Structural model results



Note. *p < 0.05, **p < 0.01 and ***p < 0.001.

In terms of tests of hypotheses H1-H3, the results support H1 (β = -0.128, *p* = 0.017) and indicate that legislative protection is a significant factor that negatively affects privacy concerns in SHMS contexts. This result aligns with numerous studies that suggest a negative influence of legislative protection on patients' information privacy concerns in different health informatics service contexts (e.g., Nguyen et al., 2022; Segura Anaya et al., 2018; Xu, 2019). The results also support hypothesis H3 (β = 0.230, *p* = 0.000). This finding also aligns with existing literature. For instance, Kulyk et al. (2020) explored the impact of culture on security and privacy risk perception in smart health environments across three countries. Velykoivanenko et al. (2021) evaluated the impact of data collection such as religion and sexual orientation in relation to privacy in the context of healthcare trackers (Velykoivanenko et al., 2021). The results, however, do not support hypothesis H2 (β = 0.204, *p* = 0.000), which posited a negatively significant relationship between transparency and privacy concerns. This finding is interesting and, while unanticipated, is consistent with an argument from the interviews in which one participant from the government health authority commented, "*Many people have privacy concerns based on assumptions, and once we educate them and attempt to manage health data in a more transparent way, they are gonna have more concerns*" (*participant#1*).

Hypotheses H4 and H5, referring to negative associations between ethical issues and privacy concerns, were not supported (β = -0.047, 0.013; *p* = 0.422, 0.798, respectively). These findings

suggest that neither ethical considerations nor equity/fairness are critical factors associated with privacy concerns in SHMSs, which is surprising given that earlier studies have shown that equity and ethical considerations (such as ethical commitment) are important for managing privacy in digital healthcare services (e.g., Maher et al., 2019; Princi & Krämer, 2020; Zakaria & Ramli, 2017).

With respect to the technological theme, the relationship between traceability and privacy concerns in H6 was not supported (β = -0.022, *p* = 0.652). While many previous studies report a negative relationship between traceability and privacy (e.g., Beaudin et al., 2006; Chadborn et al., 2019; Landau et al., 2010), the lack of significance in this relationship in our study might be due to an underlying understanding that SHMSs are designed around the concept of tracking data. In contrast, the results support H7, showing security negatively influences privacy concerns (β = -0.389, *p* = 0.000). Other studies also confirm that security reduces users' privacy concerns in various information health technology contexts (Graham, 2021; Talal et al., 2019; Yang et al., 2017).

Hypothesis H8, which hypothesized a negative association between privacy concerns and individual health empowerment was not supported (β = -0.053, *p* = 0.294). This finding contradicts previous studies that found privacy concerns have a negative impact on the health empowerment of individuals (e.g., Hajian et al., 2023; Mata-Cervantes et al., 2016; Nelson et al., 2016), showing that HIT privacy concerns play an important role in people's health empowerment. Consistent with prior literature (Rissel, 1994; Zimmerman, 2000), the results of Study 2 support H9 and confirm a positive association between individual health empowerment and community health empowerment (β = 0.139, *p* = 0.000). Previous studies suggest that trust in an HIT positively impacts both individual and community health empowerment (Jiang et al., 2022; McClair et al., 2021; Suárez Vázquez et al., 2017).

Our findings support trust as being positively related to individual health empowerment (β = 0.331, *p* = 0.000), but not community health empowerment (β = 0.065, *p* = 0.088). These findings provide support for hypothesis H10, but not H11, suggesting the trust in the HIT may be more individually focused, and individuals might not perceive the technology as directly contributing to the empowerment of entire communities. Regarding the personal and social factors in relation to individual health empowerment posited in H12, education, health literacy skills, income, traumatic experience, and racial/ethnic background were supported (β = -0.113, 0.316, 0.103, -0.126, 0.136; *p* = 0.016, 0.000, 0.029, 0.067, 0.004, respectively), while age and gender were not supported. These findings suggest that individuals with higher education or with more prior traumatic experience would have more concerns for their well-being.

Conversely, people with higher health literacy skills, higher income levels, or dependent on their racial/ethnic backgrounds, would likely have less concern for their well-being.

Regarding the personal and social factors in relation to community health empowerment posited in H13, age, education, health literacy skills, and traumatic experience were supported (β = -0.404, 0.115, 0.085, -0.457; p = 0.000, 0.001, 0.018, 0.000, respectively), while gender, income, and racial/ethnic background were not supported. These findings indicate that age and prior traumatic experience would likely negatively influence community health empowerment, while education and health literacy skills would positively influence community health empowerment.

Finally, we conducted a mediation test for a potential indirect link between privacy concerns and community health empowerment through the mediating factor of individual health empowerment. The findings reveal that privacy concerns have neither a significant negative direct (β = -0.008; *p* = 0.342), nor indirect effect on community health empowerment in the SHMS context. This finding challenges conventional expectations based on existing literature (e.g., Andrejevic et al., 2021; Demiris, 2006).

Multi-group analysis

Considering age differences in the context of SHMSs use is fundamental to tailoring interventions, addressing disparities, and promoting inclusive, effective, and ethical health technologies across the lifespan (Deng et al., 2018; Kim & Ho, 2021; Pirzada et al., 2021; Segura Anaya et al., 2018); thus, it is critical to determine if certain privacy norms may influence the perception of privacy concerns among different age groups; or whether the concept of empowerment aligns with individualistic values and communal health goals among different age groups. As such, we examined variations in age classifications on perceptions of individual and community health empowerment, specifically, the difference between elderly and non-elderly SHMS user groups. To do so, a multi-group analysis (MGA) implemented to compare whether the coefficient differences between the two groups are significant. The MGA analysis is built its logic through theorizing that privacy concerns that are negatively associated with individual health empowerment vary over one's lifespan in the SHMS context (Miltgen & Peyrat-Guillard, 2014; Schomakers & Ziefle, 2023).

MGA is a method for testing non-parametric significance. We particularly examined the *p*-value to determine the significance of different group-specific path coefficients. A *p*-value smaller than 0.50 or larger than 0.95 is considered significant (Karahoca et al., 2018; Sarstedt et al., 2011). We created an elderly group comprising individuals aged 65 and above using the survey data, and a non-elderly group consisting of participants below 65 years old.

Subsequently, we ran an MGA following the guide and procedures outlined by Shrout and Bolger (2002).

The MGA analysis results suggest that the two groups of people have significant differences in perceptions and understandings in terms of the effects between privacy concerns, individual health empowerment, community health empowerment, and other relationships proposed in the model. In terms of the antecedents of privacy concerns, the MGA analysis results show that security is significantly associated with privacy concerns among the non-elderly (β = -0.438, p = 0.000), but not among the elderly. In contrast, ethical considerations are considered a significant determinant of privacy concerns for SHMS use among the elderly (β = -0.333, p = 0.000), but not the non-elderly. However, the MGA results show that the relationship between cultural and religious differences and privacy is significant for both the elderly and non-elderly groups (β = 0.374, 0.190; p = 0.000, 0.001, respectively).

The MGA analysis results also show privacy concerns are a significant impacting factor of individual health empowerment among the non-elderly (β = -0.103, p = 0.049), but not among the elderly. Similarly, the relationship between individual and community health empowerment is significant among the non-elderly (β = 0.322, p = 0.000), but not the elderly. Trust in SHMSs is a significant factor of individual health empowerment among both the elderly and non-elderly (β = 0.325, 0.367; p = 0.000, 0.000, respectively). The findings also present significant influences of education and racial/ethnic factors among the non-elderly (β = -0.143, 0.112; p= 0.023, 0.045, respectively), but non-significant among the elderly. In terms of the factors hypothesized to affect community health empowerment, education is important to shape community health empowerment for the non-elderly (β= 0.199, p= 0.006), but not among the elderly. Additionally, income is found to be a significant factor in both the elderly and non-elderly (β = -0.479, -0.135; p= 0.038, 0.036, respectively).

3.5.5 Applicability Check

As an integral part of the research process, applicability checks allow practitioners to provide feedback to researchers concerning the research objects (such as models, processes, and theories) being developed or utilized in research (Rosemann & Vessey, 2008). To internalize our quantitative findings from the proposed model and improve the relevance of research to practice (Rosemann & Vessey, 2008), we performed a variation of applicability checks by carrying out follow-up interviews, taking into account scheduling constraints (Drechsler & Breth, 2019). These interviews involved five participants (see the participants with * in Appendix Table C. 3) from Study 1 and comprised the evaluations of three dimensions of

relevance: namely, *importance*, *accessibility*, and *applicability* under the guidelines by Rosemann and Vessey (2008).

Overall, the findings were perceived as important, accessible, and applicable to the specified SHMS contexts. In terms of *importance*, every participant observed that the findings were timely, important, and aligned with practical needs by addressing the contention between privacy concerns and health empowerment in SHMS. For example, one participant stated, "*You know, privacy issues, particularly the absence of informed information or inappropriate information shared in the system can set us back from using the system. However, it should be beneficial to our health management goals. I think the work you're doing is really important. I can truly see the value in what you're working to achieve here, which helps provide an important solution regarding how service providers better handle privacy practices in a real health monitoring environment*" (*Participant#3*). Another participant opined, "*The findings are really important that prompt us to re-think of privacy concerns in a specific monitoring system scenario and provide a fresh way to resolving the debate between privacy and health empowerment*" (*Participant#10*).

Accessibility involves evaluating whether the research is readable, understandable, and focuses on results rather than the research process (Klein et al., 2006; Rosemann & Vessey, 2008). In the interviews, we introduced our research objectives and the mixed-methods research design, and the key findings based on the proposed research model. Based on the introduction, all participants found our research and its relevant findings easy to read and understand. Considering that participants might have limited interest in delving into health empowerment theory, we chose not to provide the definition of the theory at the beginning. However, we noticed that two participants (*participant#4, #10*) encountered some challenges in grasping the research model. To address this issue, we promptly offered additional explanations regarding health empowerment theory. In response, they acknowledged that they found no difficulty in understanding the model design and its pertinent findings.

The *applicability* of research to practice emphasizes whether the paper to be published is complete, and whether it offers directions, guidance, and concrete recommendations (Klein et al., 2006; Rosemann & Vessey, 2008). All participants were not only of the opinion that our findings were complete but also believed that they could be implemented effectively in practice. One participant commented as follows: "*I think the themes and relationships are logically presented and seem worthy of testing in a real healthcare monitoring environment. For instance, I fully agree with the assumption that cultural differences have a major impact on privacy concerns, especially given the multicultural background of our country. People with*

different cultures can impact on their way how they perceive privacy concerns" (*participant#13*). Another participant added, "*I can see that testing the model, including its components and relationships, should have no challenge for those service providers involved health monitoring systems. It would undoubtedly assist them in considering privacy concerns and main factors and better managing users' health empowerment and improving overall health condition finally*" (*participant#4*). When we discussed the findings that suggested privacy concerns were not a significant factor in individual health empowerment, one participant commented, *"People, especially older folks, are much more focused on getting their health needs met. If there is any way to share their health information to get those health needs met, I would say a priority. It's very much more on having their needs met than how those needs are met"* (*participant#1*). In summary, the feedback collected during the applicability check interviews was positive and encouraging. It demonstrated that the participants understood our findings and also considered them important to be considered for implementation in practice.

3.6 Discussion

Prioritizing the value of health empowerment over the general values of health and privacy, we followed a developmental mixed-methods research approach to explore the contention between health and privacy values as it persists in the SHMSs of today and surface inconsistencies between the findings of our exploration and the assumptions that have driven the prevailing thoughts on the issue. Findings from the qualitative study (Study 1) of this research suggest that the legislative protection, transparency, cultural and religious differences, ethical considerations, equity, security, and traceability of an SHMS are influencing factors on individuals' privacy concerns in relation to individual and community health empowerment. Those findings also support other relationships among privacy concerns, trust, and individual and community health empowerment, which we subsequently tested in a quantitative study (Study 2). The findings from the quantitative study reveal several inconsistencies with the underlying assumptions that the prior HIT literature is built upon concerning the contention between health and privacy values.

Following the guidelines of Venkatesh and colleagues (Venkatesh et al., 2013; Venkatesh et al., 2016), we will now elaborate on the meta-inferences derived from the findings of both studies and discuss their implications. We describe three meta-inferences contrary to and challenging traditional assumptions regarding privacy concerns associated with health technologies, highlighting shifts in value priorities with age, and indicating diminished concerns for ethical and equity considerations related to privacy values. These findings also provide insights to the

policymakers, healthcare providers, and technology developers on individuals' impetuses for SHMS health empowerment.

3.6.1 Meta Inferences and Theoretical Implications

Meta-inference 1: our findings challenge the conventional assumption that privacy concerns should negatively impact both individual and community health empowerment.

The conventional assumption is that privacy concerns inherently hinder health-related advancements at both individual and collective levels (Agaku et al., 2014; Ali & Dang, 2022; Gao et al., 2015; Hassandoust, Akhlaghpour, et al., 2021; Seh et al., 2020). This is the trade-off between privacy loss and improved health outcomes that has been pervasive in the HIT literature for years. Contrary to this assumption, our findings suggest that the perceived trade-off between privacy concerns and health empowerment might not be as pronounced.

Elder individuals seem uninterested in concerns for their privacy and are more willing to prioritize the tangible benefits of health empowerment over potential privacy risks associated with smart health technologies. Similarly, while privacy is often considered a crucial factor in adopting health technologies at a community level, our findings propose that community health initiatives may not be significantly hindered by privacy apprehensions. This aligns with the findings from previous studies in similar contexts (e.g., Ebardo, 2018; Lee & Lee, 2020; Tran & Nguyen, 2021). Therefore, there might be a need to shift the conventional perspective that often assumes privacy concerns associated with the personal health data disclosure act as a barrier to the widespread acceptance and utilization of health technologies.

This overarching tendency underscores an emphasis on the perceived benefits of improved health outcomes, both at the personal and communal levels, which often take precedence over values associated with potential privacy loss. For many older individuals, the tangible advantages linked to health empowerment substantially influence the weighing of priorities (Esmaeilzadeh, 2019), thereby shaping a prevailing inclination towards embracing smart health technologies, even in the face of privacy-related apprehensions (Esmaeilzadeh, 2022). The SHMS benefits derived from health empowerment are often immediate and tangible. Monitoring vital signs, managing chronic conditions, and receiving timely health alerts contribute to a sense of control and well-being (Kang & Hwang, 2022; Princi & Krämer, 2020). In contrast, privacy concerns may seem abstract and distant, especially when weighed against concrete health improvements (Hallam & Zanella, 2017).

Regarding the community health considerations, individuals may adopt a collective benefit perspective (Schulz-Baldes et al., 2007). They may perceive that sharing health data for the

greater good of the community, such as contributing to public health well-being or early detection of health trends, outweighs or overrides individuals' privacy concerns in relation to using healthcare systems. Individuals may believe that certain concessions in individual privacy are justifiable for the benefit of the broader population (Mir et al., 2018).

Based on the findings of this study, trust in health systems (i.e., SHMSs) and community health programs can play a significant role. If individuals have confidence that health data is managed responsibly and the benefits extend to the broader community, they may be more willing to share information without heightened concerns about privacy. Individuals feel empowered by the idea that their shared health data contributes to community-level health decision making, resource allocation, or the development of targeted health interventions. Therefore, based on these findings, there is a need to reassess the dynamics of the relationship between privacy concerns and health empowerment. Factors beyond privacy considerations may play a more substantial role in influencing individual and community attitudes toward health technologies.

Meta-inference 2: the value of privacy relative to health and the attribution of community health empowerment on one's own health empowerment are not consistent across the span of one's lifetime.

The relative value of privacy to health is not static across one's lifetime and varies based on factors such as age and culture (Zou et al., 2024). For example, younger people may express more significant concerns about privacy loss than older people (Pirzada et al., 2021). Younger individuals, often referred to as digital natives, have grown up in an era where digital technologies and online interactions are prevalent. They might be more conscious and concerned about the privacy implications of sharing health-related information. In contrast, older people may not be as accustomed to the digital landscape and may not perceive the same level of privacy concerns in sharing health information online (Pirzada et al., 2021).

Moreover, older people, who may have different health priorities or perceptions of risk, might not see privacy concerns as being as important as their health empowerment, and they tend to prioritize the benefits of health-related technologies over potential privacy risks. On the other hand, younger people might perceive greater health risks associated with privacy breaches, leading to a stronger negative impact on their health empowerment. This could be due to concerns about the misuse of health data or potential discrimination based on health information. In addition, different age groups may have distinct cultural norms and expectations regarding privacy. Younger people usually place a higher value on personal data protection, influenced by changing societal attitudes, while older people may have different privacy expectations shaped by their experiences and trusting cultural backgrounds.

We also found that the attribution of community health empowerment to one's own health empowerment matters to the younger people and not older. As we get older, we may become more isolated and less attached to our communities (Donovan & Blazer, 2020) – this would understandably make us not feel as though the health of our communities has anything to do with our own health. Younger individuals might be more idealistic and community-oriented as they establish themselves in society and see their health as interconnected with the health of the broader community due to a sense of shared responsibility. In contrast, older individuals may prioritize personal well-being over community health, most likely due to the lack or limited extent of social contact with others (Donovan & Blazer, 2020; George et al., 2012), especially if they perceive a diminishing role or influence in their community, and they may have a more individualistic perspective on health, placing greater emphasis on personal experiences and less on community impact. Again, cultural and generational variations could also play a role. Younger generations might be more attuned to collective health empowerment due to cultural shifts and changing societal values, while older generations might retain a more traditional or individualistic viewpoint (North & Fiske, 2015). The differentiation in empowerment dynamics across age groups suggests that a one-size-fits-all approach is insufficient. Theoretical models should incorporate age-specific variables, acknowledging that younger and older users may require different empowerment strategies to maximize the benefits of SHMSs while mitigating privacy concerns.

Meta-inference 3: the role of ethics and equity considerations become inconsistent at best when the value of privacy is weighed against health.

Equity and fairness considerations of privacy loss may be perceived as abstract concepts for SHMS users. The immediate and tangible aspects of privacy breaches may overshadow abstract equity considerations. Moreover, the perceived advantages to individual health and well-being may be more concrete and tangible, leading individuals to focus on these aspects rather than abstract equity principles. This implies that when faced with health challenges, the urgency of addressing pressing problems may overshadow other values. Although ethical frameworks call for a balance between promoting health outcomes and respecting individuals' rights, ensuring that privacy safeguards are in place, and promoting transparency in health data practices (Khanna & Srivastava, 2020; Lankshear & Mason, 2001), individuals may be less concerned about ethical and equity considerations if they believe the benefits outweigh the potential risks to privacy. This might be because they are not fully aware of the ethical and equity considerations associated with privacy loss in the context of smart health systems. Lack of awareness or understanding of the broader implications may result in a greater emphasis on immediate health-related benefits. Moreover, if individuals trust the healthcare systems

(i.e., SHMS) and believe that their health data is handled responsibly, used for legitimate purposes, and is secure, they may be less inclined to raise ethical or equity-related concerns.

On the other hand, the findings of the study show that the elder group reports ethical considerations as a significant factor in relation to privacy concerns. As individuals grow older, accumulated life experiences, exposure to evolving ethical norms, and a deeper understanding of the societal context may contribute to a heightened ethical awareness. This increased ethical consciousness, observed in the elder group, indicates a more profound consideration of the moral implications associated with privacy loss. However, despite this ethical consciousness, as individuals age, there is a tendency to prioritize health and well-being over privacy concerns. This might be because of growing recognition of the importance of health in later stages of life, where the immediate and tangible benefits of health empowerment may outweigh abstract privacy issues.

3.6.2 Implications for Research and Practice

This study presents a notable opportunity to embrace contrarian thinking and explore alternative viewpoints, with the aim of gaining a deeper understanding of the intricate interplay of privacy and health values within the digital environments that SHMS users experience. It challenges the conventional notion that privacy concerns uniformly impede health empowerment across one's lifespan. As one of the pioneering papers reporting the prioritization of health empowerment over privacy concerns in SHMSs, our study offers implications for research and practical applications.

The implications of this research also encompass both theoretical extensions and important insights derived from the proposed research model and contradictory findings. This study contributes to the extension of health empowerment theory by applying it in a digital healthcare context, leading to a re-evaluation of the dynamics between privacy values and health empowerment within these specific environments. This extension allows us to develop the SHMS health empowerment research model, while also considering modern surveillance capabilities and community sharing opportunities. Moreover, our findings reflect how SHMSs facilitate health empowerment, emphasizing the enhancement of individuals' and communities' control over health data and outcomes. This aligns with health empowerment theory, which posits that empowerment is both an individual and collective process, significantly affecting health behaviors and outcomes. These insights reinforce health empowerment theory, demonstrating that empowerment is a critical factor in the adoption and effective use of SHMSs. This theory should continue to inform the design and implementation of SHMSs, ensuring that these systems provide users with the knowledge,

resources, and control necessary to feel empowered in managing their health. In achieving this, we find that health empowerment theory can be effectively aligned with the nuances of an SHMS environment.

Moreover, the findings of this study suggest contrasting insights that challenge the assumptions that underpin extant HIT research concerning the contention between privacy and health. Prioritizing the value of health empowerment over the traditional focus solely on health and privacy might seem counterintuitive, yet it presents a revolutionary proposition for the digital age. This shift is less about abandoning health or privacy entirely, and more about recognizing how empowerment acts as a powerful driver for achieving better health outcomes. As individuals gain knowledge, self-management skills, and agency, they become active participants in their health journey, making informed choices, seeking timely care, and experiencing deeper well-being through self-determination and control. This focus extends beyond health metrics, promoting individual and community benefits, while also tackling systemic inequities in access to needed health resources. It also unleashes the potential for collective action, as empowered individuals become advocates for their communities and a healthier society for all. While navigating the digital world requires balancing empowerment with data protection and ethical frameworks, prioritizing it allows us to harness technology for good, enabling both individuals and communities to take charge of their health.

Our findings show that privacy loss was a less formidable challenge and had no real potentially beneficial consequences beyond advantages to one's own health. This insight is an important contribution that is counter to expectations derived from prior literature. It helps to argue that the prior literature perspective on the value of privacy relative to health is a historical perspective grounded in healthcare contexts that did not involve digital and community sharing opportunities. Also, in contrast to traditional literature on health empowerment theories which predominantly focused on individual agency, this study introduces insights into community-level health empowerment. It challenges assumptions that privacy concerns universally impede collective health initiatives. Therefore, it underscores the need to consider communal dynamics in the health empowerment framework. Finally, the study aids in advancing a positive narrative around health empowerment. By highlighting that privacy concerns may not be insurmountable obstacles or even obstacles at all for certain groups, it encourages a more optimistic perspective on the role of technology in fostering health empowerment at both individual and community levels.

In practical terms, the findings suggest SHMS practitioners should reassess the dynamics of the relationship between privacy concerns and health empowerment. The subsequent section

summarizes unconventional implications for practitioners in the SHMS domain to contemplate. Emphasizing the perceived benefits of improved health outcomes both at the personal and communal levels would be an effective strategy to address the contention between privacy and health empowerment, because such benefits often take precedence in privacy values in SHMS environments. Factors other than privacy concerns could have a more pronounced impact on shaping individual and community perspectives regarding HIT.

Our findings also show that the value of privacy relative to health is not consistent across the span of one's lifetime. It implies that individuals under the age of 65 generally prioritize personal data protection more, influenced by changing societal attitudes, whereas older individuals may have distinct privacy expectations shaped by their experiences and trusting cultural backgrounds. Thus, SHMS practitioners are strongly encouraged to consider age as a significant factor when formulating privacy-related strategies to better serve SHMS users. Challenging the conventional notion that privacy loss holds ethical and equitable value, our findings also suggest that the significance of individual health empowerment may surpass ethical concerns associated with privacy loss, especially when the outcome involves improved healthcare. Thus, SHMS practitioners should be aware that the perceived advantages to individual health and well-being may be more concrete and tangible, prompting individuals to prioritize these aspects over abstract ethical principles.

3.6.3 Limitations and Future Studies

Like all research studies, this study has a few limitations. However, those limitations provide future research opportunities. While our findings suggest a tendency for individuals to prioritize health over privacy when facing health issues, this conclusion should be viewed within the context of our study's limitations and the need for further research to validate these results. The survey results may be impacted by sample selection bias. Respondents who participated in this survey were individuals from Australia, New Zealand, and the United States at the time of the survey, which can be considered as limiting the generalizability of this study, considering the importance of geographical, regulatory, and cultural (localization) factors in individuals and community health empowerment. Therefore, future research may consider approaching individuals in the context of other countries. Another limitation is that in this study we are dealing with perspectives of potential SHMS users rather than actual experiences from real users. Future research could enhance the study by incorporating the insights and feedback from individuals who have practical experience with SHMS, allowing for a more comprehensive understanding of the dynamics between privacy concerns and health empowerment.

The unexpected findings, challenging preconceived notions about the negative impact of privacy concerns on both personal and community health empowerment, pave the way for a new avenue in future research. For instance, transparency as a significant factor of privacy concerns can be further explored from a dual perspective. Clear distinctions for cultural and religious differences, ethical considerations, and equity/fairness remain crucial and could be better elucidated in both qualitative interviews and quantitative surveys. The findings also suggest a significant tendency towards paradoxical behavior in smart health monitoring contexts. Concrete solutions designed to address this paradoxical behavior within SHMSs are currently undeveloped and warrant greater attention in future research. These aspects are prone to confusion during discussions on privacy issues. Moreover, although the factor of coordination among individual users and service providers was not included due to reliability and validity issues, it should be included in future examinations as it is still an essential contextual factor related to privacy concerns and data governance. The study also suggests exploring the evolving dynamics of health empowerment. Researchers can look deeper from a contrarian perspective into the interplay between individual and community empowerment, privacy considerations, and the evolving landscape of health technologies.

3.7 Conclusion

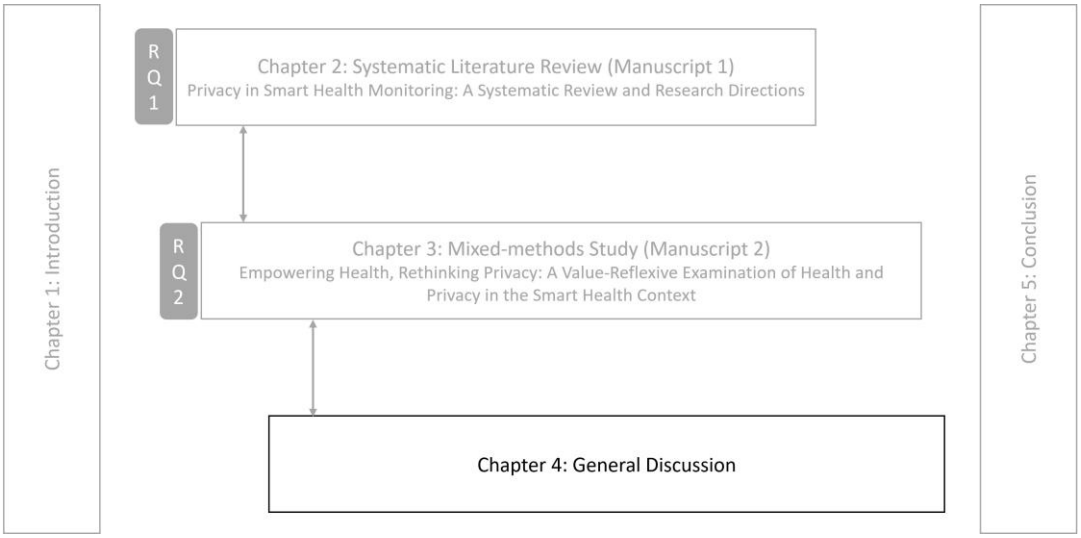
In response to a special issue call for employing contrarian thinking by problematizing values that define the digital world, our aim was to explore the contention between health and privacy values in SHMS and surface inconsistencies and disparities between our exploration's findings and the prevailing thoughts on the value of privacy in HIT use. Our findings challenge the conventional belief that privacy concerns should negatively impact both personal and community health empowerment. We also show that the value of privacy relative to health is not consistent across the span of one's lifetime and that the role of ethics and equity considerations become inconsistent at best when the value of privacy is weighed against health. This study lays the groundwork for future studies by offering a notable opportunity to adopt contrarian thinking and question the conventional belief that privacy concerns uniformly impede health empowerment throughout one's life.

Preface to Chapter 4

Chapter 4 provides a comprehensive discussion on the key findings and contributions of Chapters 2 and 3. It offers implications for research and practice, identifies future research directions, and acknowledges some limitations. The position of Chapter 4 in this thesis is illustrated in Figure 3. 4.

Figure 3. 4

The position of Chapter 4 in the thesis



Chapter 4 General Discussion

This thesis adopted a post-positivist approach. The findings showed that the reality of privacy phenomena and their impact on health empowerment in the context of SHMSs have been imperfectly explored but grants such reality can be discovered as accurately as possible. Using this approach, a comprehensive SLR was carried out as detailed in Manuscript 1 (see Chapter 2). The SLR addresses first research question (RQ1): *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?* Answering this question involved addressing criticisms regarding the incomplete contextualization of privacy in existing smart health monitoring studies. Based on an analysis of 49 peer-reviewed articles, a comprehensive understanding was gained of the issues involved and a contextual framework was developed (see Figure 2. 2). Overall, this review uncovered the reality of privacy phenomena studied in the reviewed literature, presenting contextualized privacy in terms of definitions and contextualization, privacy-related proxies, antecedents, and outcomes. The findings also highlighted the contextual matters of surveillance and stakeholder dynamics in the context of SHMSs. All these contributed to a comprehensive understanding of contextualized privacy in the SHMS context.

More essentially, this review work made it possible to identify existing knowledge gaps and potential research avenues. This significantly aligned with the research purpose of this thesis and inspired further investigation into the second research question (RQ2): *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?* Research avenues resulting from the review work inspired the development of the rest of the thesis. For example, Avenue 2 highlighted the importance of multi-level stakeholder analysis as another promising avenue for research on privacy in SHMS contexts (see future research Avenue #2 in Chapter 2). It indicated that the existing literature has provided insufficient analysis across various groups (e.g., individual, group, community) regarding the antecedents and outcomes of privacy phenomena in SHMS contexts. Exploring multi-level stakeholders is important for mapping a complete picture of privacy conceptualization and crucial for understanding the mechanisms and reasons behind the occurrence of privacy-related concerns (Ancona et al., 2001). Thus, rather than focusing solely on a single stakeholder such as individuals' perceptions, the study broadened its investigation to the multi-level using mixed methods. A community-level approach was found to be particularly crucial for research on HIT, as improving community health is the primary and ultimate goal of remotely delivered virtual healthcare ecosystems like SHMSs (Schiavone et al., 2021). Considering the importance of community health, privacy concerns were

explored in relation to individual and community-level health empowerment in SHMS contexts using health empowerment theory. Therefore, the analysis in Manuscript 2 not only focused on health empowerment of individuals but also introduced insights into community-level health empowerment (see Chapter 3). Based on Avenue 2, the model developed from the empirical study in Chapter 3 included three key constructs: privacy concerns, individual health empowerment, and community health empowerment.

Avenue 3 was another future research avenue that emerged from the review study, and highlighted the need for a mixed-methods design rather than using a single method to investigate the privacy dynamic in SHMSs contexts (see future research Avenue #3 in Chapter 2). A mixed-methods approach allows researchers to address exploratory questions within the same study inquiry (Venkatesh et al., 2013). It enables a holistic understanding and integrative insights into findings from a combination of qualitative and quantitative aspects, which strikes a balance between depth and breadth (Venkatesh et al., 2013). Moreover, this specific design is particularly suitable for exploring new contexts where issues are challenging to explain or describe using existing views (Ågerfalk, 2013). Further justification for employing a developmental mixed-methods design in this research can be found in Appendix Table C. 2. Given these methodological benefits, a mixed-methods approach was employed in Manuscript 2 to explore privacy and health in the context of SHMSs (see Chapter 3). This approach is based on a sequential two-stage design incorporating both qualitative and quantitative empirical studies. Manuscript 2 included a close examination of the reality of privacy concerns in SHMSs, identifying the important factors that influence these concerns and exploring their impact on privacy in relation to health empowerment within SHMSs.

Avenue 5 highlighted the significance of theory in the IS field that lies in its ability to explain the what, why, and/or how of phenomena (Mueller & Urbach, 2017). Oversimplifying theory adoptions falls short of researchers' ambitions to address the complex nature of privacy issues within SHMS contexts. While embracing a broader perspective that effectively addresses the complexity of SHMS contexts, researchers are encouraged adopt theories that go beyond offering simple causal explanations. As mentioned in Chapter 2, scholars can consider dynamic and longitudinal perspectives using process theories/models and stage theories. For instance, Nelson et al. (2016) exemplify this approach in response to Avenue 5, acknowledging the significant outcome of using smart trackers with both individuals and society at large. Adopting the self-regulation theory, a process theory, they identified key elements contributing to the health empowering capabilities of smart trackers. Inspired by Avenues 2 and 5, this study applied health empowerment theory from the empirical study in Manuscript 2. Health empowerment theory emphasizes the ongoing process through which individuals gain control

over their health and health-related activities in a broader sense, i.e., a professional community (Rissel, 1994; Spreitzer, 1995). It involves a series of activities and interactions that result in greater health empowerment within the community. The study used health empowerment theory to achieve comprehensive explanations for privacy concerns from a dynamic perspective relating to both individual and community health improvement (see Chapter 3).

The remaining sections of this chapter discuss the findings based on the research questions addressed in Chapters 2 and 3. Following that, research implications, practical implications, future research directions, and the limitations of the study are discussed.

4.1 Key Findings & Contributions

This section summarizes the findings from Chapter 2 and Chapter 3 and responds to the research questions of this thesis from an overall perspective. The discussions can be read in conjunction with Table 4. 1. This table is presented at the end of this section, summarizing the key findings and contributions of Chapters 2 and 3.

4.4.1 Findings and Contributions of Chapter 2

Findings of Chapter 2. In Chapter 2, the research question (RQ1) was: *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?* This question was posed for the following reasons. Researchers often encounter challenges in effectively communicating the meaning of privacy through clear definitions and limited perspective of privacy to a single stakeholder (e.g., Bhatt & Chakraborty, 2020; Dadhich et al., 2022; Peek et al., 2016; Ravishankar et al., 2015). However, contextualized privacy definitions are either absent or articulated poorly in the existing literature. These weaknesses create contextual ambiguity, which impedes researchers' abilities to set their studies' direction, choose theories, and interpret their findings (Dinev et al., 2013).

The findings in Chapter 2 indicated significant shortcomings as follows. First, a consistent and sufficient definition of privacy from diverse conceptual perspectives has been generally underdeveloped in the existing literature. Only a third of the reviewed studies explicitly defined or implicitly described privacy phenomena in their focal areas. Yet, clarifying the contextualized definition of privacy from one or multiple perspectives can enrich the understanding of privacy within multidisciplinary environments like smart health monitoring (Zahra et al., 2014). Second, the existing literature has provided insufficient analysis across various levels regarding the antecedents and outcomes of privacy phenomena in smart health monitoring contexts. Analysis of the findings showed that the antecedents from other levels

such as societal, environmental, cross-cultural, or national levels, were seldom explored. Lack of multi-level entity analysis makes it difficult to understand how privacy concerns interplay and influence each other across these levels (Smith et al., 2011). This can result in an incomplete picture of how privacy is managed and perceived among different groups within HIT environments.

Third, a significant dearth in the application of the theory was identified, with an overreliance on TAM- or UTAUT-related models. While the absence of relevant theories raises questions about the validity and value of the research (Sutton & Staw, 1995), studies using theories were found to commonly employ theoretical frameworks like TAM, UTAUT, and UTAUT 2 in order to understand how people adopt and use health information technologies. However, such models have faced criticism for being overly simplistic and limited. They concentrate solely on individuals' perceptions and intentions to use technologies, lacking specificity related to the health domain (Lee et al., 2003; Shachak et al., 2019). Fourth, only a small subset of studies employed a mixed-methods approach (e.g., Arar et al., 2021; Cristiano et al., 2022a). However, a mixed-methods design is particularly useful because it helps provide a holistic understanding of a phenomenon at an early research stage (Venkatesh et al., 2013). It is hard to define a research program as truly being mixed-methods research unless it provides combining findings from both qualitative and quantitative studies (Venkatesh et al., 2013).

Fifth, only a few studies explored surveillance-related contextual factors (e.g., Beaudin et al., 2006; Chadborn et al., 2019). However, surveillance has been recognized as an important theme in the reviewed literature. The use of surveillance or monitoring devices (or services) without appropriate privacy protection mechanisms in the system is very likely to stimulate competing demands for privacy and data sharing when individuals use SHMSs, which can result in individuals' unwillingness to employ smart health devices or services (Pirzada et al., 2021; Prati et al., 2019; Westin, 2003).

The findings also rectified the shortcomings of reviewed studies by providing a comprehensive review of privacy contextualization in SHMSs. It included examining privacy definitions from various perspectives, and reviewing the antecedents and outcomes of privacy, relevant theories, methodological transparency, research agenda, and other pertinent scopes.

Contributions of Chapter 2. Chapter 2 offers significant contributions to the entire thesis. First, it provides a contextual framework for a comprehensive understanding of privacy in SHMSs. Second, it highlights multi-level analysis as an important research avenue for researchers on privacy in SHMS contexts. Motivated by multi-level analysis, the empirical study (Manuscript 2) can investigate both individual and community-level health empowerment rather than

focusing solely on the individual level. Third, Chapter 2 supports the importance of deriving value from incorporating more theories that better capture the intricate dynamics of smart health environments. It encourages researchers to embrace a broader perspective (rather than TAM-related frameworks) to effectively address the complexity of smart health contexts. Specifically, the findings of Chapter 2 suggest that researchers can integrate psychological and socio-cultural theories, including psychological empowerment and balance theory, in order to offer deeper insights into multi-entity engagement and the broader social implications of SHMSs. Given these contributions, the study employed health empowerment theory – a psychological theory to address the privacy phenomenon in a complex health monitoring context.

Fourth, the findings underscore the value of the mixed-methods approach, because a mixed-methods approach facilitates a comprehensive investigation of privacy dynamics in the context of smart health monitoring, thereby enhancing the depth and breadth of research findings in this critical area (Venkatesh et al., 2013). Moreover, the findings contribute to informing the developmental purpose of the study's mixed-methods design. Finally, the findings highlight the importance of exploring surveillance-related contextual factors when examining privacy phenomena in SHMSs, making use of contextual factors (e.g., traceability) in the research model development in Chapter 3.

4.4.2 Findings and Contributions of Chapter 3

Overall, the aim of Chapter 3 was to explore the contention between health and privacy values as it persists in SHMSs today, as well as the surface inconsistencies and disparities between the findings of the study's exploration and the prevailing thoughts on the value of privacy in health information technology (HIT) use. Based on this aim, the research question (RQ2) of Chapter 3 was as follows: *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?*

Incorporating the key findings and contributions of Chapter 2, a mixed-methods study was conducted in order to comprehensively investigate the privacy dynamic in the context of smart health monitoring. Health empowerment theory was utilized, because, as mentioned earlier, it made it possible to derive significant value and offer a broader perspective that effectively addresses the complexity of smart health contexts. Hypotheses were proposed and developed by utilizing the SHMS health empowerment model, taking into account a surveillance-related contextual factor (i.e., traceability).

Qualitative Findings of Chapter 3. The qualitative findings obtained from Study 1 of Chapter 3 related to seven antecedent factors impacting individuals' privacy concerns with SHMSs in terms of three value-based themes. As summarized in Table 4. 1, these factors are *legislative protection*, *transparency*, and *cultural and religious differences* (regulatory and sociocultural theme), *ethical considerations* and *equity/fairness* (ethical theme), and *traceability* and *security* (technological theme). The findings also suggested a potential association between individuals' privacy concerns surrounding the use of SHMSs and individual health empowerment, a potential association between individual and community health empowerment in the use of SHMSs, and a potential association between individual and community health empowerment in the use of SHMSs. Details of the qualitative findings can be found in Appendix Table C. 4.

Quantitative Finding of Chapter 3. The quantitative findings from Study 2 of Chapter 3 mainly encompassed a group of confirmations for the proposed hypothesis. As summarized in Table 4. 1, these findings confirmed that legislative protection is negatively associated with privacy concerns in relation to SHMS. *Legislative protection* of data privacy refers to the right to information, provisions prohibiting or restricting the use of mechanisms of data governance, rules on IT-security-legislation, and provisions supporting the use of mechanisms (Weber, 2010). *Transparency* refers to ensuring everything is visible, denoting one's openness and open communication when pursuing trustworthiness (Kim et al., 2014). The findings confirmed that transparency is negatively associated with privacy concerns in relation to SHMS. *Cultural and religious differences* influence people's attitudes and behaviors when they are involved in using healthcare monitoring devices (Karadag et al., 2019). The findings confirmed that cultural and religious differences are positively associated with privacy concerns in relation to SHMSs. *Security* is a central constant topic and security management includes the execution of risk assessments, the setup of data security roles, and the definition of data security policies, standards, and procedures (Abraham et al., 2019). According to the quantitative findings, security is negatively associated with privacy concerns in relation to SHMSs.

The quantitative findings supported that *individual health empowerment* is positively associated with *community health empowerment*, aligning with the proposal of health empowerment theory where community health empowerment has been recognized as a raised level of individual health empowerment (Rissel, 1994). Finally, *trust* occurs when a party believes that the other party has characteristics advantageous to its own interest (Chang & Fang, 2013; McKnight & Chervany, 2001). It is associated with many themes such as the motivation, credibility, transparency, and responsibility of a system (Mittelstadt, 2017). The

findings confirmed that trust in SHMSs is positively associated with individual health empowerment.

Contributions of Chapter 3. The qualitative stage (Study 1) of Chapter 3 contributed to the proposal of hypotheses and the development of the SHMS Health Empowerment model. This model (see Figure 3. 2 in Chapter 3) presents a testable framework capturing the relationships between identified antecedent factors – grouped into regulatory, sociocultural, ethical, and technological themes – and their impact on privacy concerns in SHMSs. The model also elucidates the potential associations among privacy concerns, individual health empowerment, community health empowerment, and trust, offering a comprehensive understanding of these dynamics in SHMSs. This model and the relevant hypotheses allowed the study to proceed to the quantitative stage (Study 2) of Chapter 3.

The quantitative stage (Study 2) of Chapter 3 focused on testing the assumptions in the model from the qualitative stage through an online questionnaire survey. Three key contributions from the findings can be considered as follows. First, the quantitative findings in this stage challenge conventional belief in the relationship between privacy concerns and health empowerment, concluding that the impact of privacy concerns on both individual and community health empowerment is not uniformly negative. In other words, the perceived trade-off between privacy concerns and health empowerment might not be as pronounced as a number of prior studies believe. The findings propose that community health initiatives may not be significantly hindered by privacy apprehensions. Therefore, there may be a need to shift the conventional perspective that often assumes privacy concerns associated with personal health data disclosure act as a barrier to the widespread acceptance and utilization of health technologies.

Another contribution from the quantitative findings is indicating that the importance of privacy relative to health empowerment varies across different life stages, indicating that the value placed on privacy is not consistent throughout one's lifetime. In other words, the relative value of privacy to health is not static across one's lifetime and varies based on factors such as age and culture. For instance, younger individuals might be more idealistic and community oriented as they are establishing themselves in society and see their health as interconnected with the health of the broader community based on a sense of shared responsibility. In contrast, older individuals may prioritize personal well-being over community health, especially if they perceive a diminishing role or influence in their community, and they may have a more individualistic perspective on health, placing greater emphasis on personal experiences and less on community impact.

Finally, the quantitative findings indicate that ethical and equity considerations have variable significance when trading off or balancing the value of privacy against health benefits, suggesting that these relationships can be complex and context dependent. When faced with health challenges, the urgency of addressing pressing problems may overshadow other values. Although ethical frameworks advocate for balancing the promotion of health outcomes with respect for individuals' rights, ensuring that privacy has safeguards, and promoting transparency in health data practices (Khanna & Srivastava, 2020; Lankshear & Mason, 2001), individuals may be less concerned about ethical and equity considerations if they believe the benefits outweigh the potential risks to privacy. In short, the role of ethics and equity considerations becomes inconsistent when the value of privacy is weighed against health.

Table 4. 1

Key findings and contributions of Chapters 2 and 3

Thesis chapter	Approach	Key findings of this thesis	Key contributions of this thesis
Chapter 2: Privacy in Smart Health Monitoring: A Systematic Literature Review (Manuscript 1) RQ1: What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?	Systematic literature review	● A consistent and sufficient definition of privacy from diverse conceptual perspectives was generally underdeveloped in the existing literature. ● The existing literature provided insufficient analysis across various levels regarding the antecedents and outcomes of privacy phenomena in smart health monitoring contexts.	● Provided a contextual framework for a comprehensive understanding of privacy in SHMSs.
		● Only a small portion of the reviewed literature focused on entities beyond individual users.	● Recognized multi-level analysis as an important research avenue for researchers on privacy in SHMSs.
		● A significant dearth in the application of theory was identified, with an overreliance on TAM- or UTAUT-related models.	● Recognized the significant value of incorporating more comprehensive theories that capture the intricate dynamics of smart health environments. ● Understood that integrating psychological and socio-cultural theories (such as psychological empowerment and balance theory) could offer deeper insights into multi-entity engagement and the broader social implications of SHMSs. Adopted health empowerment theory, a psychological theory to address the privacy phenomenon in a complex health monitoring context.
		● Only a small subset of studies employed a mixed methods approach, although this approach allows researchers to comprehensively investigate the privacy dynamic in the context of smart health monitoring.	● Highlighted the value of a mixed-methods approach to comprehensively investigate the multifaceted privacy concerns inherent in SHMSs, thereby enhancing the depth and breadth of research findings in this critical area.
		● Only a few studies explored surveillance-related contextual factors, although surveillance was recognized as an important theme in the reviewed literature.	● Supported the importance of exploring surveillance-related contextual factors in terms of the privacy phenomenon resulting from the use of SHMSs. ● Involved a contextual factor (i.e., traceability) in the research model development.
Chapter 3: Health and Privacy: A Value-reflexive Examination (Manuscript 2) RQ2: *How do users' value perceptions of*	Mixed-methods: 1) Qualitative study	● Captured seven antecedent factors related to three value-based themes impacting individuals' privacy concerns with SHMSs: – Regulatory and sociocultural theme: 1) Legislative protection 2) Transparency 3) Cultural and religious differences – Ethical theme: 4) Ethical considerations 5) Equity/fairness – Technological theme: 6) Traceability 7) Security ● Identified a potential association between individuals' privacy concerns when using SHMSs and individual health empowerment. ● Identified a potential association between individual and community health empowerments in the use of SHMSs.	● Developed hypotheses and constructed the SHMS Health Empowerment Model, anchoring in Health Empowerment Theory. – The model presents a testable framework capturing the relationships between identified antecedent factors and their impact on privacy concerns in SHMSs. – The model elucidated the potential associations among privacy concerns, individual health empowerment, community health empowerment, and trust, offering a comprehensive understanding of these dynamics.

health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?		● Identified that trust has a potential association with individual and community health empowerment in the use of SHMSs. ● Captured personal and social factors significantly related to both individual health empowerment and community health empowerment.	
	Mixed-methods: 2) Quantitative study	Tested the hypotheses: ● Legislative protection is negatively associated with privacy concerns in relation to SHMSs. ● Transparency is negatively associated with privacy concerns in relation to SHMSs. ● Cultural and religious differences are positively associated with privacy concerns in relation to SHMSs. ● Security is negatively associated with privacy concerns in relation to SHMSs. ● Individual health empowerment is positively associated with community health empowerment. ● Trust in SHMSs is positively associated with individual health empowerment. ● Privacy concerns are a significant impacting factor on individual health empowerment among the non-elderly, but not among the elderly.	● The quantitative findings of this mixed-methods study challenged conventional belief in the relationship between privacy concerns and health empowerment by viewing the impact of privacy concerns on both individual and community health empowerment as not uniformly negative. ● Suggested that the importance of privacy relative to health empowerment varies across different life stages, indicating that the value placed on privacy is not consistent throughout one's lifetime. ● Highlighted that ethical and equity considerations demonstrate variable significance when trading off or balancing the value of privacy against health benefits, suggesting that these relationships can be complex and context-dependent.

4.1 Implications for Research

As detailed in the discussion above, in respect to Chapter 2, the implications for research consist in developing a contextual framework for SHMS privacy research that accommodates the diverse perspectives and contextual nuances of privacy in the context of SHMSs. The framework (see Figure 2. 2) provides valuable insights for scholars aiming to understand the multifaceted privacy concerns in SHMS settings. Privacy is a multidisciplinary concept with a multifaceted nature rooted in diverse justifications (Burgoon, 1982; Smith et al., 2011). By understanding its multi-faceted nature, researchers can better understand the diverse privacy concerns and needs that arise in various contexts and different technologies (Mulligan et al., 2016). A hybrid model is ideally suited for exploring events that prompt specific changes in outcomes or states. It would enable a more comprehensive understanding and explanation within a specific IS field (Burton-Jones et al., 2015; de Guinea & Webster, 2017). The framework is motivated by the notion of this hybrid model and the antecedents–privacy concerns–outcomes (APCO) model of information privacy (Smith et al., 2011). The framework distinguishes between antecedents of privacy, privacy phenomena, and outcomes of privacy, leveraging a hybrid perspective.

The framework addresses the literature gap, identifying the fragmented and limited exploration of contextualizing privacy in the area of SHMSs. The implications of the study include six potential research avenues with relevant research questions for future researchers to utilize. The avenues are in terms of *contextualized definition*, *multi-level analysis*, *methods of analysis*, *stakeholder analysis*, *contributing to IS theories*, and *investigating less-explored aspects of emerging themes from the present review* of Chapter 2. For example, one of the avenues implies that clarifying the contextual and dynamic nature of privacy through a clarified definition is a pragmatic approach for accurately grasping and analyzing privacy issues. Researchers interested in this avenue are encouraged to explore research questions such as: *Privacy holds diverse interpretations. How do researchers define it pragmatically?* Moreover, these avenues laid the ground for the remainder of the present research. As discussed earlier, this research followed the second and third avenues by undertaking a multi-level exploration of privacy and health in SHMS settings and using a mixed-method design. Details of the avenues and relevant research questions can be found in Chapter 2.

Chapter 3 suggested a notable opportunity for future research to embrace contrarian thinking and explore alternative viewpoints. This would help researchers to gain a deeper understanding of the intricate interplay of privacy and health values within the digital environments that SHMS users experience. The findings suggest a nuanced perspective is

needed on the relationship between privacy concerns and health empowerment across an individual's lifespan. Additionally, the findings invite a reconsideration of several assumptions that have shaped existing research on the balance between privacy and health. Prioritizing the value of health empowerment over the traditional focus on solely health and privacy might seem counterintuitive, yet it presents a revolutionary proposition for the digital age. Given that privacy concerns may not be insuperable obstacles or even obstacles at all for certain groups, the findings imply a more optimistic perspective on the role of technology in fostering health empowerment at both individual and community levels.

The overall implications of the research encompass both theoretical extensions and insights derived from the proposed research model and its contradictory findings. The empirical study of Chapter 3 contributes to an extension of health empowerment theory and applying it in a digital healthcare context, leading to a re-evaluation of the dynamics between privacy values and health empowerment within SHMSs. In contrast to traditional literature on health empowerment theories, which predominantly focused on the individual users, this study introduces insights into community-level health empowerment. In other words, this extension allows for the incorporation of both individual and community levels of empowerment into the SHMS health empowerment research model, taking into account modern surveillance capabilities and opportunities for community sharing. This extension aids in challenging assumptions that privacy concerns universally impede collective health initiatives. It underscores the need to consider communal dynamics in the health empowerment framework. Moreover, applying health empowerment theory to explore the dynamics between health and privacy in the SHMS context can help explain the traditional assumptions of need-related theories like Maslow's hierarchy of needs. Following Maslow's hierarchy principle, health is a basic-level need, while privacy is a higher-level need. This implies that in the SHMS context, individual users of SHMSs raise privacy issues only after their health needs have been adequately addressed by the system. The findings of the present study are in line with Maslow's hierarchy, revealing that if people's health is secure, they may care about privacy in their SHMS use, particularly across age groups.

4.2 Implications for Practice

Implementing privacy protection in smart health monitoring is challenging due to the intricate network of stakeholders and their diverse protection mechanisms. The participation of various stakeholders has been found to provoke privacy issues among individuals, serving as a significant antecedent factor and outcome of privacy concerns. The review work in Chapter 2 emphasized four key stakeholders within SHMSs: individuals, healthcare providers, smart

technology providers, and government authorities (OECD, 2015; Peek et al., 2016; Swinkels et al., 2018).

Individuals include any end-users of smart health applications. In the dynamic environment of smart health monitoring, where collaboration among stakeholders is paramount, it is crucial for individual users to recognize themselves not only as beneficiaries but also as vital stakeholders, given their active involvement. Individuals' perceptions of privacy and their surveillance concerns are found to block them from using health monitoring technologies and sharing their health data with other stakeholders in smart health monitoring systems. However, individuals should understand the duality of privacy and surveillance in smart health monitoring applications.

In respect to *healthcare providers*, the adoption of smart health monitoring technologies can offer advantages to healthcare providers, including enhanced operational efficiency, cost reductions in patient care delivery, improved quality measurement, and expanded reporting capabilities. However, concerns about privacy and associated challenges may arise if healthcare providers encounter difficulties in implementing effective data governance mechanisms or if there is a lack of meaningful awareness among this group of stakeholders. Healthcare providers should develop data governance mechanisms for their privacy activities.

Smart technology providers are at the forefront of introducing surveillance technologies in smart health monitoring applications. Privacy issues have been demonstrated to influence the design, strategies, and development of functionalities within smart health systems when considered from a design thinking lens. There is a significant amount of literature on privacy-focused technologies in smart health monitoring applications. However, there is relatively little research that delves into the negative impacts of privacy concerns on smart technology providers. Therefore, it is imperative for smart technology providers to have a thorough understanding of the privacy concerns associated with their technologies.

Governmental authorities include government agencies, policymakers, and legislators that help achieve better data governance among stakeholders. However, antecedents, including individual-level regulatory expectations and trust in business operators and stakeholder-level health tracking data mechanisms, are all associated with the active involvement of government authorities. Moreover, smart health initiatives, like the development of smart homes, are intricately linked with the overarching objective of smart city development pursued by local government authorities. Therefore, it is imperative for government bodies to prioritize the management of individuals' privacy concerns by enhancing regulatory frameworks and fostering collaboration with other stakeholders involved in these systems.

Overall, the findings highlight that there is a need to reassess the dynamics of the relationship between privacy concerns and health empowerment in the SHMS context. Emphasizing the perceived benefits of improved health outcomes both at the personal and communal levels would be an effective strategy to address the contention between privacy and health empowerment, because such benefits often take precedence in privacy values in SHMS environments. Factors other than privacy concerns (such as trust) could have a more pronounced impact on shaping individual and community perspectives regarding SHMSs.

The findings – derived from the quantitative approach of Manuscript 2 – also imply that the value of privacy relative to health is not consistent across the span of one's lifetime. It implies that individuals under the age of 65 generally prioritize personal data protection to a greater degree, influenced by changing societal attitudes, whereas older individuals may have distinct privacy expectations shaped by their experiences and trusting cultural backgrounds. Thus, SHMS practitioners are strongly encouraged to consider age as a significant factor when formulating privacy-related strategies to better serve SHMS users. Challenging the conventional notion that privacy loss holds ethical and equitable value, the study's findings also suggest that the significance of individual health empowerment may surpass ethical concerns associated with privacy loss, especially when the outcome involves improved healthcare. Thus, SHMS practitioners should be aware that the perceived advantages to individual health and well-being may be more concrete and tangible, prompting individuals to prioritize these aspects over abstract ethical principles.

4.3 Future Research

The findings in Chapter 2 uncover existing knowledge gaps and identify potential research avenues for future investigation. Based on the findings, a contextual framework of privacy in SHMSs was developed in Chapter 2 that provides valuable insights for future research seeking to understand multifaceted privacy concerns in SHMS settings. For example, future researchers are encouraged to use a mixed-methods design rather than using a single method in order to comprehensively investigate the privacy dynamic in the context of smart health monitoring. Future studies can concentrate on analyzing multi-stakeholder engagement, delving into the stakeholders' ecosystem to develop privacy protection management recommendations in smart health monitoring. Researchers are encouraged to focus on the influencing factors arising from lesser-explored aspects of emerging themes, such as barriers to surveillance and difficulties in involving new stakeholders with new business plans, as well as the profound impact of emotional responses such as stress, anxiety, and discomfort stemming from privacy concerns.

In Chapter 3, the unexpected findings, challenging preconceived notions about the negative impact of privacy concerns on both personal and community health empowerment, pave the way for a new avenue in future research. For instance, transparency as a significant factor of privacy concerns can be further explored from a dual perspective. Clear distinctions based on cultural and religious differences, ethical considerations, and equity/fairness remain crucial and could be better elucidated in both qualitative interviews and quantitative surveys. These aspects are prone to confusion during discussions on privacy issues. Moreover, although the factor of coordination among individual users and service providers was not included in this study due to reliability and validity issues, it should be included in future examinations as it is still an essential contextual factor related to privacy concerns and data governance. The study also suggests exploring the evolving dynamics of health empowerment. Researchers can look more deeply from a contrarian perspective into the interplay between individual and community empowerment, privacy considerations, and the evolving landscape of health technologies.

4.4 Limitations

Chapter 2 has some limitations. First, despite the broad search terms for surveillance, it is possible that some critical articles and concepts were missed since previous researchers may have used alternative terms to surveillance, monitor, track, or detect to describe the surveillance situation. Second, a number of reviewed articles used various terms for smart health monitoring systems, such as eHealth, remote health, connected health, or smart home which may have caused inconsistencies in the article inclusion. Third, the review aimed only at key stakeholders – individuals, healthcare providers, smart technology providers, and government authorities. Future literature reviews could include more novel stakeholders, for example, insurance service providers, which may be essential in smart health monitoring systems.

Chapter 3 also has several limitations. However, these limitations provide future research opportunities. The survey results may have been impacted by sample selection bias. Respondents who participated in this survey were individuals from Australia and New Zealand, which can be considered as limiting the generalizability of this study, taking into account the importance of geographical, regulatory, and cultural (localization) factors in individual and community health empowerment. Therefore, future research may consider approaching individuals in the context of other countries. Another limitation is that this study deals with the perspectives of potential SHMS users rather than actual experiences from real users. Future research could enhance the study by incorporating the insights and feedback of individuals

who have practical experience with SHMSs, allowing for a more comprehensive understanding of the dynamics between privacy concerns and health empowerment.

Chapter 5 Conclusion

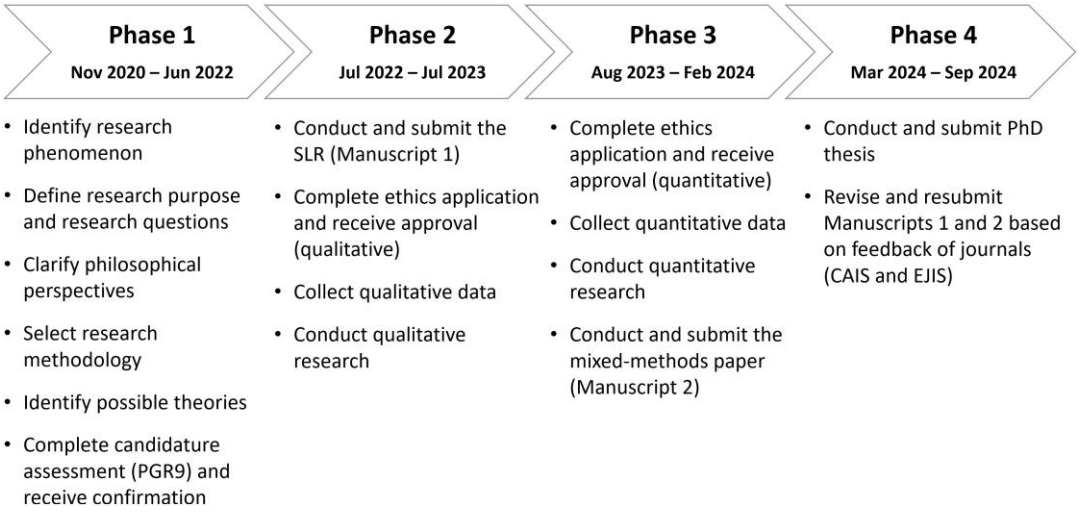
This chapter is divided into the following parts: a review of the research journey, a review of the research purpose, a review of the research questions, and concluding remarks.

5.1 Review of Research Journey

The journey of this research began in November 2020 and included four phases. Phase 1 identified that health and privacy have increasingly come into contention in the digital age, serving as opposing forces where the gain of one requires the loss of the other. Smart health monitoring systems (SHMSs) grant unparalleled health insights to empower individuals and communities, but their intrusive nature of data collection raises concerns for privacy. Identifying privacy phenomena within the context of SHMSs greatly motivated the study's initial review as well as to define the research purpose and questions. Based on this, the next step was to clarify the philosophical perspectives, select an appropriate research methodology, and to identify possible theories suitable for this research. A PhD candidature assessment (PGR9 presentation) was undertaken and confirmation received. Figure 5. 1 summarizes the key activities completed throughout the PhD journey.

Figure 5. 1

Research journey



In Phase 2, an SLR (Manuscript 1) was undertaken, which was submitted to the *Communications of the Association for Information Systems (CAIS)* and is currently under a major revision. The findings indicated the deficiency of privacy definitions in SHMS contexts, and insufficient analysis across various levels regarding the antecedents and outcomes of relevant privacy phenomena. The findings also highlighted a significant lack of a comprehensive theoretical application and mixed-methods approaches, as well as a lack of

exploration into surveillance-related contextual factors. These findings provided crucial insights for further research on privacy concerns in relation to health improvement in SHMSs (Manuscript 2). In the same phase, the ethics application was completed and approval was received for the qualitative data collection, which was the first stage of the mixed-methods study (Manuscript 2). This approval enabled the collection of qualitative data through conducting interviews with 15 participants. The interview transcripts were analyzed using thematic analysis, from which theoretical factors were derived and the research model of SHMS health empowerment was developed. In Phase 3, the focus shifted to quantitative research – the second stage of this mixed-methods study. To be able to test and validate the SHMS health empowerment model derived from the findings of the qualitative stage, another ethics application was submitted and approval was received for the quantitative data collection. Data was collected using an online questionnaire survey before the entire mixed-methods research was ultimately finalized. It was then submitted to the *European Journal of Information Systems (EJIS*) and is now under major revisions based on the reviewers' feedback (Manuscript 2).

In the final phase – Phase 4 – the PhD thesis was written and submitted following the Format Two requirements, which include two manuscripts. During this phase, both manuscripts were revised based on feedback from the journals the manuscripts had been submitted to.

5.2 Overall Research Purpose

SHMSs utilize advanced surveillance technologies to monitor changes in individuals' personal vital signs and daily health. These technologies include devices such as blood glucose wearables and electrocardiogram (ECG) monitors, which are crucial for the functionality of SHMSs. In light of surveillance technologies, SHMSs enable interactive contexts of health empowerment, fostering multi-level empowerment among individual community members and other stakeholders, including health service practitioners. However, consumers' privacy concerns about the surveillance technologies embedded in SHMSs are widely reported as a key reason they avoid using health monitoring applications and sharing their health data with other stakeholders, like health professionals.

Because of contemporary demands of convenience, personalization, and capitalism (Puntoni et al., 2021; Zuboff, 2015), the needs for health and privacy in the modern digital world have increasingly come into contention, serving as opposing forces where the gain of one requires the loss of the other (Agaku et al., 2014; Fox, Clohessy, et al., 2021; Mechanic & Meyer, 2000; Nelson et al., 2016; Niknejad et al., 2022; Seh et al., 2020; Srivastava et al., 2022). Within the literature, some degree of privacy loss is assumed to be an important determinant for

effective health diagnosis and treatment throughout the course of one's life (Agaku et al., 2014; Ali & Dang, 2022; Gao et al., 2015; Hassandoust, Akhlaghpour, et al., 2021; Seh et al., 2020). However, should we assume privacy loss is acceptable for everyone when balanced against their health, or are there aspects of the fundamental right to privacy that persist beyond the promise of better health? Further, does the consideration of individual privacy even matter when the health of an entire community is at stake?

For much of human history, both health and privacy have stood as fundamental rights, deeply ingrained in the fabric of human existence (Cohen & Ezer, 2013; Di Iorio et al., 2021). They are distinct rights by nature, valued highly for different reasons, but each is inextricably linked to Maslow's hierarchy of needs (Maslow, 2013; Shapiro et al., 2019; Zimmerman, 2000). While individual values are organized into a cohesive system that influences and elucidates individuals' attitudes and behaviors (Schwartz et al., 2012), certain values are compatible with each other while others may be contradictory (Schwartz et al., 2012). So, in the context of empowering health versus concerns for privacy, which values do we value? How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes? Few perspectives in the current literature have challenged the traditional assumptions of privacy and health value or explored important factors that impact privacy concerns in the given context. Thus, it is urgent to understand privacy phenomena in the context of SHMSs and address the contention between health and privacy values in relation to SHMS, highlighting inconsistencies and disparities between the study's findings and prevailing thoughts on the value of privacy in HIT use like SHMSs.

5.3 Review of Research Question 1

What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context?

Privacy is often characterized as multidimensional, elastic, and dynamic, adapting to the nuances of individual life experiences. Crucially, privacy is context-dependent and people's beliefs about privacy may vary. Its importance may be assessed differently for various reasons and contexts, particularly in HIT-based monitoring situations like SHMSs. Contextualization enriches our understanding of the subjects under investigation and unveils alternative interpretations of the phenomena from more insightful perspectives (Zahra et al., 2014). Contextualization is a foundational step that sets the stage for deeper exploration.

Given the importance of privacy contextualization and the deficiencies of the existing literature, which fails to meet the requirement of compiling a full picture of contextualized

privacy, the first purpose of this study was to conduct a systematic literature review. This review sought to achieve a comprehensive contextualization of privacy in SHMSs, laying the groundwork for a more in-depth exploration of privacy issues. The first research question in this study was: *What are the key insights provided by the existing IS privacy literature that can inform our perspective on privacy in the SHMS context* (RQ1)? To address this question, Chapter 2 examined privacy definitions from various perspectives and reviewed antecedents and outcomes of privacy, relevant theories, methodological transparency, research agenda, and other pertinent scopes. Key findings and contributions are presented in Table 4. 1 of Chapter 4. This presentation answers RQ1, i.e., providing key insights and perspectives on privacy in the SHMS context.

5.4 Review of Research Question 2

RQ2: How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?

Despite the conventional notions in mainstream research, few perspectives have challenged the traditional assumptions of privacy and health value (e.g., Princi & Krämer, 2020; Zarcadoolas et al., 2013). The literature suggests that privacy matters to HIT users, even when weighed against one's health. However, before this knowledge can serve as an ironclad underlying assumption of how individuals perceive and experience the tension between privacy and health in the SHMS context, it is important to delve more deeply. A more nuanced examination is required – one that takes a contrarian view of existing assumptions and differentiates among and between individuals and their community empowerment interests.

To achieve the purpose above, Chapter 3 explored privacy concerns in relation to health empowerment by conducting a value-reflexive examination of health and privacy in the health empowerment context via the use of SHMSs. Leveraging health empowerment theory and adopting a mixed-methods design, the study pursued alternative perspectives that may challenge prevailing attitudes or trends but made it possible to discover the intricacies of privacy phenomena within SHMSs. An exploration of the contention between health and privacy values as it persists in SHMSs was approached from the perspective of prioritizing health empowerment over the general values of health and privacy. The findings presented in Chapter 3 relate to the contention between health and privacy values in SHMSs and the inconsistencies and disparities between this study's findings and the prevailing thoughts on the value of privacy in health information technology use like SHMSs.

These findings from Chapter 3 made it possible to address the second research question of this thesis: *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes* (RQ2)? Based on the qualitative findings and the existing literature, antecedent factors impacting individuals' privacy concerns with SHMSs were identified in terms of three value-based themes. These factors include *legislative protection*, *transparency*, and *cultural and religious differences* (regulatory and sociocultural theme); *ethical considerations* and *equity/fairness* (ethical theme); and *traceability* and *security* (technological theme). A potential association was identified between individuals' privacy concerns when using SHMSs and individual health empowerment. Other factors including trust and personal social factors were also identified to have a potential association with individual and community health empowerment in the use of SHMSs.

Then, based on these findings, the SHMS Health Empowerment Model was developed, along with hypotheses anchored in Health Empowerment Theory. The developed SHMS health empowerment model was then tested and validated. In brief, the quantitative findings indicated that *legislative protection*, *transparency*, *cultural and religious differences*, and *security* are the important factors influencing privacy concerns in SHMSs. In terms of how users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes, the findings revealed that the perceived trade-off between privacy concerns and health empowerment might not be as pronounced as commonly believed. The value of privacy relative to health and the attribution of community health empowerment on one's own health empowerment are not consistent across the span of one's lifetime. The role of ethics and equity considerations become inconsistent at best when the value of privacy is weighed against health.

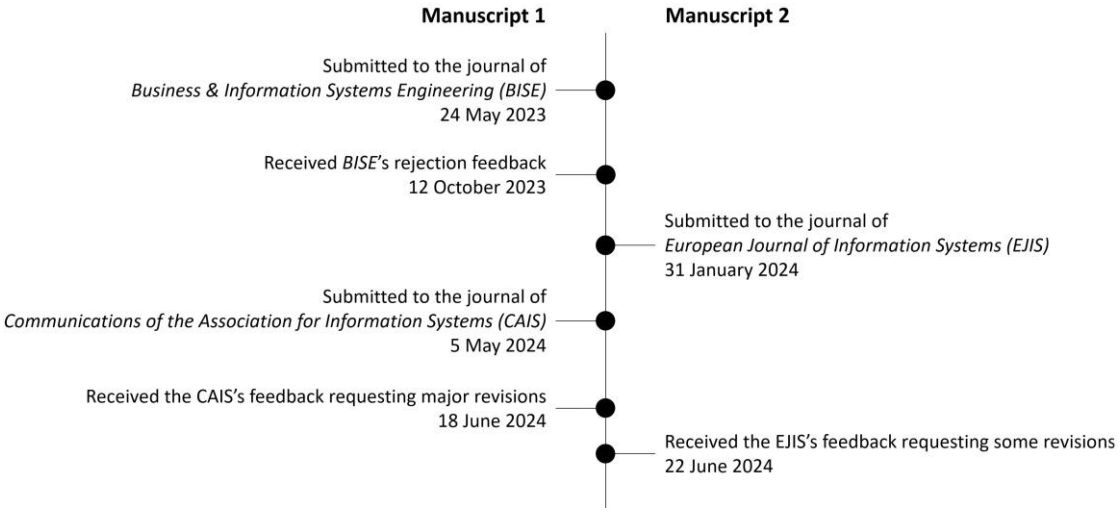
5.5 Submission Status

The progress timeline of the submissions is presented in Figure 5. 2. Manuscript 1 is based on the SLR paper. It was submitted to *Business & Information Systems Engineering (BISE)*, a peer-reviewed journal with A-rank based on Australian Business Deans Council (ABDC) ranking, on 24 May 2023. This submission had a rejection outcome on 12 October 2023, showing some room for improvement in the motivation, methodological clarity, and contributions of the study. Based on feedback from both BISE and supervisors, the narrative flow was changed and more reviewed articles were included in the SLR study. Revised Manuscript 1 was submitted to *Communications of the Association for Information Systems (CAIS)*, another peer-reviewed journal with A-rank at ABDC list, on 5 May 2024. A decision was received from CAIS on 18 June 2024, requiring major revisions and a resubmission in six months. Under the guidance of

supervisors, the study is now being revised based on the reviewers' comments. Due to reasonable and manageable comments from the review team, Manuscript 1 will likely be resubmitted in August 2024.

Figure 5. 2

Submission timeline



Manuscript 2 is based on the mixed-methods paper. It was submitted to the *EJIS*, a peer-reviewed journal with A*-rank at ABDC list on 31 January 2024. This submission responded to a call for papers for a special issue on *Embracing Contrarian Thinking: Value-Reflexive Research for a Digital World.*[3] On 22 June 2024, it received positive feedback from EJIS; however major revisions were requested with a deadline of 20 September 2024, before the manuscript can be considered for publication.

5.6 Concluding Remarks

This thesis has provided a comprehensive contextualization of privacy in SHMSs. It has explored the complex dynamics, or the ongoing contention between health and privacy values and revealed inconsistencies and disparities between the findings and prevailing thoughts on the value of privacy in health information technology use, such as the use of SHMSs. The findings from this thesis challenge the conventional assumption that privacy concerns negatively impact both individual and community health empowerment. It is evident that the dynamic relationship between privacy and health within an HIT-based smart monitoring environment often diverges from traditional notions, and can be further assessed through a deeper exploration.

[3] Detailed requirement for this call for papers can be found at https://www.callforpapers.co.uk/embracing-contrarian-thinking

Moving forward, it is crucial to recognize the importance of adopting a nuanced perspective that accounts for individual variations and community empowerment aspirations within SHMS contexts. By doing so, we can better navigate the contention between privacy and health, ultimately paving the way for more effective and inclusive approaches to HIT usage. In concluding this study, it is clear that further research and continued dialogue are essential to fully comprehend and address the complexities of privacy and health within SHMSs. Only through ongoing exploration and collaboration can we offer solutions that consider both privacy concerns and health empowerment in an increasingly digital world.

References

Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424-438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Accenture.com. (2020). *How can leaders make recent digital health gains last?* Retrieved from https://www.accenture.com/us-en/insights/health/leaders-make-recent-digital-health-gains-last

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *In Proceedings of the 5th ACM Conference on Electronic Commerce*.

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & 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), 374-378. https://doi.org/10.1136/amiajnl-2013-002079

Ågerfalk, P. J. (2013). Embracing diversity through mixed methods research. *European Journal of Information Systems*, *22*(3), 251-256. https://doi.org/10.1057/ejis.2013.6

Akmandor, A. O., & Jha, N. K. (2018). Smart health care: An edge-side computing perspective. *IEEE Consumer Electronics Magazine*, *7*(1), 29-37. https://doi.org/10.1109/MCE.2017.2746096

Al-rawashdeh, M., Keikhosrokiani, P., Belaton, B., Alawida, M., & Zwiri, A. (2022). IoT adoption and application for smart healthcare: A systematic review. *Sensors*, *22*(14), 1-20. https://doi.org/10.3390/s22145377

Al-Shaqi, R., Mourshed, M., & Rezgui, Y. (2016). Progress in ambient assisted systems for independent living by the elderly. *SpringerPlus*, *5*(1). https://doi.org/10.1186/s40064-016-2272-8

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, *36*, 93-101. https://doi.org/10.1007/s10916-010-9449-4

Alabdulatif, A., Khalil, I., Forkan, A. R. M., & Atiquzzaman, M. (2019). Real-time secure health surveillance for smarter health communities. *IEEE Communications Magazine*, *57*(1), 122-129. https://doi.org/10.1109/MCOM.2017.1700547

Alashoor, T., Keil, M., Liu, L., & Smith, J. (2015). *How values shape concerns about privacy for self and others* 2015 International Conference on Information Systems: Exploring the Information Frontier, Fort Worth, Texas.

Ali, Z. S., & Dang, H. (2022). Factors impacting the use of the NZ COVID Tracer application in New Zealand. *Smart Health*, *24*, 1-14. https://doi.org/10.1016/j.smhl.2022.100278

Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. A. (2023). An empirical study on secure usage of mobile health apps: The attack simulation approach. *Information and Software Technology*, *163*. https://doi.org/10.1016/j.infsof.2023.107285

Almujally, N. A., Aljrees, T., Saidani, O., Umer, M., Faheem, Z. B., Abuzinadah, N., Alnowaiser, K., & Ashraf, I. (2023). Monitoring acute heart failure patients using

internet-of-things-based smart monitoring system. *Sensors*, *23*(10). https://doi.org/10.3390/s23104580

Alraja, M. (2022). Frontline healthcare providers' behavioural intention to Internet of Things (IoT)-enabled healthcare applications: A gender-based, cross-generational study. *Technological Forecasting and Social Change*, *174*, 1-15. https://doi.org/10.1016/j.techfore.2021.121256

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66-84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

Alzahrani, T., Hunt, M., & Whiddett, D. (2021). Barriers and facilitators to using smart home technologies to support older adults: Perspectives of three stakeholder groups. *International Journal of Healthcare Information Systems and Informatics*, *16*(4), 1-14. https://doi.org/10.4018/IJHISI.20211001.oa22

Ancona, D. G., Goodman, P. S., Lawrence, B. S., & Tushman, M. L. (2001). Time: A new research lens. *Academy of Management Review*, *26*(4), 645-663. https://doi.org/10.2307/3560246

Anderson, S., Rayburn, S. W., & Sierra, J. J. (2019). Future thinking: the role of marketing in healthcare. *European Journal of Marketing*, *53*(8), 1521-1545. https://doi.org/10.1108/EJM-10-2017-0779

Andrejevic, M., Davies, H., DeSouza, R., Hjorth, L., & Richardson, I. (2021). Situating 'careful surveillance'. *International Journal of Cultural Studies*, *24*(4), 567-583. https://doi.org/10.1177/1367877921997450

Angel, M. P., & Calo, R. (2023). Distinguishing privacy law: A critique of privacy as social taxonomy. *Columbia Law Review*, 1-44. https://doi.org/10.2139/ssrn.4347191

Arar, M., Jung, C., Awad, J., & Chohan, A. H. (2021). Analysis of smart home technology acceptance and preference for elderly in Dubai, UAE. *Designs*, *5*(4), 70.

Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygård, J. F., & Vitenberg, R. (2022). A survey on blockchain for healthcare: Challenges, benefits, and future directions. *IEEE Communications Surveys & Tutorials*, 386-424. https://doi.org/10.1109/COMST.2022.3224644

Aronson, E. (2004). *The social animal* (9th ed.). Worth Publishers.

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, *45*, 93-98. https://doi.org/https://doi.org/10.1016/j.chb.2014.11.075

Avgerou, C. (2019). Contextual explanation: Alternative approaches and persistent challenges. *MIS Quarterly*, *43*(3), 977-1006. https://doi.org/10.25300/MISQ/2019/13990

Awad, N. F., & 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*, *30*(1), 13-28.

Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *Academy of Management Review*, *14*(4), 496-515.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, *63*, 363-374. https://doi.org/10.1016/j.enpol.2013.08.043

Banasiewicz, A. (2021). Learning with Data in the Twenty-First Century. In A. Banasiewicz (Ed.), *Organizational Learning in the Age of Data* (pp. 103-159). Springer International Publishing.

Bansal, G., Zahedi, F. M., & 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), 138-150. https://doi.org/10.1016/j.dss.2010.01.010

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*, 624-644.

Bantan, M., & Shawosh, M. (2024). Chief Privacy Officer: A Systematic Literature Review and Future Research Directions. *Communications of the Association for Information Systems*, *54*(1), 13.

Banville, M. C. (2020). Resisting surveillance: Responding to wearable device privacy policies. *In Proceedings of the 38th ACM International Conference on Design of Communication*. https://doi.org/10.1145/3380851.3416764

Bargh, M. S., Choenni, S., & Meijer, R. (2017). On addressing privacy in disseminating judicial data: towards a methodology. *Transforming Government: People, Process and Policy*, *11*(1), 9-41. https://doi.org/10.1108/TG-12-2015-0051

Beaudin, J. S., Intille, S. S., & Morris, M. E. (2006). To track or not to track: user reactions to concepts in longitudinal health monitoring. *Journal of Medical Internet Research*, *8*(4), 1-29. https://doi.org/10.2196/jmir.8.4.e29

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041. https://doi.org/10.2307/41409971

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management*, *57*(2), 1-16. https://doi.org/10.1016/j.im.2019.05.003

Bhatt, V., & Chakraborty, S. (2020, 7-9 Oct. 2020). Importance of trust in IoT based wearable device adoption by patient: An empirical investigation. *In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*. https://doi.org/10.1109/I-SMAC49090.2020.9243533

Blakely, T. A., & Woodward, A. J. (2000). Ecological effects in multi-level studies. *Journal of Epidemiology & Community Health*, *54*(5), 367-374.

Bouncken, R. B., Qiu, Y., Sinkovics, N., & Kürsten, W. (2021). Qualitative research: extending the range with flexible pattern matching. *Review of Managerial Science*, *15*(2), 251-273. https://doi.org/10.1007/s11846-021-00451-2

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Burgoon, J. K. (1982). Privacy and Communication. *Annals of the International Communication Association*, *6*(1), 206-249. https://doi.org/10.1080/23808985.1982.11678499

Burrows, A., Coyle, D., & Gooberman-Hill, R. (2018). Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place*, *50*, 112-118. https://doi.org/10.1016/j.healthplace.2018.01.006

Burton-Jones, A., McLean, E. R., & Monod, E. (2015). Theoretical perspectives in IS research: from variance and process to conceptual latitude and conceptual fit. *European Journal of Information Systems*, *24*(6), 664-679. https://doi.org/10.1057/ejis.2014.31

Butpheng, C., Yeh, K.-H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry*, *12*(7), 1191.

Califf, C. B., Sarker, S., & Sarker, S. (2020). The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. *MIS Quarterly*, *44*(2).

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586-606. https://doi.org/10.1207/s15506878jobem4604_6

Cappelli, P. (1991). The missing role of context in OB: The need for a meso-level approach. *Organizational Behavior*, *13*, 55-110.

Capterra.com. (2021). *New technologies for telehealth in Canada: 61% of Canadians want to implement AI*. Retrieved from https://www.capterra.ca/blog/2039/telehealth-in-canada-technology-ai

Carver, L. F., & Mackinnon, D. (2020). Health applications of gerontechnology, privacy, and surveillance: A scoping review. *Surveillance & Society*, *18*(2), 216-230. https://doi.org/10.24908/ss.v18i2.13240

Casaló Luis, V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5), 583-603. https://doi.org/10.1108/14684520710832315

Chadborn, N. H., Blair, K., Creswick, H., Hughes, N., Dowthwaite, L., Adenekan, O., & Pérez Vallejos, E. (2019). Citizens' juries: When older adults deliberate on the benefits and risks of smart health and smart homes. *Healthcare*, *7*(54), 1-17. https://doi.org/10.3390/healthcare7020054

Chalhoub, G., Kraemer, M. J., & Flechais, I. (2024). Useful shortcuts: Using design heuristics for consent and permission in smart home devices. *International Journal of Human-Computer Studies*, *182*, 103177. https://doi.org/https://doi.org/10.1016/j.ijhcs.2023.103177

Chalhoub, G., Kraemer, M. J., Nthala, N., & Flechais, I. (2021). "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. *In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445691

Chan, T. K. H., Cheung, C. M. K., & Lee, Z. W. Y. (2021). Cyberbullying on social networking sites: A literature review and future research directions. *Information & Management*, *58*(2), 103411. https://doi.org/10.1016/j.im.2020.103411

Chang, Y., & Fang, S. (2013). Antecedents and distinctions between online trust and distrust: Predicting high-and low-risk internet behaviors. *Journal of Electronic Commerce Research*, *14*(2), 149-166.

Chen, Y., Zhang, L., & Wei, M. (2021). How does smart healthcare service affect resident health in the digital age? Empirical evidence from 105 cities of China. *Frontiers in Public Health*, *9*, 1-9. https://doi.org/10.3389/fpubh.2021.833687

Chin, W. W. (2009). How to write up and report PLS analyses. In *Handbook of partial least squares: Concepts, methods and applications* (pp. 655-690). Springer Berlin Heidelberg.

Choi, J. R., & Kim, S. (2024). Predicting individuals' privacy protection and self-tracking behaviors in the context of smart health. *Telematics and Informatics*, *86*, 102069. https://doi.org/10.1016/j.tele.2023.102069

Choi, Y. K., Thompson, H. J., & Demiris, G. (2020). Use of an internet-of-things smart home system for healthy aging in older adults in residential settings: Pilot feasibility study. *JMIR Aging*, *3*(2). https://doi.org/10.2196/21964

Cilliers, L., & Flowerday, S. (2014). User acceptance of telemedicine by health care workers A case of the Eastern Cape Province, South Africa. *The Electronic Journal of Information Systems in Developing Countries 65*(1), 1-10. https://doi.org/10.1002/j.1681-4835.2014.tb00467.x

CNBC.com. (2022). *The biggest security risks of using fitness trackers and apps to monitor your health*. Retrieved from https://www.cnbc.com/2022/11/26/the-biggest-risks-of-using-fitness-trackers-to-monitor-health.html

Cohen, J., & Ezer, T. (2013). Human rights in patient care: a theoretical and practice framework. *Health and Human Rights*, *15*(2), 7-19.

Cohen, L., Manion, L., & Morrison, K. (2013). *Research methods in education* (7 ed.). Routledge.

Creswell, J. W. (2009). *Research design : qualitative, quantitative, and mixed methods approaches* (Third edition. ed.). Sage Publications.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (Third ed.). Sage.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.

Cristiano, A., Musteata, S., De Silvestri, S., Bellandi, V., Ceravolo, P., Cesari, M., Azzolino, D., Sanna, A., & Trojaniello, D. (2022a). Older adults' and clinicians' perspectives on a smart health platform for the aging population: Design and evaluation study. *JMIR Aging*, *5*(1), e29623. https://doi.org/10.2196/29623

Cristiano, A., Musteata, S., De Silvestri, S., Bellandi, V., Ceravolo, P., Cesari, M., Azzolino, D., Sanna, A., & Trojaniello, D. (2022b). Older adults' and clinicians' perspectives on a smart health platform for the aging population: Design and evaluation study. *JMIR Aging*, *5*(1). https://doi.org/10.2196/29623

Crotty, M. J. (1998). The foundations of social research: Meaning and perspective in the research process. *The Foundations of Social Research*, 1-256.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323-342. https://doi.org/10.1111/1540-4560.00067

Dadhich, M., Hiran, K. K., Rao, S. S., & Sharma, R. (2022). Factors Influencing Patient Adoption of the IoT for E-Health Management Systems (e-HMS) Using the UTAUT Model: A High Order SEM-ANN Approach. *International Journal of Ambient Computing and Intelligence*, *13*(1), 1-18. https://doi.org/10.4018/IJACI.300798

DAMA International. (2009). *The DAMA guide to the data management body of knowledge*. Technics Publications, LLC.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

Davison, R. M., & Martinsons, M. G. (2016). Context is king! Considering particularism in research design and reporting. *Journal of Information Technology 31*, 241-249. https://doi.org/10.1057/jit.2015.19

de Guinea, A. O., & Webster, J. (2017). Combining variance and process in information systems research: Hybrid approaches. *Information and organization*, *27*(3), 144-162.

De Hoogh, A. H. B., & Den Hartog, D. N. (2008). Ethical and despotic leadership, relationships with leader's social responsibility, top management team effectiveness and subordinates' optimism: A multi-method study. *The Leadership Quarterly*, *19*(3), 297-311. https://doi.org/10.1016/j.leaqua.2008.03.002

De Moya, J. F., & Pallud, J. (2020). From panopticon to heautopticon: A new form of surveillance introduced by quantified ‐ self practices. *Information Systems Journal*, *30*(6), 940-976.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*, 261-272. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.05.010

del Río-Lanza, A.-B., Suárez-Vázquez, A., Suárez-Álvarez, L., & Iglesias-Argüelles, V. (2020). Mobile health (mhealth): facilitators and barriers of the intention of use in patients with chronic illnesses. *Journal of Communication in Healthcare*, *13*(2), 138-146. https://doi.org/10.1080/17538068.2020.1777513

Deloitte. (2019). *Smart health communities and the future of health*. Retrieved from https://www2.deloitte.com/us/en/insights/industry/health-care/smart-health-communities.html

Demiris, G. (2006). The diffusion of virtual communities in health care: concepts and challenges. *Patient Education and Counseling*, *62*(2), 178-188. https://doi.org/10.1016/j.pec.2005.10.003

Deng, Z., Hong, Z., Ren, C., Zhang, W., & Xiang, F. (2018). What predicts patients' adoption intention toward mHealth services in China: empirical study. *JMIR Mhealth Uhealth*, *6*(8), 1-14. https://doi.org/10.2196/mhealth.9316

Dewey, J. (1958). *Experience and Nature*. Dover Publications.

Dhanireddy, S., Walker, J., Reisch, L., Oster, N., Delbanco, T., & Elmore, J. G. (2014). The urban underserved: attitudes towards gaining full access to electronic medical records. *Health Expectations*, *17*(5), 724-732. https://doi.org/10.1111/j.1369-7625.2012.00799.x

Di Iorio, C. T., Carinci, F., Oderkirk, J., Smith, D., Siano, M., de Marco, D. A., de Lusignan, S., Hamalainen, P., & Benedetti, M. M. (2021). Assessing data protection and governance in health information systems: a novel methodology of privacy and ethics impact and performance assessment (PEIPA). *Journal of Medical Ethics*, *47*(12), 1-8. https://doi.org/10.1136/medethics-2019-105948

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389-402. https://doi.org/10.1057/palgrave.ejis.3000590

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413-422. https://doi.org/10.1080/01449290410001715723

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316.

Donovan, N. J., & Blazer, D. (2020). Social isolation and loneliness in older adults: review and commentary of a national academies report. *The American Journal of Geriatric Psychiatry*, *28*(12), 1233-1244.

Drechsler, A., & Breth, S. (2019). How to go global: A transformative process model for the transition towards globally distributed software development projects. *International Journal of Project Management*, *37*(8), 941-955. https://doi.org/10.1016/j.ijproman.2019.08.003

Duckert, M., & Barkhuus, L. (2022). Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness. *Proceedings of the ACM on Human-Computer Interaction*, *6*(GROUP), 1-22. https://doi.org/10.1145/3492830

Ebardo, R. (2018). The Use of Activity Trackers for Health Empowerment and Commitment: The Philippine Cycling Perspective. *arXiv preprint arXiv:1901.05050*.

Edwards, V. M., & Steins, N. A. (1999). A framework for analysing contextual factors in common pool resource research. *Journal of environmental policy and planning*, *1*(3), 205-221.

El-Masri, M., & Tarhini, A. (2017). Factors affecting the adoption of e-learning systems in Qatar and USA: Extending the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2). *Educational Technology Research and Development*, *65*(3), 743-763. https://doi.org/10.1007/s11423-017-9526-1

Esmaeilzadeh, P. (2019). The process of building patient trust in health information exchange (HIE): The impacts of perceived benefits, perceived transparency of privacy policy, and familiarity. *Communications of the Association for Information Systems*, *45*, 364-396. https://doi.org/10.17705/1CAIS.04521

Esmaeilzadeh, P. (2022). Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. *BMC Medical Informatics and Decision Making*, *22*(1), 1-18. https://doi.org/10.1186/s12911-022-01815-8

Esmaeilzadeh, P. (2023). Older Adults' Perceptions About Using Intelligent Toilet Seats Beyond Traditional Care: Web-Based Interview Survey. *JMIR mHealth and uHealth*, *11*(1). https://doi.org/10.2196/46430

Essén, A. (2008). The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices. *Social Science & Medicine*, *67*(1), 128-136. https://doi.org/10.1016/j.socscimed.2008.03.005

Etemad-Sajadi, R., & Dos Santos, G. G. (2019). Senior citizens' acceptance of connected health technologies in their homes. *International Journal of Health Care Quality Assurance*, *32*(8), 1162-1174.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175-191. https://doi.org/10.3758/BF03193146

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541-562. https://doi.org/10.1016/j.jbi.2012.12.003

Finch, K., & Tene, O. (2014). Welcome to the metropticon: Protecting privacy in a hyperconnected town. *Fordham Urban Law Journal*, *41*(5), 1581-1616.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric*, *10*(2).

Forsyth, A. (2020). What is a healthy place? Models for cities and neighbourhoods. *Journal of Urban Design*, *25*(2), 186-202. https://doi.org/10.1080/13574809.2019.1662718

Fortune.com. (2023). *The best technology to prevent falls, monitor safety, and help older adults age in place longer*. Retrieved from https://fortune.com/well/2023/02/03/technology-can-help-older-adults-age-in-place-longer/

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 106806. https://doi.org/10.1016/j.chb.2021.106806

Fox, G., & James, T. L. (2021). Toward an understanding of the antecedents to health information privacy concern: A mixed methods study. *Information Systems Frontiers*, *23*(6), 1537-1562. https://doi.org/10.1007/s10796-020-10053-0

Fox, G., van der Werff, L., Rosati, P., Takako Endo, P., & Lynn, T. (2021). Examining the determinants of acceptance and use of mobile contact tracing applications in Brazil: An extended privacy calculus perspective. *Journal of the Association for Information Science and Technology*. https://doi.org/10.1002/asi.24602

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & De Colle, S. (2010). *Stakeholder theory: The state of the art*. Cambridge University Press.

Fritz, R. L., Corbett, C. L., Vandermause, R., & Cook, D. (2016). The influence of culture on older adults' adoption of smart home monitoring. *Gerontechnology*, *14*(3), 146-156. https://doi.org/10.4017/GT.2016.14.3.010.00

Galanxhi-Janaqi, H., & Nah, F. H. F. (2004). U‐commerce: emerging trends and research issues. *Industrial Management & Data Systems*, *104*(9), 744-755. https://doi.org/10.1108/02635570410567739

Ganascia, J.-G. (2011). The new ethical trilemma: Security, privacy and transparency. *Comptes Rendus Physique*, *12*(7), 684-692.

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704-1723. https://doi.org/10.1108/IMDS-03-2015-0087

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health*, *2*(8), e425-e434. https://doi.org/10.1016/S2589-7500(20)30137-0

George, C., Whitehouse, D., & Duquenoy, P. (2012). *eHealth: legal, ethical and governance challenges*. Springer Science & Business Media.

Ghorayeb, A., Comber, R., & Gooberman-Hill, R. (2021). Older adults' perspectives of smart home technology: Are we developing the technology that older people want? *International Journal of Human Computer Studies*, *147*, 1-13. https://doi.org/10.1016/j.ijhcs.2020.102571

GlobeNewswire. (2023). *Smart Medical Devices Market Expecting to Hit USD 474 Billion by 2032, with a CAGR of 12.3 %*. Retrieved from https://www.globenewswire.com/news-release/2023/12/13/2795357/0/en/Smart-Medical-Devices-Market-Expecting-to-Hit-USD-474-Billion-by-2032-with-a-CAGR-of-12-3-Market-us.html

Graham, C. (2021). Fear of the unknown with healthcare IoT devices: An exploratory study. *Information Security Journal: A Global Perspective*, *30*(2), 100-110. https://doi.org/10.1080/19393555.2020.1810369

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, *26*(2), 91-108.

Greco, L., Percannella, G., Ritrovato, P., Tortorella, F., & Vento, M. (2020). Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern Recognition Letters*, *135*, 346-353. https://doi.org/10.1016/j.patrec.2020.05.016

Grill, E., Müller, M., & Mansmann, U. (2016). *Supplement issue: Health—Exploring complexity: An Interdisciplinary systems approach* European Journal of Epidemiology, Munich, Germany.

Groves, P., Kayyali, B., & Van Kuiken, S. (2013). The 'big data' revolution in healthcare: Accelerating value and innovation. *McKinsey Quarterly*, *2*, 10-14.

Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing? *International Journal of Human-Computer Studies*, *43*(5), 907-928. https://doi.org/10.1006/ijhc.1995.1081

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research*, *2*(163-194), 105.

Gupta, S., Kamboj, S., & Bag, S. (2021). Role of risks in the development of responsible artificial intelligence in the digital healthcare domain. *Information Systems Frontiers*, *25*, 2257-2274. https://doi.org/10.1007/s10796-021-10174-0

Hair, J., Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2023). *Advanced issues in partial least squares structural equation modeling*. Sage.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

Hajian, A., Prybutok, V. R., & Chang, H.-C. (2023). An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective. *Computers in Human Behavior*, *138*, 1-11. https://doi.org/10.1016/j.chb.2022.107471

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217-227. https://doi.org/10.1016/j.chb.2016.11.033

Harding, J. F., Sibley, C. G., & Robertson, A. (2011). New Zealand = Māori, New Zealand = bicultural: Ethnic group differences in a national sample of Māori and Europeans. *Social Indicators Research*, *100*, 137-148. https://doi.org/10.1007/s11205-010-9608-5

Harman, H. H. (1976). *Modern factor analysis*. University of Chicago press.

Hassan, A. H., Sulaiman, R. B., Abdulgabber, M. A., & Kahtan, H. (2023). Balancing technological advances with user needs: User-centered principles for AI-driven smart city healthcare monitoring. *International Journal of Advanced Computer Science and Applications*, *14*(3), 365-376. https://doi.org/10.14569/IJACSA.2023.0140341

Hassan, N. R., & Lowry, P. B. (2015). Seeking middle-range theories in information systems research. *In International Conference on Information Systems (ICIS 2015), Fort Worth, TX, December*.

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), 463-471. https://doi.org/10.1093/jamia/ocaa240

Hassandoust, F., Johnston, A., & Singh, T. (2021). Smart pay-as-you-live services in healthcare: A balance theory perspective. *In ICIS 2021 Proceedings*.

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311-335. https://doi.org/10.1016/j.comcom.2020.02.018

Helm, P., & Seubert, S. (2020). Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies. *Surveillance & Society*, *18*(2), 185-198. http://ezproxy.aut.ac.nz/login?url=https://www.proquest.com/scholarly-journals/normative-paradoxes-privacy-literacy-choice/docview/2427317048/se-2?accountid=8440

https://resolver.ebscohost.com/openurl?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ%3Apubliccontent&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=article&rft.jtitle=Surveillance+%26+Society&rft.atitle=Normative+Paradoxes+of+Privacy%3A+Literacy+and+Choice+in+Platform+Societies&rft.au=Helm%2C+Paula%3BSeubert%2C+Sandra&rft.aulast=Helm&rft.aufirst=Paula&rft.date=2020-01-01&rft.volume=18&rft.issue=2&rft.spage=185&rft.isbn=&rft.btitle=&rft.title=Surveillance+%26+Society&rft.issn=&rft_id=info:doi/

Henderson, S. C., & Snyder, C. A. (1999). Personal information privacy: implications for MIS managers. *Information & Management*, *36*(4), 213-220. https://doi.org/10.1016/S0378-7206(99)00019-1

Hsu, C., Lee, M., & Su, C. (2013). The role of privacy protection in healthcare information systems adoption. *Journal of Medical Systems*, *37*, 1-12. https://doi.org/10.1007/s10916-013-9966-z

Hunter, I., Elers, P., Lockhart, C., Guesgen, H., Singh, A., & Whiddett, D. (2020). Issues associated with the management and governance of sensor data and information to assist aging in place: Focus group study with health care professionals. *JMIR Mhealth Uhealth*, *8*(12), 1-10. https://doi.org/10.2196/24157

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, *54*, 102122. https://doi.org/10.1016/j.ijinfomgt.2020.102122

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, *24*, 393-414. https://doi.org/10.1007/s10796-020-10044-1

Ismail, L., Materwala, H., Karduck, A. P., & Adem, A. (2020). Requirements of health data management systems for biomedical care and Rresearch: Scoping review. *Journal of Medical Internet Research*, *22*(7), N.PAG-N.PAG. https://doi.org/10.2196/17508

Israel, B. A., Checkoway, B., Schulz, A., & Zimmerman, M. (1994). Health education and community empowerment: conceptualizing and measuring perceptions of individual, organizational, and community control. *Health Education Quarterly*, *21*(2), 149-170. https://doi.org/10.1177/109019819402100203

Jakobi, T., Patil, S., Randall, D., Stevens, G., & Wulf, V. (2019). It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM*

Transactions on Computer-Human Interaction, *26*(1), 2:1-2:44. https://doi.org/10.1145/3281444

Janamian, T., Crossland, L., & Jackson, C. L. (2016). Embracing value co‐creation in primary care services research: A framework for success. *Medical Journal of Australia*, *204*(S7), S5-S11.

Jiang, F., Liu, Y., Hu, J., & Chen, X. (2022). Understanding Health Empowerment from the perspective of information processing: questionnaire study. *Journal of Medical Internet Research*, *24*(1), 1-18. https://doi.org/10.2196/27178

Jones, T. M., Harrison, J. S., & Felps, W. (2018). How applying instrumental stakeholder theory can provide sustainable competitive advantage. *Academy of Management Review*, *43*(3), 371-391. https://doi.org/10.5465/amr.2016.0111

Kang, M. J., & Hwang, Y. C. (2022). Exploring the factors affecting the continued usage intention of IoT-based healthcare wearable devices using the TAM model. *Sustainability*, *14*(19), 12492.

Kaplan, B. (2016). How should health data be used?: Privacy, secondary use, and big data sales. *Cambridge Quarterly of Healthcare Ethics*, *25*(2), 312-329. https://doi.org/10.1017/S0963180115000614

Kaplan, H. C., Brady, P. W., Dritz, M. C., Hooper, D. K., Linam, W. M., Froehle, C. M., & Margolis, P. (2010). The influence of context on quality improvement success in health care: a systematic review of the literature. *The Milbank Quarterly*, *88*(4), 500-559.

Kapondera, S. K., Bernardi, R., & Panteli, N. (2019). A framework for understanding the empowerment effects of telecentres on rural communities in developing countries. *In International conference on social implications of computers in developing countries*.

Karadag, E., Parlar Kilic, S., Ugur, O., & Akyol, M. A. (2019). Attitudes of nurses in Turkey toward care of dying individual and the associated religious and cultural factors. *Journal of Religion and Health*, *58*, 303-316. https://doi.org/10.1007/s10943-018-0657-4

Karahoca, A., Karahoca, D., & Aksöz, M. (2018). Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes*, *47*(4), 742-770. https://doi.org/10.1108/K-02-2017-0045

Kennedy, M.-R., Huxtable, R., Birchley, G., Ives, J., & Craddock, I. (2021). "A question of trust" and "a leap of faith"—Study participants' perspectives on consent, privacy, and trust in smart home research: Qualitative study. *JMIR Mhealth Uhealth*, *9*(11), e25227. https://doi.org/10.2196/25227

Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. *Informatics in Medicine Unlocked*, *30*, 100903. https://doi.org/https://doi.org/10.1016/j.imu.2022.100903

Khanna, S., & Srivastava, S. (2020). Patient-Centric Ethical Frameworks for Privacy, Transparency, and Bias Awareness in Deep Learning-Based Medical Systems. *Applied Research in Artificial Intelligence and Cloud Computing*, *3*(1), 16-35.

Kim, B., Hong, S., & Cameron, G. T. (2014). What corporations say matters more than what they say they do? A test of a truth claim and transparency in press releases on corporate websites and Facebook pages. *Journalism & Mass Communication Quarterly*, *91*(4), 811-829. https://doi.org/10.1177/1077699014550087

Kim, B., Kam, H. J., Park, Y. R., Yoo, S., Oh, J. S., Kim, Y.-H., & Lee, J.-H. (2018). Enchanted life space: adding value to smart health by integrating human

desires. *Healthcare Informatics Research*, *24*(1), 3-11. https://doi.org/10.4258/hir.2018.24.1.3

Kim, H.-W., & Gupta, S. (2014). A user empowerment approach to information systems infusion. *IEEE Transactions on Engineering Management*, *61*(4), 656-668. https://doi.org/10.1109/TEM.2014.2354693

Kim, T. B., & Ho, C.-T. B. (2021). Validating the moderating role of age in multi-perspective acceptance model of wearable healthcare technology. *Telematics and Informatics*, *61*, 101603. https://doi.org/10.1016/j.tele.2021.101603

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE Technical Report, Issue.

Klein, G., Jiang, J., & Saunders, C. (2006). Leading the horse to water. *Communications of the Association for Information Systems*, *18*(1), 259-274. https://doi.org/10.17705/1CAIS.01813

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134. https://doi.org/https://doi.org/10.1016/j.cose.2015.07.002

Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. *European Journal of Information Systems*, *31*(3), 388-409. https://doi.org/10.1080/0960085X.2021.1927212

Krauss, S. E. (2005). Research paradigms and meaning making: A primer. *The Qualitative Report*, *10*(4), 758-770.

Kreitmair, K. V. (2024). Mobile health technology and empowerment. *Bioethics*, *38*(6), 481-490.

Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N., & Volkamer, M. (2020). Security and privacy awareness in smart environments–a cross-country investigation. *In Proceedings of AsiaUSEC 2020, Financial Cryptography and Data Security*. https://doi.org/10.1007/978-3-030-54455-3_7

Kumar, R., Singh, D., Srinivasan, K., & Hu, Y. C. (2023). AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions. *Healthcare*, *11*(1), 81. https://doi.org/10.3390/healthcare11010081

Kuo, K.-M., Ma, C.-C., & Alexander, J. W. (2014). How do patients respond to violation of their information privacy? *Health Information Management Journal*, *43*(2), 23-33. https://doi.org/10.12826/18333575.2013.0011.Ma

Kwiecień, I., Kowalczyk-Rolczynska, P., & Popielas, M. (2020). Are the generations ready to accept the new technologies in life insurance underwriting? Questionnaire study in Poland. *IBIMA Business Review*, *2020*. https://doi.org/10.5171/2020.539912

Landau, R., Werner, S., Auslander, G. K., Shoval, N., & Heinik, J. (2010). What do cognitively intact older people think about the use of electronic tracking devices for people with dementia? A preliminary analysis. *International Psychogeriatrics*, *22*(8), 1301-1309. https://doi.org/10.1017/S1041610210001316

Langley, J., Wolstenholme, D., & Cooke, J. (2018). 'Collective making'as knowledge mobilisation: the contribution of participatory design in the co-creation of knowledge in healthcare. *BMC Health Services Research*, *18*, 1-10. https://doi.org/10.1186/s12913-018-3397-y

Lankshear, G., & Mason, D. (2001). Technology and ethical dilemmas in a medical setting: Privacy, professional autonomy, life and death. *Ethics and Information Technology*, *3*, 223-233. https://doi.org/10.1023/A:1012248219018

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social Issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22-42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Laverack, G. (2001). An identification and interpretation of the organizational aspects of community empowerment. *Community Development Journal*, *36*(2), 134-145.

Laverack, G., & Wallerstein, N. (2001). Measuring community empowerment: a fresh look at organizational domains. *Health Promotion International*, *16*(2), 179-185. https://doi.org/10.1093/heapro/16.2.179

LeBaron, V., Bennett, R., Alam, R., Blackhall, L., Gordon, K., Hayes, J., Homdee, N., Jones, R., Martinez, Y., Ogunjirin, E., Thomas, T., & Lach, J. (2020). Understanding the experience of cancer pain from the perspective of patients and family caregivers to inform design of an in-home smart health system: multimethod approach. *JMIR Formative Research*, *4*(8). https://doi.org/10.2196/20836

Lee, T., & Lee, H. (2020). Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19. *Media International Australia*, *177*(1), 47-60. https://doi.org/10.1177/1329878X20949545

Lee, W. W., Zankl, W., & Chang, H. (2016). An ethical approach to data privacy protection. *ISACA Journal*, *6*.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, *12*(1), 50. https://doi.org/10.17705/1CAIS.01250

Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems*, *144*, 271-290. https://doi.org/10.1016/j.future.2023.02.021

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445. https://doi.org/https://doi.org/10.1016/j.dss.2011.01.017

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8-17.

Li, J., Silvera-Tawil, D., Varnfield, M., Hussain, M. S., & Math, V. (2021). Users' perceptions toward mHealth technologies for health and well-being monitoring in pregnancy care: Qualitative interview study. *JMIR Formative Research*, *5*(12). https://doi.org/10.2196/28628

Li, X. (2018). Understanding eHealth literacy from a privacy perspective: eHealth literacy and digital privacy skills in American disadvantaged communities. *American Behavioral Scientist*, *62*(10), 1431-1449.

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), 453-496. https://doi.org/10.17705/1CAIS.02828

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471-481. https://doi.org/10.1016/j.dss.2012.06.010

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343-354. https://doi.org/10.1016/j.dss.2013.09.018

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114.

Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, *127*. https://doi.org/10.1016/j.chb.2021.107026

Liu, Y., Jiang, F., & Lin, P. (2021). Influence mechanism of the affordances of chronic disease management apps on continuance intention: questionnaire study. *In JMIR mHealth and uHealth*.

Locke, K., & Golden-Biddle, K. (1997). Constructing opportunities for contribution: Structuring intertextual coherence and "problematizing" in organizational studies. *Academy of Management journal*, *40*(5), 1023-1062.

Lomotey, R. K., Pry, J., & Sriramoju, S. (2017). Wearable IoT data stream traceability in a distributed health information system. *Pervasive and Mobile Computing*, *40*, 692-707. https://doi.org/10.1016/j.pmcj.2017.06.020

Lu, L., Zhang, J., Xie, Y., Gao, F., Xu, S., Wu, X., & Ye, Z. (2020). Wearable health devices in health care: narrative systematic review. *JMIR Mhealth and Uhealth*, *8*(11). https://doi.org/10.2196/18907

Lu, X., Hao, J., Shan, B., & Gu, A. (2021). Determinants of the Intention to Use Smart Healthcare Devices: A Framework and Public Policy Implications. *Journal of Healthcare Engineering*, *2021*. https://doi.org/10.1155/2021/4345604

Luque, A. E., Van Keken, A., Winters, P., Keefer, M. C., Sanders, M., & Fiscella, K. (2013). Barriers and facilitators of online patient portals to personal health records among persons living with HIV: formative research. *JMIR Research Protocols*, *2*(1). https://doi.org/10.2196/resprot.2302

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572-585. https://doi.org/10.1007/s11747-006-0003-3

Lyles, C. R., Adler-Milstein, J., Thao, C., Lisker, S., Nouri, S., & Sarkar, U. (2021). Alignment of key stakeholders' priorities for patient-facing tools in digital health: mixed methods study. *Journal of Medical Internet Research*, *23*(8), e24890.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293-334. https://doi.org/10.2307/23044045

Maher, N. A., Senders, J. T., Hulsbergen, A. F., Lamba, N., Parker, M., Onnela, J.-P., Bredenoord, A. L., Smith, T. R., & Broekman, M. L. (2019). Passive data collection and use in healthcare: A systematic review of ethical issues. *International Journal of Medical Informatics*, *129*, 242-247. https://doi.org/10.1016/j.ijmedinf.2019.06.015

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. https://doi.org/10.1287/isre.l040.0032

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). Big data: The next frontier for innovation, competition, and productivity. *McKinsey Global Institute*.

Mardonova, M., & Choi, Y. (2018). Review of wearable device technology and its applications to the mining industry. *Energies*, *11*(3). https://doi.org/10.3390/en11030547

Market.Us. (2023). *Global smart medical devices market*. Retrieved from https://market.us/report/smart-medical-devices-market/

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science*, *34*(5), 583-598.

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science and Technology Law Review*, *18*(1), 176-218. https://doi.org/10.2139/ssrn.2709584

Marx, G. T. (2015). Coming to terms: the kaleidoscope of privacy and surveillance. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 32-49). Cambridge University Press.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, *50*(4), 370-396.

Maslow, A. H. (1970). *Motivation and Personality* (2nd ed.). Harper & Row.

Maslow, A. H. (2013). *Toward a psychology of being*. Start Publishing LLC.

Mata-Cervantes, G., Clay, C. E., & Baxter, C. (2016). Empowering patients through their personal health record. In *NHS England*.

Matt, C., Becker, M., Kolbeck, A., & Hess, T. (2019). Continuously healthy, continuously used?–A thematic analysis of user perceptions on consumer health wearables. *Pacific Asia Journal of the Association for Information Systems*, *11*(1), 108-132. https://doi.org/10.17705/1pais.11105

May, C. R., Mair, F., Finch, T., MacFarlane, A., Dowrick, C., Treweek, S., Rapley, T., Ballini, L., Ong, B. N., & Rogers, A. (2009). Development of a theory of implementation and integration: Normalization Process Theory. *Implementation Science*, *4*(1), 1-9. https://doi.org/10.1186/1748-5908-4-29

McClair, T. L., Sripad, P., Casseus, A., Hossain, S., Abuya, T., & Gottert, A. (2021). The client empowerment in community health systems scale: development and validation in three countries. *Journal of Global Health*, *11*.

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, *6*(2), 35-59. https://doi.org/10.1080/10864415.2001.11044235

McLeod, S. (2007). Maslow's hierarchy of needs. *Simply Psychology*, *1*(1-18). https://www.simplypsychology.org/maslow.html

Mechanic, D., & Meyer, S. (2000). Concepts of trust among patients with serious illness. *Social Science & Medicine*, *51*(5), 657-668.

Meier, C. A., Fitzgerald, M. C., & Smith, J. M. (2013). eHealth: extending, enhancing, and evolving health care. *Annual Review of Biomedical Engineering*, *15*, 359-382.

Mettler, T., & Wulf, J. (2020). Health promotion with physiolytics: What is driving people to subscribe in a data-driven health plan. *PLoS One*, *15*(4), e0231705. https://doi.org/10.1371/journal.pone.0231705

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European*

Journal of Information Systems, *23*(2), 103-125. https://doi.org/10.1057/ejis.2013.17

Minheere, A., Lambrechts, W., Mampaey, J., Stough, T., Caniëls, M. C., & Semeijn, J. (2023). Patient power and empowerment: mitigating elements of valuable patient participation in healthcare collaboratives. *Behavioral Sciences*, *13*(4), 347.

Ministry of Health New Zealand. (1998). *The Social, Cultural and Economic Determinants of Health in New Zealand: Action to Improve Health.* Retrieved from https://www.health.govt.nz/system/files/documents/publications/det-health.pdf

Mir, D. J., Shvartzshnaider, Y., & Latonero, M. (2018, April 23-27). *It takes a village: A community based participatory framework for privacy design* 2018 IEEE European Symposium on Security and Privacy Workshops, https://doi.org/10.1109/EuroSPW.2018.00022

Mittelstadt, B. (2017). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology*, *19*(3), 157-175.

Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing and Management*, *58*(3), 102535.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS Medicine*, *6*(7), e1000097. https://doi.org/10.1136/bmj.b2535

Morley, J., & Floridi, L. (2019). The limits of empowerment: how to reframe the role of mHealth tools in the healthcare ecosystem. *Science and Engineering Ethics*, 1-25. https://doi.org/10.1007/s11948-019-00115-1

Mowday, R. T., & Sutton, R. I. (1993). Organizational behavior: Linking individuals and groups to organizational contexts. *Annual Review of Psychology*, *44*, 195-229.

Mueller, B., & Urbach, N. (2017). Understanding the why, what, and how of theories in IS research. *Communications of the Association for Information Systems*, *41*, 349-388. https://doi.org/10.17705/1CAIS.04117

Mujirishvili, T., Maidhof, C., Florez-Revuelta, F., Ziefle, M., Richart-Martinez, M., & Cabrero-García, J. (2023). Acceptance and privacy perceptions toward video-based active and assisted living technologies: Scoping review. *Journal of Medical Internet Research 25*, e45297. https://doi.org/10.2196/45297

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Nelson, E. C., Verhagen, T., & Noordzij, M. L. (2016). Health empowerment through activity trackers: An empirical smart wristband study. *Computers in Human Behavior*, *62*, 364-374. https://doi.org/10.1016/j.chb.2016.03.065

New Zealand IoT Alliance. (2017). *An analysis of the impact of the Internet of Things on the New Zealand economy*. Retrieved from https://iotalliance.org.nz/wp-content/uploads/sites/4/2018/09/Accelerating-a-Connected-New-Zealand-eBOOK.pdf

Nguyen, T. T., Tran Hoang, M. T., & Phung, M. T. (2022). “To our health!” Perceived benefits offset privacy concerns in using national contact-tracing apps. *Library Hi Tech*, *41*(1), 174-191. https://doi.org/10.1108/LHT-12-2021-0461

Niknejad, N., Foroutani, S., Nazari, B., Ghani, I., & Hussin, A. R. C. (2022). Smart Wellness Wearables Usage Intention Among Users in Malaysia: An Extension of Value-Based Adoption Model and Unified Theory of Acceptance and Use of Technology2. *Available at SSRN 4030570*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030570

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119-158.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, *24*(3), 831-852. https://doi.org/10.1007/s11948-015-9674-9

North, M. S., & Fiske, S. T. (2015). Modern attitudes toward older adults in the aging world: a cross-cultural meta-analysis. *Psychological Bulletin*, *141*(5), 993.

OECD. (2015). *Introducing high-value, privacy-protective health information systems*.

Onghena, P., Maes, B., & Heyvaert, M. (2019). Mixed methods single case research: State of the art and future directions. *Journal of Mixed Methods Research*, *13*(4), 461-480.

Osama, M., Ateya, A. A., Sayed, M. S., Hammad, M., Pławiak, P., Abd El-Latif, A. A., & Elsayed, R. A. (2023). Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions. *Sensors*, *23*(17), 7435. https://doi.org/10.3390/s23177435

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642-660. https://doi.org/10.1057/s41303-017-0056-z

Pan, J., Ding, S., Wu, D., Yang, S., & Yang, J. (2019). Exploring behavioural intentions toward smart healthcare services among medical practitioners: A technology transfer perspective. *International Journal of Production Research*, *57*(18), 5801-5820. https://doi.org/10.1080/00207543.2018.1550272

Pang, P. C.-I., McKay, D., Chang, S., Chen, Q., Zhang, X., & Cui, L. (2020). Privacy concerns of the Australian My Health Record: Implications for other large-scale opt-out personal health records. *Information Processing & Management*, *57*(6), 102364. https://doi.org/10.1016/j.ipm.2020.102364

Papa, A., Mital, M., Pisano, P., & Del Giudice, M. (2020). E-health and wellbeing monitoring using smart healthcare devices: An empirical investigation. *Technological Forecasting and Social Change*, *153*, 119226. https://doi.org/10.1016/j.techfore.2018.02.018

Paré, G., Tate, M., Johnstone, D., & Kitsiou, S. (2016). Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews. *European Journal of Information Systems*, *25*(6), 493-508. https://doi.org/10.1057/s41303-016-0020-3

Peek, S. T. M., Wouters, E. J., Luijkx, K. G., & Vrijhoef, H. J. (2016). What it takes to successfully implement technology for aging in place: focus groups with stakeholders. *Journal of Medical Internet Research 18*(5), e98. https://doi.org/10.2196/jmir.5253

Perez, A. J., & Zeadally, S. (2021). Recent advances in wearable sensing technologies. *Sensors*, *21*(20), 1-34. https://doi.org/10.3390/s21206828

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, *15*(4), 2-17. https://doi.org/10.1002/dir.1019

Pickard, A. J. (2013). *Research methods in information*. Facet publishing.

Pirzada, P., Wilde, A., Doherty, G. H., & Harris-Birtill, D. (2021). Ethics and acceptance of smart homes for older adults. *Informatics for Health and Social Care*, *47*(1), 10-37. https://doi.org/10.1080/17538157.2021.1923500

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, *50*, 32-44. https://doi.org/10.1016/j.intmar.2019.10.004

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903. https://doi.org/10.1037/0021-9010.88.5.879

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531-544. https://doi.org/10.1177/014920638601200408

Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of Counseling Psychology*, *52*(2), 126.

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: a scoping review. *International Journal of Information Management*, *74*, 102719.

Pramanik, M. I., Lau, R. Y. K., Demirkan, H., & Azad, M. A. K. (2017). Smart health: Big data enabled health paradigm within smart cities. *Expert Systems with Applications*, *87*, 370-383. https://doi.org/https://doi.org/10.1016/j.eswa.2017.06.027

Prati, A., Shan, C., & Wang, K. I.-K. (2019). Sensors, vision and networks: From video surveillance to activity recognition and health monitoring. *Journal of Ambient Intelligence and Smart Environments*, *11*(1), 5-22. https://doi.org/10.3233/AIS-180510

Princi, E., & Krämer, N. C. (2020). Out of control – Privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology*, *11*, 1-15. https://doi.org/10.3389/fpsyg.2020.582054

Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and Artificial Intelligence: An Experiential Perspective. *Journal of Marketing*, *85*(1), 131-151. https://doi.org/10.1177/0022242920953847

Rahman, M. J., Morshed, B. I., Harmon, B., & Rahman, M. (2022). A pilot study towards a smart-health framework to collect and analyze biomarkers with low-cost and flexible wearables. *Smart Health*, *23*. https://doi.org/10.1016/j.smhl.2021.100249

Ramaswamy, V., & Ozcan, K. (2014). *The co-creation paradigm*. Stanford University Press.

Rappaport, J. (1987). Terms of empowerment/exemplars of prevention: Toward a theory for community psychology. *American Journal of Community Psychology*, *15*(2), 121-148. https://doi.org/10.1007/BF00919275

Rashidi, P., & Mihailidis, A. (2013). A survey on ambient-assisted living tools for older adults. *IEEE Journal of Biomedical and Health Informatics*, *17*(3), 579-590. https://doi.org/10.1109/JBHI.2012.2234129

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and Internet of Things in healthcare and medical sector: Applications, challenges, and future perspectives. *Journal of Food Quality*, 1-20. https://doi.org/10.1155/2021/7608296

Ravishankar, V. K., Burleson, W., & Mahoney, D. (2015). Smart home strategies for user-centered functional assessment of older adults. *International Journal of Automation and Smart Technology*, *5*(4), 233-242. https://doi.org/10.5875/ausmt.v5i4.952

Ravitch, S. M., & Carl, N. M. (2019). *Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological*. Sage Publications.

Ray, P. P., Dash, D., & Kumar, N. (2020). Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. *Computer Communications*, *160*, 111-131. https://doi.org/10.1016/j.comcom.2020.05.029

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology 36*(1), 16-38.

Ribeiro, C. D. S., van de Burgwal, L. H. M., & Regeer, B. J. (2019). Overcoming challenges for designing and implementing the One Health approach: A systematic review of the literature. *One Health*, *7*, 100085. https://doi.org/10.1016/j.onehlt.2019.100085

Rissel, C. (1994). Empowerment: the holy grail of health promotion? *Health Promotion International*, *9*(1), 39-47.

Rogers, E. M. (2003). *Diffusion of Innovations, 5th Edition*. Free Press.

Rohan, M. J. (2000). A rose by any name? The values construct. *Personality and Social Psychology Review*, *4*(3), 255-277. https://doi.org/10.1207/S15327957PSPR0403_4

Rosemann, M., & Vessey, I. (2008). Toward improving the relevance of information systems research to practice: the role of applicability checks. *MIS Quarterly*, 1-22. https://doi.org/10.2307/25148826

Rouidi, M., Elouadi, A. E., Hamdoune, A., Choujtani, K., & Chati, A. (2022). TAM-UTAUT and the acceptance of remote healthcare technologies by healthcare professionals: A systematic review. *Informatics in Medicine Unlocked*, *32*, 101008. https://doi.org/10.1016/j.imu.2022.101008

Ruhlandt, R. W. S. (2018). The governance of smart cities: A systematic literature review. *Cities*, *81*, 1-23.

Runkle, J., Sugg, M., Boase, D., Galvin, S. L., & C. Coulson, C. (2019). Use of wearable sensors for pregnancy health and environmental monitoring: Descriptive findings from the perspective of patients and providers. *Digital Health*, *5*, 1-14. https://doi.org/10.1177/2055207619828220

Ryan, A. B. (2006). Post-positivist approaches to research. *Researching and Writing your Thesis: a guide for postgraduate students*, 12-26.

Sahin, I. (2006). Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. *Turkish Online Journal of Educational Technology-TOJET*, *5*(2), 14-23.

Salehi-Amiri, A., Jabbarzadeh, A., Hajiaghaei-Keshteli, M., & Chaabane, A. (2022). Utilizing the Internet of Things (IoT) to address uncertain home health care supply chain network. *Expert Systems with Applications*, *208*, 118239. https://doi.org/10.1016/j.eswa.2022.118239

Sandberg, J., & Alvesson, M. (2011). Ways of constructing research questions: gap-spotting or problematization? *Organization*, *18*(1), 23-44.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business ethics*, *46*, 111-126.

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results. In M. Sarstedt, M. Schwaiger, & C. R. Taylor (Eds.), *Measurement and Research Methods in International Marketing* (Vol. 22, pp. 195-218). Emerald Group Publishing Limited.

Sayibu, M., Chu, J., Akintunde, T. Y., Rufai, O. H., Amosun, T. S., & George-Ufot, G. (2022). Environmental conditions, mobile digital culture, mobile usability, knowledge of app in COVID-19 risk mitigation: A structural equation model analysis. *Smart Health*, *25*. https://doi.org/10.1016/j.smhl.2022.100286

Schaefer, G. O., & Ballantyne, A. (2022). Ethics of digital contact tracing wearables. *Journal of Medical Ethics*, *48*(9), 611-615. https://doi.org/10.1136/medethics-2020-106958

Schiavone, F., Mancini, D., Leone, D., & Lavorato, D. (2021). Digital business models and ridesharing for value co-creation in healthcare: A multi-stakeholder ecosystem analysis. *Technological Forecasting and Social Change*, *166*, 120647.

Schoeman, F. (1984). Privacy: Philosophical Dimensions. *American Philosophical Quarterly*, *21*(3), 199-213. http://www.jstor.org.ezproxy.aut.ac.nz/stable/20014049

Schomakers, E.-M., & Ziefle, M. (2023). Privacy vs. security: trade-offs in the acceptance of smart technologies for aging-in-place. *International Journal of Human–Computer Interaction*, *39*(5), 1043-1058. https://doi.org/10.1080/10447318.2022.2078463

Schulz-Baldes, A., Vayena, E., & Biller-Andorno, N. (2007). Sharing benefits in international health research: Research ‐ capacity building as an example of an indirect collective benefit. *European Molecular Biology Organization (EMBO) Reports*, *8*(1), 8-13.

Schwartz, S. H. (2012). An overview of the Schwartz theory of basic values. *Online Readings in Psychology and Culture*, *2*(1), 1-20. https://doi.org/10.9707/2307-0919.1116

Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J.-E., & Demirutku, K. (2012). Refining the theory of basic individual values. *Journal of Personality and Social Psychology*, *103*(4), 663-688. https://doi.org/doi.org/10.1037/a0029393

Schwartz, S. H., Sagiv, L., & Boehnke, K. (2000). Worries and values. *Journal of Personality*, *68*(2), 309-346. https://doi.org/10.1111/1467-6494.00099

Seberger, J. S., & Patil, S. (2021). Post-COVID public health surveillance and privacy expectations in the United States: Scenario-based interview study. *JMIR Mhealth Uhealth*, *9*(10), e30871. https://doi.org/10.2196/30871

Segura Anaya, L., Alsadoon, A., Costadopoulos, N., & Prasad, P. (2018). Ethical implications of user perceptions of wearable devices. *Science and Engineering Ethics*, *24*(1), 1-28. https://doi.org/10.1007/s11948-017-9872-8

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: insights and implications. *Healthcare*, *8*(2), 1-18. https://doi.org/10.3390/healthcare8020133

Seibert, S. E., Wang, G., & Courtright, S. H. (2011). Antecedents and consequences of psychological and team empowerment in organizations: a meta-analytic review. *Journal of Applied Psychology*, *96*(5), 981-1003. https://doi.org/10.1037/a0022676

Seiferth, A., & Schaarschmidt, M. (2020). Sharing personal health and fitness data with health insurance providers: An empirical study considering trust and risk. *In Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Shachak, A., Kuziemsky, C., & Petersen, C. (2019). Beyond TAM and UTAUT: Future directions for HIT implementation research. *Journal of Biomedical Informatics 100*, 103315. https://doi.org/10.1016/j.jbi.2019.103315

Shah, R., & Ward, P. T. (2003). Lean manufacturing: context, practice bundles, and performance. *Journal of Operations Management 21*(2), 129-149.

Shalley, C. E., Zhou, J., & Oldham, G. R. (2004). The effects of personal and contextual characteristics on creativity: Where should we go from here? *Journal of Management 30*(6), 933-958. https://doi.org/10.1016/j.jm.2004.06.007

Shapiro, D. E., Duquette, C., Abbott, L. M., Babineau, T., Pearl, A., & Haidet, P. (2019). Beyond burnout: a physician wellness hierarchy designed to prioritize interventions at the systems level. *The American Journal of Medicine*, *132*(5), 556-563. https://doi.org/10.1016/j.amjmed.2018.11.028

Sharkey, A., & Sharkey, N. (2012). Granny and the robots: Ethical issues in robot care for the elderly. *Ethics and Information Technology*, *14*(1), 27-40. https://doi.org/10.1007/s10676-010-9234-6

Shearer, N. B. (2007). Toward a nursing theory of health empowerment in homebound older women. *Journal of Gerontological Nursing*, *33*(12), 38-45. https://doi.org/10.3928/00989134-20071201-05

Shen, J., Xiao, L. D., Liu, Y., Zhang, H., & Wu, L. (2021). A phenomenological study on new care needs of maslow's need-hierarchy among disabled residents at nursing homes in modern Chinese society. *Journal of Transcultural Nursing*, *32*(5), 501-507. https://doi.org/10.1177/1043659620967426

Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics*, *125*, 1-12. https://doi.org/10.1016/j.ijmedinf.2019.01.014

Shimizu, Y., Ishizuna, A., Osaki, S., Hashimoto, T., Tai, M., Tanibe, T., & Karasawa, K. (2022). The social acceptance of smart health services in Japan. *International Journal of Environmental Research and Public Health*, *19*(3), 1298. https://doi.org/10.3390/ijerph19031298

Shimizu, Y., Osaki, S., Hashimoto, T., & Karasawa, K. (2021). How do people view various kinds of smart city services? Focus on the acquisition of personal information. *Sustainability (Switzerland)*, *13*(19). https://doi.org/10.3390/su131911062

Shrout, P. E., & Bolger, N. (2002). Mediation in experimental and nonexperimental studies: new procedures and recommendations. *Psychological Methods*, *7*(4), 422. https://doi.org/10.1037/1082-989X.7.4.422

Sidorova, A., Evangelopoulos, N., Valacich, J. S., & Ramakrishnan, T. (2008). Uncovering the intellectual core of the information systems discipline. *MIS Quarterly*, 467-482.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167-196. https://doi.org/10.2307/249477

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087-1155. https://doi.org/10.2307/3481326

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477-564. https://doi.org/10.2307/40041279

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, *44*, 745-772.

Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical issues in big data analytics: A stakeholder perspective. *Communications of the Association for Information Systems*, *44*, 718-747. https://doi.org/10.17705/1CAIS.04434

Sovacool, B. K., & Del Rio, D. D. F. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews*, *120*. https://doi.org/10.1016/j.rser.2019.109663

Spence Laschinger, H. K., Gilbert, S., Smith, L. M., & Leslie, K. (2010). Towards a comprehensive theory of nurse/patient empowerment: applying Kanter's empowerment theory to patient care. *Journal of Nursing Management*, *18*(1), 4-13. https://doi.org/10.1111/j.1365-2834.2009.01046.x

Spreitzer, G. M. (1995). Psychological empowerment in the workplace: Dimensions, measurement, and validation. *Academy of Management Journal*, *38*(5), 1442-1465. https://doi.org/10.5465/256865

Srivastava, N. K., Chatterjee, N., Subramani, A., Akbar Jan, N., & Singh, P. K. (2022). Is health consciousness and perceived privacy protection critical to use wearable health devices? Extending the model of goal-directed behavior. *Benchmarking: An International Journal*, *29*(10), 3079-3096. https://doi.org/10.1108/BIJ-12-2020-0631

Stavropoulos, T. G., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S., & Kompatsiaris, I. (2020). IoT wearable sensors and devices in elderly care: a literature review. *Sensors*, *20*(10), 2826. https://doi.org/10.3390/s20102826

Stewart, K., & Segars, A. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*, 36-49. https://doi.org/10.1287/isre.13.1.36.97

Suárez Vázquez, A., Del Río Lanza, A. B., Suárez Álvarez, L., & Vázquez Casielles, R. (2017). Empower me? Yes, please, but in my way: different patterns of experiencing empowerment in patients with chronic conditions. *Health Communication*, *32*(7), 910-915. https://doi.org/10.1080/10410236.2016.1196409

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal*, *49*(4), 633-642.

Suman, A. B. (2017). In search for the value of connectivity: Accountable citizens fostering accountable governance via connectivity: The case of environmental

health policies. *In 2017 IEEE International Conference on Cloud Engineering (IC2E)*. https://doi.org/10.1109/IC2E.2017.49

Sutton, R. I., & Staw, B. M. (1995). What theory is not. *Administrative Science Quarterly*, 371-384.

Swift, C., & Levin, G. (1987). Empowerment: An emerging mental health technology. *Journal of Primary Prevention*, *8*(1-2), 71-94. https://doi.org/10.1007/BF01695019

Swinkels, I. C. S., Huygens, M. W. J., Schoenmakers, T. M., Nijeweme-D'Hollosy, W. O., Van Velsen, L., Vermeulen, J., Schoone-Harmsen, M., Jansen, Y. J., Van Schayck, O. C., & Friele, R. (2018). Lessons learned from a living lab on the broad adoption of eHealth in primary health care. *Journal of Medical Internet Research 20*(3), e83.

Talal, M., Zaidan, A., Zaidan, B., Albahri, A. S., Alamoodi, A., Albahri, O. S., Alsalem, M., Lim, C. K., Tan, K. L., Shir, W., & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of Medical Systems*, *43*(3). https://doi.org/10.1007/s10916-019-1158-z

Tallon, P. P. (2013). Corporate governance of big data: Perspectives on value, risk, and cost. *Computer*, *46*(6), 32-38. https://doi.org/10.1109/MC.2013.155

Talwar, S., Dhir, A., Islam, N., Kaur, P., & Almusharraf, A. (2023). Resistance of multiple stakeholders to e-health innovations: Integration of fundamental insights and guiding research paths. *Journal of Business Research*, *166*. https://doi.org/10.1016/j.jbusres.2023.114135

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1-22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

Taylor, S. J., Bogdan, R., & DeVault, M. (2016). *Introduction to qualitative research methods: A guidebook and resource* (4th ed.). John Wiley & Sons, Incorporated.

The Ministry of Health New Zealand. (2017). *HISO 10064:2017 Health Information Governance Guidelines* https://www.tewhatuora.govt.nz/assets/Publications/10064-health-information-governance-guideline-2017.docx

Thelancet.com. (2023). *Wearable health data privacy*. Retrieved from https://www.thelancet.com/journals/landig/article/PIIS2589-7500(23)00055-9/fulltext

Thiebes, S., Gao, F., Briggs, R. O., Schmidt-Kraepelin, M., & Sunyaev, A. (2023). Design concerns for multiorganizational, multistakeholder collaboration: A study in the healthcare industry. *Journal of Management Information Systems*, *40*(1), 239-270. https://doi.org/10.1080/07421222.2023.2172771

Torre, D. A. (1986). *Empowerment: Structured conceptualization and instrument development (power, questionnaire construction, multidimensional scaling)*. Cornell University.

Tran, C. D., & Nguyen, T. T. (2021). Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. *Technology in Society*, *67*, 101755. https://doi.org/10.1016/j.techsoc.2021.101755

Trkman, M., Popovič, A., & Trkman, P. (2023). The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications. *Government Information Quarterly*, *40*(1). https://doi.org/10.1016/j.giq.2022.101787

Truex, D., Holmström, J., & Keil, M. (2006). Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems*, *7*(1), 33.

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*.

Valle-Cruz, D. (2019). Public value of e-government services through emerging technologies. *International Journal of Public Sector Management*, *32*(5), 530-545. https://doi.org/10.1108/IJPSM-03-2018-0072

van Uden-Kraan, C. F., Drossaert, C. H., Taal, E., Seydel, E. R., & van de Laar, M. A. (2009). Participation in online patient support groups endorses patients' empowerment. *Patient Education and Counseling*, *74*(1), 61-69. https://doi.org/10.1016/j.pec.2008.07.044

Vargo, S. L., Maglio, P. P., & Akaka, M. A. (2008). On value and value co-creation: A service systems and service logic perspective. *European Management Journal*, *26*(3), 145-152. https://doi.org/10.1016/j.emj.2008.04.003

Velykoivanenko, L., Niksirat, K. S., Zufferey, N., Humbert, M., Huguenin, K., & Cherubini, M. (2021). Are those steps worth your privacy? Fitness-tracker users' perceptions of privacy and utility. *In Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. https://doi.org/10.1145/3494960

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21-54. https://doi.org/10.25300/MISQ/2013/37.1.02

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, *17*(7), 435-495. https://doi.org/10.17705/1jais.00433

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157-178. https://doi.org/10.2307/41410412

Wagner, A., Wessels, N., Brakemeier, H., & Buxmann, P. (2021). Why free does not mean fair: Investigating users' distributive equity perceptions of data-driven services. *International Journal of Information Management*, *59*. https://doi.org/10.1016/j.ijinfomgt.2021.102333

Wagner, G., Prester, J., Roche, M. P., Schryen, G., Benlian, A., Paré, G., & Templier, M. (2021). Which factors affect the scientific impact of review papers in IS research? A scientometric study. *Information & Management*, *58*(3), 103427. https://doi.org/10.1016/j.im.2021.103427

Wagner, S. C., & Sanders, G. L. (2001). Considerations in ethical decision-making and software piracy. *Journal of Business Ethics*, *29*, 161-167. https://doi.org/10.1023/A:1006415514200

Wakefield, S. E., Elliott, S. J., Eyles, J. D., & Cole, D. C. (2006). Taking environmental action: the role of local composition, context, and collective. *Environmental Management*, *37*, 40-53.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220. https://doi.org/10.2307/1321160

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information systems*, *13*(1), 2.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii-xxiii.

Weick, K. E. (1995). What theory is not, theorizing is. *Administrative science quarterly*, *40*(3), 385-390.

Weiss, L., & Johar, G. V. (2013). Egocentric categorization and product judgment: Seeing your traits in what you own (and their opposite in what you don't). *Journal of Consumer Research*, *40*(1), 185-201. https://doi.org/10.1086/669330

Westin, A. F. (1967). *Privacy and freedom*. The Bodley Head.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431-453.

Wiegard, R.-B., & Breitner, M. H. (2019). Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. *Electronic Markets*, *29*(1), 107-123. https://doi.org/10.1007/s12525-017-0274-1

Windasari, N. A., Lin, F., & Kato-Lin, Y. (2021). Continued use of wearable fitness technology: A value co-creation perspective. *International Journal of Information Management*, *57*, 102292. https://doi.org/10.1016/j.ijinfomgt.2020.102292

Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, *35*(1), 36-51. https://doi.org/10.1080/01972243.2018.1542648

Winter, J. S., & Davidson, E. (2022). Harmonizing regulatory regimes for the governance of patient-generated health data. *Telecommunications Policy*, *46*(5), 102285. https://doi.org/10.1016/j.telpol.2021.102285

Wolfenden, L., Reilly, K., Kingsland, M., Grady, A., Williams, C. M., Nathan, N., Sutherland, R., Wiggers, J., Jones, J., & Hodder, R. (2019). Identifying opportunities to develop the science of implementation for community-based non-communicable disease prevention: a review of implementation trials. *Preventive Medicine*, *118*, 279-285. https://doi.org/10.1016/j.ypmed.2018.11.014

Xing, F., Peng, G., Zhang, B., Li, S., & Liang, X. (2021). Socio-technical barriers affecting large-scale deployment of AI-enabled wearable medical devices among the ageing population in China. *Technological Forecasting and Social Change*, *166*, 120609. https://doi.org/10.1016/j.techfore.2021.120609

Xu, H., & Bélanger, F. (2013). Information systems journal special issue on: Reframing privacy in a networked world. *Information Systems Journal*, *23*(4), 371-375. https://doi.org/10.1111/isj.12026

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824. https://doi.org/10.17705/1jais.00281

Xu, H., & Zhang, N. (2022). From contextualizing to context theorizing: assessing context effects in privacy research. *Management Science*, *68*(10), 7383-7401. https://doi.org/10.1287/mnsc.2021.4249

Xu, Z. (2019). An empirical study of patients' privacy concerns for health informatics as a service. *Technological Forecasting and Social Change*, *143*, 297-306. https://doi.org/10.1016/j.techfore.2019.01.018

Yan, Z., Kantola, R., & Zhang, P. (2011). *A research model for human-computer trust interaction* 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China. https://doi.org/10.1109/TrustCom.2011.37

Yang, C. (2022). Digital contact tracing in the pandemic cities: Problematizing the regime of traceability in South Korea. *Big Data and Society*, *9*(1). https://doi.org/10.1177/20539517221089294

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: An extension of the theory of planned behavior. *Industrial Management & Data Systems*, *117*(1), 68-89. https://doi.org/10.1108/IMDS-01-2016-0017

Yin, R. K. (2017). *Case study research and applications: design and methods* (6th Ed. ed.). Sage.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570-601. https://doi.org/10.1016/j.im.2018.10.001

Zahra, S. A. (2007). Contextualizing theory building in entrepreneurship research. *Journal of Business Venturing*, *22*(3), 443-452. https://doi.org/https://doi.org/10.1016/j.jbusvent.2006.04.007

Zahra, S. A., Wright, M., & Abdelgawad, S. G. (2014). Contextualization and the advancement of entrepreneurship research. *International Small Business Journal*, *32*(5), 479-500. https://doi.org/10.1177/0266242613519807

Zakaria, N., & Ramli, R. (2017). Physical factors that influence patients' privacy perception toward a psychiatric behavioral monitoring system: a qualitative study. *Neuropsychiatric Disease and Treatment*, *14*, 117-128. https://doi.org/10.2147/NDT.S115261

Zaman, U., Mehmood, F., Iqbal, N., Kim, J., & Ibrahim, M. (2022). Towards secure and intelligent Internet of Health Things: A Survey of enabling technologies and applications. *Electronics (Switzerland)*, *11*(12), 1-43. https://doi.org/10.3390/electronics11121893

Zarcadoolas, C., Vaughon, W. L., Czaja, S. J., Levy, J., & Rockoff, M. L. (2013). Consumers' perceptions of patient-accessible electronic medical records. *Journal of Medical Internet Research*, *15*(8). https://doi.org/10.2196/jmir.2507

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, *12*(1), 86-122. https://doi.org/10.17705/1pais.12104

Zhang, J., Li, H., Luo, X., & Warkentin, M. (2017). Exploring the effects of the privacy‐handling management styles of social networking sites on user satisfaction: a conflict management perspective. *Decision Sciences*, *48*(5), 956-989. https://doi.org/10.1111/deci.12243

Zhang, N. A., Wang, C. A., Karahanna, E., & Xu, Y. (2022). Peer privacy concern: Conceptualization and measurement. *MIS Quarterly*, *46*(1), 491-530. https://doi.org/10.25300/MISQ/2022/14861

Zhang, Y., Liu, C., Luo, S., Xie, Y., Liu, F., Li, X., & Zhou, Z. (2019). Factors influencing patients' intentions to use diabetes management apps based on an extended Unified Theory of Acceptance and Use of Technology model: Web-based survey. *Journal of Medical Internet Research 21*(8), e15023. https://doi.org/10.2196/15023

Zhu, Y., Lu, Y., Gupta, S., Wang, J., & Hu, P. (2022). Promoting smart wearable devices in the health-AI market: the role of health consciousness and privacy protection. *Journal of Research in Interactive Marketing*, *17*(2), 257-272. https://doi.org/10.1108/JRIM-10-2021-0246

Zimmer, M. P., Vassilakopoulou, P., Grisot, M., & Niemimaa, M. (2023). Call for Papers - Special Issue: Embracing Contrarian Thinking: Value-Reflexive Research for a Digital World. *European Journal of Information Systems*, 1-4.

Zimmerman, M. A. (1990). Taking aim on empowerment research: On the distinction between individual and psychological conceptions. *American Journal of Community Psychology*, *18*(1), 169-177.

Zimmerman, M. A. (2000). Empowerment Theory. In J. Rappaport & E. Seidman (Eds.), *Handbook of Community Psychology* (pp. 43-63). Springer.

Zou, Y., Sun, K., Afnan, T., Abu-Salma, R., Brewer, R., & Schaub, F. (2024). Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Proceedings on Privacy Enhancing Technologies*, *1*, 133-150. https://doi.org/10.56553/popets-2024-0009

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology 30*(1), 75-89. https://doi.org/10.1057/jit.2015.5

Appendices

Appendix A: Chapter 2 - Review Studies Summary

Appendix Table A. 1

Previous review studies on privacy in the health information technology domain

Article	Study context	Review type	Search strategy					Included studies	Contextual definition	Highlight of contextual matters		Theoretical model	Method	Research agenda
			Keywords	Database	Coverage date	Inclusion / exclusion	Process of screening and selection			Antecedent	Outcome			
Al-rawashdeh et al. (2022)	IoT adoption and smart healthcare	Systematic review	✓	✓	2015-2021	✓✓	✓	22	N/A	N/A	✓	N/A	✓	N/A
Al-Shaqi et al. (2016)	Ambient assisted living systems (AALS)	Comprehensive and critical review	✓	✓	2001-2016	✓	Not clear	133	N/A	N/A	N/A	N/A	N/A	N/A
Carver and Mackinnon (2020)	Wearables and smart home or ambient assistive living (AAL) devices	Scoping review	✓	✓	2007-2018	✓	✓	20	N/A	Surveillance	N/A	N/A	N/A	N/A

Hassan et al. (2023)	AI-driven smart city healthcare monitoring	Systematic review	✓	✓	N/A	Not clear	✓	70	N/A	N/A	Not clear	N/A	N/A	N/A
Ismail et al. (2020)	eHealth	Scoping Review	N/A	✓	1793-2020	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Keshta (2022)	AI-driven IoT for smart health care	Systematic review	✓	✓	N/A	✓	✓	50	N/A	N/A	N/A	N/A	N/A	Not clear
Kumar et al. (2023)	AI-powered blockchain for public Health, smart health applications	Contemporary review, Systematic review		✓	2012-2022	✓✓	✓	120	N/A	N/A	N/A	N/A	N/A	Not clear
Lu et al. (2020)	Wearable health devices in health care	Narrative systematic review	✓	✓	2015-2019	✓✓	✓	82	N/A	N/A	N/A	N/A	N/A	Not clear
Mujirishvili et al. (2023)	Active and assisted living (AAL) technologies	Scoping review	✓	✓	Up to 2021	✓✓	✓	22	N/A	Not clear	✓	N/A	✓	N/A
Ratta et al. (2021)	IoT and blockchain in healthcare systems	Not specify	Not clear	✓	2008-2020	✓✓	Not clear	22	N/A	Not clear	N/A	N/A	N/A	Not clear
Shen et al. (2019)	Health information exchange (HIE), health information technology (HIT)	Systematic review	✓	✓	2004-2017	✓	✓	59	✓	✓	✓	✓	✓	✓
Talal et al. (2019)	IoT-based smart home	Systematic review	✓	✓	2007-2017	✓✓	✓	9	N/A	Not clear	N/A	N/A	N/A	✓
Zaman et al. (2022)	Internet of Health Things	Systematic review	✓	✓	2016-2022	✓✓	Not clear	384	Not clear	✓	N/A	N/A	N/A	✓

Appendix B: Chapter 2 - Coding Results

Appendix Table B. 1

Theories used to explain the antecedents

Category	Antecedents	Privacy proxy	Theory
Individual	Perceived health information sensitivity	Perceived privacy risk	PCT (Wiegard & Breitner, 2019)
	Surveillance concerns	N/A	Theory of communicative action (Chadborn et al., 2019)
	Mobile users' information privacy concerns	Perceived privacy risk	MUIPC (Wiegard & Breitner, 2019)
Stakeholder	Stakeholders' experience of using mHealth	Perceived risk (including privacy risk)	Categorization theory (Pan et al., 2019)
	Implementation of data mechanisms	N/A	CI theory, Notions of borders (Burrows et al., 2018)

For the individual antecedents, PCT was the most commonly used theory in privacy research. In the smart health domain, PCT was used as the extended risk-benefit analysis framework to predict the impact of perceived health information sensitivity on perceived privacy risk (Wiegard & Breitner, 2019). The MUIPC model was considered as an important predictor of individuals' perception of privacy risk in a smart monitoring service (Wiegard & Breitner, 2019). In addition, the theory of communicative action was used to interpret the divergence between the experience and views of participants regarding their privacy concerns when using smart home monitoring devices (or services) (Chadborn et al., 2019).

In terms of organizational antecedents, categorization theory (or principles) was used to explain the interplay between individuals and products, proposing that customers classify the products they own as integral to their personal self (Weiss & Johar, 2013). In the healthcare area, categorization theory was employed to interpret medical practitioners' initial impression and acceptance of smart healthcare. In this theory, customers' acceptance of a new product may be based on similarity with earlier products rather than on the technology itself (Pan et al., 2019). CI theory highlights a desirable state in which individuals strive to keep perceived private information private in accordance with the context (Nissenbaum, 2010). In the privacy and smart health monitoring literature, the notion of borders and CI theory were jointly used to explain the stakeholder antecedent, with the argument that data management mechanisms of smart homes should meet the criteria of robustness and plasticity inherent to boundary

objects because they are associated with the privacy expectations of other household members in smart homes (Burrows et al., 2018).

Appendix Table B. 2

Theories used to explain the outcomes

Category	Outcomes	Privacy proxy	Theory
Individual	Adoption/use/ participation	Perceived privacy risk	The concept of risk-risk tradeoff, PCT (Tran & Nguyen, 2021)
		Privacy concerns	Unique theoretical framework of 'surveillance culture' (Choi & Kim, 2024)
		N/A	IDT, Person-centered care (Fritz et al., 2016)
		N/A	Balance theory (Hassandoust, Johnston, et al., 2021)
	Continuous use	N/A	UTAUT 2, HITAM, HIPC (Matt et al., 2019)
	Intention to adoption/use	N/A	UTAUT (Arar et al., 2021; Dadhich et al., 2022)
		Privacy concerns	UTAUT (Zhu et al., 2022)
		Perceived privacy risk	UTAUT (Zhang et al., 2019)
		Privacy concerns	PCT, TPB (Princi & Krämer, 2020)
		Perceived privacy risk	TAM, IDT, PMT, PCT (Karahoca et al., 2018)
		Loss of privacy	TAM (Liu & Tao, 2022)
	Attitude toward adoption	Loss of privacy	TAM (Papa et al., 2020)
	Trust in technology/services	Loss of privacy	TAM (Liu & Tao, 2022)
		N/A	TAM, TRA, TPB, UTAUT2 (Bhatt & Chakraborty, 2020)
	Perceived value	Perceived privacy risk	The concept of risk-risk tradeoff, PCT (Tran & Nguyen, 2021)
		Perceived privacy risk	PCT, TPB, TRA (Wiegard & Breitner, 2019)
	Feelings of health empowerment	Privacy protection	Self-regulation theory (Nelson et al., 2016)
	Perceived usefulness	Loss of privacy	TAM (Papa et al., 2020)
		N/A	UTAUT (Sayibu et al., 2022)
	Perceived ease of use	Loss of privacy	TAM (Papa et al., 2020)
Organizational	Medical practitioners' attitude to adopting smart healthcare services	N/A	Valence framework (Pan et al., 2019)
Stakeholder	Smart home development	N/A	Foucault's theory (governmentality and bio-power) (Suman, 2017)
	Implementation of smart health services	N/A	Normalization process theory (NPT) (Peek et al., 2016)

In terms of the individual outcome aspect, theories of TAM, UTAUT, and/or UTAUT2 were commonly used to test individual-related outcomes affected by privacy. Based on the individual's perceived usefulness (PU) and perceived ease of use (EOU) of that information technology (Davis, 1989), TAM in smart health studies was extended with other characteristics, e.g., some AI-specific factors, to examine the impact of the loss of privacy on users' trust in smart technology and their adoption intention (Liu & Tao, 2022). UTAUT was formulated with four core determinants (i.e., experience, voluntariness, age, and gender) aiming to explain users' intentions to use information technology (Venkatesh et al., 2003). For instance, it was applied to test the relationship between privacy issues and individuals' intention to adopt certain smart health monitoring services (Dadhich et al., 2022). Extending UTAUT with three additional constructs of habit, price value, and hedonic motivation (El-Masri & Tarhini, 2017; Venkatesh et al., 2012), researchers combined UTAUT2 with other theories to explain the privacy impact on individuals' continuous use (e.g., Matt et al., 2019) and their trust in the new smart healthcare devices (or services) (e.g., Bhatt & Chakraborty, 2020). Moreover, PCT was often employed to investigate the trade-off between benefits and privacy-related risks (e.g., Tran & Nguyen, 2021; Wiegard & Breitner, 2019). In the reviewed literature, PCT was used to test the impact of privacy issues on individuals' perception of an application's value and individuals' intention to use the application following integration with other theories, such as the concept of risk-risk trade-off (Tran & Nguyen, 2021), IDT (Karahoca et al., 2018), PMT (Karahoca et al., 2018), TPB, and TRA (Princi & Krämer, 2020; Wiegard & Breitner, 2019). Other theories, including the balance theory (Hassandoust, Johnston, et al., 2021), the health information technology acceptance model (HITAM), the health information privacy concerns model (HIPC) (Matt et al., 2019), and the unique theoretical framework of 'surveillance culture' (Choi & Kim, 2024), were applied in the literature to explore individuals' use or their continuous use of smart healthcare services in health monitoring contexts. Moreover, self-regulation theory was used to examine the feelings of health empowerment as an outcome at the individual level (Nelson et al., 2016).

With regard to the organizational outcomes, researchers used the valence framework to evaluate the privacy-related impact of smart healthcare services on medical practitioners' attitudes toward adopting these services from an integrated economics and psychology perspective (Pan et al., 2019). In terms of stakeholder-related outcomes, Foucault's theory integrating governmentality and bio-power was applied to explore the relationship between privacy and overall smart home development from a collective perspective of key stakeholders (Suman, 2017). This theory is related to oppressive practices enabled by authoritarian relations

of power and knowledge (Banville, 2020). Moreover, normalization process theory (NPT) was adopted to investigate the overall implementation effectiveness of smart health services affected by privacy issues (Peek et al., 2016), proposing the necessary factors for successfully implementing and integrating interventions into routine tasks (May et al., 2009).

Appendix Table B. 3

Methods used in the published articles

Method	Frequency	Articles
Quantitative		
Survey	21	Aljedaani et al. (2023); Bhatt and Chakraborty (2020); Choi and Kim (2024); Dadhich et al. (2022); del Río-Lanza et al. (2020); Deng et al. (2018); Etemad-Sajadi and Dos Santos (2019); Karahoca et al. (2018); Kwiecień et al. (2020); Liu and Tao (2022); Lu et al. (2021); Mettler and Wulf (2020); Nelson et al. (2016); Pan et al. (2019); Papa et al. (2020); Runkle et al. (2019); Sayibu et al. (2022); Shimizu et al. (2021); Tran and Nguyen (2021); Zhang et al. (2019); Zhu et al. (2022)
Experiment	2	Princi and Krämer (2020); Seiferth and Schaarschmidt (2020)
Qualitative		
Interview	10	Alzahrani et al. (2021); Beaudin et al. (2006); Burrows et al. (2018); (Esmaeilzadeh, 2023); Fritz et al. (2016); Hassandoust, Johnston, et al. (2021); Kennedy et al. (2021); LeBaron et al. (2020); Li et al. (2021); Matt et al. (2019)
Focus group	4	Ghorayeb et al. (2021); Hunter et al. (2020); Peek et al. (2016); Xing et al. (2021)
Case study	3	Ravishankar et al. (2015); Shimizu et al. (2022); Suman (2017)
Longitudinal study	1	Chen et al. (2021)
Workshop	1	Kim et al. (2018)
Jury session	1	Chadborn et al. (2019)
Qualitative survey	1	Kulyk et al. (2020)
Mixed-methods		
Developmental	2	Cristiano et al. (2022a); Wiegard and Breitner (2019)
Diversity	2	Arar et al. (2021); Balta-Ozkan et al. (2013)
Completeness	1	Choi et al. (2020)

Appendix Table B. 4

Coding of privacy definitions/descriptions

Definitions and causal explanations	Perspectives					Article
	Right	Commodity	Control	State	N/A	
Privacy definitions						
"The concept of privacy has therefore evolved in the digital age to include contextual integrity… which advocates the flow of personal information should be contextually appropriate" (p. 113).			X			Burrows et al. (2018)
Perceived privacy is "other people can see my data without (letting) me knowing; …other people will release my data against my will; …difficult to maintain the data totally protected; …difficult to ensure that good use is made of the data" (p. 142).			X			del Río-Lanza et al. (2020)
"Four views on privacy emerged: 'privacy as modesty', 'private by nature', 'privacy normed', and 'privacy as American'" (p. 150). "'Privacy as modesty' was portrayed as the idea of being watched while not fully clothed" (p. 150). "'Private by nature' was seen as a form of privacy that involved a general way of life in which one maintains a significant part of personal life that is considered private" (p. 150). "'Privacy normed' referred to the idea that a group view (societal or cultural) exists regarding what individuals do, or not do, in private." "'Privacy as American' was associated with the language of the historical values of United States' citizens such as rights to life and liberty, which included the right to privacy" (p. 150).	X		X	X		Fritz et al. (2016)
"A fundamental aspect of privacy is the control over personal data" (p. 4). "…individuals evaluate anticipated benefits and perceived risks in order to make a rational decision regarding the disclosure of their personal data…people will rather not use IoT in healthcare when they perceive privacy risks" (p. 3).		X	X			Princi and Krämer (2020)

"…information privacy refers to individuals' control over the collection, unauthorized access and improper use of their personal information" (p. 3).	X	X			Tran and Nguyen (2021)
Privacy (or privacy proxies) with causal explanations/descriptions					
Perceived privacy captures users' attitudes toward personal health information disclosure. Privacy threats were attributable to the subthemes of perceived relativity, severity, and control.	X	X			Matt et al. (2019)
Privacy risk refers to the possibility of information abuse, such as information theft and leakage due to using mHealth services.			X		Deng et al. (2018)
Individuals' privacy concerns are related to their sensitive health data sharing and their ability to control their lifestyles.		X			Hassandoust, Johnston, et al. (2021)
Perceived risks mostly refer to the "potential for loss associated with releasing personal information".	X		X		Karahoca et al. (2018)
Different people rate privacy's importance differently for a myriad of reasons across different circumstances.				X	Kennedy et al. (2021)
Concerns were expressed regarding privacy and data sharing, e.g., what exactly is being collected and where the data is going, and when.		X			LeBaron et al. (2020)
Loss of privacy refers to how an individual perceives that using smart healthcare services infringes on their privacy. Perceived loss of privacy negatively influenced consumers' acceptance of m-health services.	X		X		Liu and Tao (2022)
Perceived privacy protection is the perception of the likelihood that a smart wristband provider will protect consumers' confidential information collected during electronic transfer from unauthorized use or disclosure.		X			Nelson et al. (2016)
There is a loss of privacy as smart wearable healthcare records personal information.			X		Papa et al. (2020)
Privacy concerns of mobile users are modeled using three dimensions: errors, perceived intrusion, and secondary use of personal information. Individuals compare perceived privacy risks (PPR) with anticipated benefits.	X	X			Wiegard and Breitner (2019)

Perceived privacy risk is defined as patients' feeling of a lack of control over their personal information after adopting mobile apps, and it is not consistent with a real privacy risk.	X		Zhang et al. (2019)
Privacy concerns reflect an individual's sense of boundary, self-protection, and control. Users' concerns about the violation of their ability to control their personal information have also become increasingly severe.	X	X	Zhu et al. (2022)

Appendix Table B. 5

Coding of privacy proxies

Privacy proxy	Frequency	Percentage	Articles
Not using a proxy	23	47%	Alzahrani et al. (2021); Arar et al. (2021); Balta-Ozkan et al. (2013); Beaudin et al. (2006); Bhatt and Chakraborty (2020); Burrows et al. (2018); Chadborn et al. (2019); Dadhich et al. (2022); Etemad-Sajadi and Dos Santos (2019); Fritz et al. (2016); Hassandoust, Johnston, et al. (2021); Hunter et al. (2020); Kennedy et al. (2021); Kulyk et al. (2020); Kwiecień et al. (2020); LeBaron et al. (2020); Li et al. (2021); Peek et al. (2016); Ravishankar et al. (2015); Sayibu et al. (2022); Shimizu et al. (2021); Suman (2017); Xing et al. (2021)
Privacy concerns (or perceived)	9	18%	Choi and Kim (2024); Choi et al. (2020); Cristiano et al. (2022a); Ghorayeb et al. (2021); Kim et al. (2018); Mettler and Wulf (2020); Princi and Krämer (2020); Runkle et al. (2019); Zhu et al. (2022)
Privacy risk (or perceived)	7	14%	Deng et al. (2018); Esmaeilzadeh (2023); Karahoca et al. (2018); Lu et al. (2021); Tran and Nguyen (2021); Wiegard and Breitner (2019); Zhang et al. (2019)
Privacy protection	3	6%	Chen et al. (2021); Nelson et al. (2016); Shimizu et al. (2022)
Perceived risk (including privacy risk)	3	6%	del Río-Lanza et al. (2020); Pan et al. (2019); Seiferth and Schaarschmidt (2020)
Loss of privacy	2	4%	Liu and Tao (2022); Papa et al. (2020)
Perceived privacy	1	2%	Matt et al. (2019)
Privacy policy	1	2%	Aljedaani et al. (2023)

Appendix Table B. 6

Surveillance focused as a matter of context

Category	Keywords	Articles
Highlight	Monitoring, tracking	Alzahrani et al. (2021)
	Monitoring	Aljedaani et al. (2023)
	Monitoring sensors	Burrows et al. (2018)
	Sensors, video camera	Arar et al. (2021); Balta-Ozkan et al. (2013)
	Personal tracking	Beaudin et al. (2006)
	Safety monitoring	Chadborn et al. (2019)
	Sensor, passive monitoring	Choi et al. (2020); Hunter et al. (2020)
	Remote monitoring	Cristiano et al. (2022a)
	Intrusiveness	Etemad-Sajadi and Dos Santos (2019)
	Intervention	Fritz et al. (2016)
	Interventions, surveillance	Shimizu et al. (2022)
	Ethical, monitoring	Kennedy et al. (2021)
	Spying, surveillance, monitoring, eavesdropping	Kulyk et al. (2020)
	Continuous tracking	Matt et al. (2019)
	Constantly tracking	Mettler and Wulf (2020)
	Constant monitoring (Regular check-ups, ongoing screening, continuing surveillance of health status, monitoring symptoms, constant observation of signs, being controlled)	Esmaeilzadeh (2023)
	Sensors	Ravishankar et al. (2015)
	Surveillance, anxieties	Shimizu et al. (2021)
	Surveillance culture, surveillance imaginary, surveillance practices, watched	Choi and Kim (2024)
	Acceptance of monitoring	Kwiecień et al. (2020)
	Watching, recording	LeBaron et al. (2020)
	Track, nonintrusive, passive	Li et al. (2021)
	Monitoring, negative beliefs	Nelson et al. (2016)
	Duration of monitoring, behavioral modification	Runkle et al. (2019)
	Social surveillance	Tran and Nguyen (2021)
	Technology surveillance	Sayibu et al. (2022)
Mention	Monitoring technology	Ghorayeb et al. (2021)
	Surveillance	Kim et al. (2018)
	Extensive collection	Princi and Krämer (2020)
	Tracking, behavioral profiles	Wiegard and Breitner (2019)
	Track	Xing et al. (2021)
	Feeling of being followed or watched	Papa et al. (2020)
	Feeling under surveillance	Zhu et al. (2022)
Not mention		Bhatt and Chakraborty (2020); Chen et al. (2021); Dadhich et al. (2022); del Río-Lanza et al. (2020); Deng et al. (2018); Hassandoust, Johnston, et al. (2021); Karahoca et al. (2018); Liu and Tao (2022); Lu et al. (2021); Pan et al. (2019); Papa et al. (2020); Seiferth and Schaarschmidt (2020); Suman (2017); Zhang et al. (2019)

Appendix Table B. 7

Stakeholder focused as a matter of context

Category	Stakeholders	Articles	Frequency	Percentage
Single stakeholder	Individuals	Aljedaani et al. (2023); Arar et al. (2021); Bhatt and Chakraborty (2020); Burrows et al. (2018); Chadborn et al. (2019); Chen et al. (2021); Choi and Kim (2024); Choi et al. (2020); Dadhich et al. (2022); del Río-Lanza et al. (2020); Esmaeilzadeh (2023); Etemad-Sajadi and Dos Santos (2019); Fritz et al. (2016); Ghorayeb et al. (2021); Hassandoust, Johnston, et al. (2021); Hunter et al. (2020); Karahoca et al. (2018); Kennedy et al. (2021); Kulyk et al. (2020); Kwiecień et al. (2020); Liu and Tao (2022); Lu et al. (2021); Matt et al. (2019); Mettler and Wulf (2020); Nelson et al. (2016); Pan et al. (2019); Papa et al. (2020); Princi and Krämer (2020); Ravishankar et al. (2015); Sayibu et al. (2022); Seiferth and Schaarschmidt (2020); Shimizu et al. (2022); (Shimizu et al., 2021); Suman (2017); Tran and Nguyen (2021); Zhang et al. (2019); Zhu et al. (2022)	35	71%
	Healthcare professionals	Hunter et al. (2020); Pan et al. (2019)	2	4%
Multiple stakeholders	Healthcare providers and individuals	Beaudin et al. (2006); Cristiano et al. (2022a); Deng et al. (2018); LeBaron et al. (2020); Li et al. (2021); Runkle et al. (2019)	6	12%
	Insurance companies and individuals	Wiegard and Breitner (2019)	1	2%
	Experts (Industrial) and individuals	Balta-Ozkan et al. (2013)	1	2%
	Service providers, technology developers, and individuals	Alzahrani et al. (2021)	1	2%

Individuals, device providers, and healthcare providers	Xing et al. (2021)	1	2%
Healthcare experts, IT experts, and law professionals	Kim et al. (2018)	1	2%
Individuals, healthcare providers, technology designers and suppliers, and policy makers	Peek et al. (2016)	1	2%

Appendix C: Chapter 3 - Supplementary Materials

Appendix Table C. 1

Literature review summary of privacy concerns in the smart health monitoring context

No	Author(s) and Year	HIT area	Privacy conceptualization	Proxy used	Determinant factors	Contention of privacy and health values	Theory /framework	Method	Participant	Main finding(s)
1	Bansal et al. (2010)	Personal health information	"privacy is defined as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 138).	Privacy concern	Perceived health information sensitivity, Previous online privacy invasion	N/A	Utility Theory	Quantitative	Student population	The conceptual model argues that individuals' intention to disclose such information depends on their trust, privacy concern, and information sensitivity, which are determined by personal dispositions—personality traits, information sensitivity, health status, prior privacy invasions, risk beliefs, and experience—acting as intrinsic antecedents of trust.
2	Burrows et al. (2018)	Smart home	"The concept of privacy has therefore evolved in the digital age to include contextual integrity (Nissenbaum, 2010), which advocates the flow of personal information should be contextually appropriate" (p. 113).	N/A	Mechanisms	N/A	Contextual integrity	Qualitative	Households	The study has uncovered a need for mechanisms that allow people to interact more directly with data that will be collected and collated in smart homes in the not-so-distant future.
3	Chadborn et al. (2019)	Smart health	N/A	N/A	Technological: misuse of technology	Our interpretation of life-world and systems-	The theory of Communicative Action	Qualitative	Older adults	Views of older people were felt to be frequently ignored by organizations implementing systems and

						world perspectives enabled a nuanced understanding of these tensions or trade-offs within the implementation and experience of a smart city for older people.	developed by Habermas			technologies. Participants demonstrated diverse levels of digital literacy and a range of concerns about misuse of technology.
4	del Río-Lanza et al. (2020)	mHealth	Perceived risk to inadequate privacy means "other people can see my data without (letting) me knowing; … other people will release my data against my will; …difficult to maintain the data totally protected; … difficult to ensure that good use is made of the data". (p. 142)	Perceived risk of inadequate privacy	N/A	N/A	N/A	Quantitative	Patients	Variables such as digital information, perceived effort and social influence increase the intention of using mHealth. On the other hand, inadequate information acts as a barrier that restrains the intention of using mHealth.
5	Deng et al. (2018)	mHealth	Privacy risk refers to the possibility of information abuse, such as information theft and leakage due to using mHealth services.	Privacy risk	N/A	N/A	Technology acceptance model (TAM)	Quantitative	Patients	The results corroborated that the proposed model fits well. Trust, perceived usefulness (PU), and perceived ease of use positively correlated with mHealth service adoption. Privacy and performance risks negatively correlated with the patients' trust and

										adoption intention toward mHealth services.
6	Dhanireddy et al. (2014)	Electronic medical records	N/A	Privacy concerns	N/A	No	No	Qualitative	Patients	Despite their initial lack of knowledge of the health record, focus group participants were overwhelmingly positive about the prospect of online access to medical records. However, they worried about potential loss of privacy and interference with the patient–provider relationship.
7	Fritz et al. (2016)	Smart home	Four views on privacy emerged: 'privacy as modesty', 'private by nature', 'privacy normed', and 'privacy as American' (p. 150)	N/A	N/A	Openness to the idea of adopting such a technology was influenced by perceived loss of privacy and compensation for this perceived loss with a feeling of safety and knowledge of receipt of health-assistance.	Diffusion of Innovation theory; Person-centered care	Qualitative	Older adults	Implications for adoption arise from the level of help needed to remain independent and the acceptable loss of privacy. As the level of need increases, the acceptable loss of privacy increases with it. This appears to be a recognized fact by older adults in this study. One participant pointed out that moving into an assisted living or nursing home would alter levels of privacy as well.
8	Gao et al. (2015)	Medical wearable device	N/A	Perceived privacy risk	N/A	Since HIT may aggravate individuals' privacy concerns over the potential misuse of	privacy calculus	Quantitative	Users of healthcare wearable devices	Consumer's decision to adopt healthcare wearable technology is affected by factors from technology, health, and privacy perspectives.

						personal health information (Li et al., 2014), consumers' decisions to adopt healthcare wearable technology would involve a highly salient privacy calculus in which users may face the tradeoff between perceived benefits and perceived privacy risks				
9	Gupta et al. (2021)	Digital healthcare	"Privacy is a key concern in the development of AI systems, specifically in the health care field, as a large amount of private information, such as phone numbers, social security numbers, pin codes, usage locations and other clinical records, etc., is involved in the AI system process" (p. 2261).	Perceived privacy risk	Ethical risk	N/A	Perceived risk theory	Quantitative	Not specify	This study attempts to establish that AI risks in digital healthcare are positively associated with responsible artificial intelligence. The moderating effect of perceived trust and perceived privacy risks are also examined. We answered two important questions: (a) what are the practices of responsible AI? and (b) what perceived risks have been associated with

										the development of responsible AI?
10	Hassandoust, Johnston, et al. (2021)	Pay-As-You-Live service and Health wearable devices	Individuals' privacy concerns are related to their sensitive health data sharing and their ability to control their lifestyles.	Privacy concerns	N/A	Potential sources of discord for consumers with the system relates to their ability to participate in the system in a way that maximizes benefit and reduces risk to their privacy and control over their lifestyle choices.	Balance theory	Qualitative	PAYL services consumers	The three entities of interest are the PAYL service users, health insurance providers, and one of the identified attitude objects. The whole system works when there is balance (participation of users in the PAYL service) but fails under conditions of imbalance.
11	Karahoca et al. (2018)	Internet of things (IoT) products in healthcare	Perceived risks mostly refer to the "potential for loss associated with releasing personal information"	Perceived Privacy Risk	N/A	Privacy calculus theory was adopted to present anticipated benefits and perceived risks which affect an individual's decision to share information with others.	TAM, IDT, protection motivation theory, privacy calculus theory	Quantitative	Residents	The results show that for females, compatibility and trialability have more impact on perceived ease of use (PEOU) whereas for males PA has more impact on PEOU. Image, perceived privacy risk, perceived vulnerability have more impact on males when compared to females.
12	Kulyk et al. (2020)	Smart home and health	N/A	privacy issues	Influence of culture	No	No	Qualitative	Owners and non-owners of	As researchers stress the importance of context in

		environments							smart home environments	determining privacy issues, our findings provide a further confirmation for this approach, indicating the need to consider both cultural factors and context of a specific system or data exchange in order to support the end users with their security and privacy protection.
13	LeBaron et al. (2020)	In-Home Smart health system	Concerns were expressed regarding privacy and data sharing, e.g., what exactly is being collected and where the data is going, and when.	Privacy concerns	N/A	N/A	N/A	Mixed methods	Patients and family caregivers	Smart health systems to support cancer pain management should (1) account for the experience of both the patient and the caregiver, (2) prioritize passive monitoring of physiological and environmental variables to reduce burden, and (3) include functionality that can monitor and track medication intake and efficacy.
14	Liu and Tao (2022)	AI-smart healthcare	Loss of privacy refers to how an individual perceives that using smart healthcare services infringes on their privacy. Perceived loss of privacy negatively influenced consumers' acceptance of mHealth services.	Loss of privacy	N/A	N/A	TAM	Quantitative	Users of smart healthcare services	The results showed that perceived usefulness, perceived ease of use, and the three AI-specific characteristics were important determinants of public acceptance of smart healthcare services, whose roles were fully or partially mediated by trust.
15	Luque et al. (2013)	Personal medical informatics	N/A	Privacy concerns	N/A	N/A	N/A	Mixed-methods	Patients	The participants have experience using computers and most are interested in

										PHR features. However, computer or broadband access and privacy are important barriers.
16	Matt et al. (2019)	Consumer Health Wearables (CHWs)	Perceived privacy captures users' attitudes toward personal health information disclosure. Privacy threats were attributable to the subthemes of perceived relativity, severity, and control.	Perceived privacy	N/A	The continuous use depends on an individual's trade-off decision between the beneficial and adverse properties of tracker use.	UTAUT 2; the Health Information Technology Acceptance Model (HITAM); Health Information Privacy Concerns Model (HIPC)	Qualitative	Users of fitness trackers	It identifies 11 subthemes to attribute to three main user determinants (perceived benefit, deficiency, and privacy).
17	Nelson et al. (2016)	Activity trackers	Perceived privacy protection is the perception of the likelihood that a smart wristband provider will protect consumers' confidential information collected during electronic transfer from unauthorized use or disclosure.	privacy protection	N/A	N/A	Self-regulation theory	Quantitative	Individuals wearing smart wristbands	This study showed that the system-specific elements of smart wristbands do influence an individual's feelings of empowerment. The provision of feedback, attractiveness and privacy protection mattered but their (significant) influence was rather weak in nature. The results confirm that health empowerment leads to normative and affective commitment.
18	Papa et al. (2020)	Smart healthcare	There is a loss of privacy as smart wearable healthcare records personal information. Intrusiveness refer to a loss of privacy as smart wearable healthcare	loss of privacy	N/A	N/A	TAM	Quantitative	Individuals (Not specified)	The results indicated that intrusiveness and comfort do not have a significant direct impact on Intention to use Behavior Intention (BI) SWH devices. At the same time Intrusiveness had

			(SWH) devices are recording personal information.							a significant impact on PU of SWH devices and Comfort has a strong significant impact on PU and PEOU of smart wearables.
19	Princi and Krämer (2020)	eHealth	"A fundamental aspect of privacy is the control over personal data" (p. 4).	Privacy concerns; Perceived privacy risks	N/A	"individuals evaluate anticipated benefits and perceived risks in order to make a rational decision regarding the disclosure of their personal data…people will rather not use IoT in healthcare when they perceive privacy risks" (p. 3).	Privacy calculus theory; theory of planned behavior	Quantitative	Individuals (Not specified)	The study demonstrates that while actual control does not affect the willingness to use IoT in healthcare, people have a higher intention to use an IoT healthcare device when they perceive to be in control of their data.
20	Sovacool and Del Rio (2020)	Smart homes	N/A	N/A	N/A	"Whether users will adopt and embrace this motley collection of devices…concerns about privacy, security, and hacking must be	N/A	Qualitative	Experts from six different types of institutions	The study critically examines the potential perils of smart home technologies alongside their promise, together with a broader range of sustainability dimensions, emphasizing not only energy and climate attributes but also issues related to privacy, trust, demographics, politics, and socio-technical systems.

						addressed" (p. 16)				
21	Tran and Nguyen (2021)	mHealth	"information privacy refers to individuals' control over the collection, unauthorized access and improper use of their personal information" (p. 3).	Perceived privacy risk	N/A	Perceived privacy risk is negatively associated with perceived value of COVID-19 contact-tracing apps.	The concept of risk-risk tradeoff; privacy calculus theory	Quantitative	Users of contact-tracing apps	Findings revealed that users engage in health risk-privacy risk tradeoff when evaluating and deciding to use the apps.
22	Wiegard and Breitner (2019)	Pay-As-You-Live service and wearable technologies	Privacy concerns of mobile users are modeled using three dimensions: errors, perceived intrusion, and secondary use of personal information. Individuals compare perceived privacy risks (PPR) with anticipated benefits.	Perceived privacy risks	Information sensitivity, Regulatory expectation Mobile users' information privacy concerns	The perceived privacy risk by individuals is negatively associated with perceived value.	PCT; TPB; TRA;	Mixed-methods	Experts from insurance companies; the participants were recruited from social network groups associated with healthcare wearable devices and two forums on the topics wearables tech, fitness and smartwatches.	The results show that current privacy risk factors dominate the perceived value of an individual to use PAYL services.
23	Xu (2019)	Health Informatics as a Service (HIaaS)	N/A	Privacy concerns	Privacy awareness, perceived informativeness, information sensitivity, privacy social norms,	N/A	The expectancy theory	Quantitative	Individuals (Not specified)	Five antecedent factors at different levels influence patients' privacy concern for HIaaS, including privacy awareness (patient level), perceived informativeness (service level), information sensitivity (information contingency), regulatory expectations (macro-

					regulatory expectation, importance of information transparency					environmental level), and importance of information transparency (organizational level). Privacy concern for HIaaS significantly affects patients' trust belief, perceived privacy risk, and adoption intention.
24	Zarcadoolas et al. (2013)	Electronic medical record	N/A	Privacy concerns	N/A	Participants appeared willing to make tradeoffs, accepting the potential risk of breaches to their personal privacy for the convenience and accessibility of electronic records.	No	Qualitative	vulnerable consumers	Major themes were enhanced consumer engagement/patient empowerment, extending the doctor's visit/enhancing communication with health care providers, literacy and health literacy factors, improved prevention and health maintenance, and privacy and security concerns.
25	Zhang et al. (2019)	Diabetes management apps	Perceived privacy risk is defined as patients' feeling of a lack of control over their personal information after adopting mobile apps, and it is not consistent with a real privacy risk.	perceived privacy risk	N/A	N/A	Unified Theory of Acceptance and Use of Technology (UTAUT)	Quantitative	Adult patients with diabetes who were familiar with diabetes management apps	Performance expectancy and social influence are the most important determinants of the intention to use diabetes management apps. Facilitating conditions and perceived privacy risk also have an impact on behavioral intention. Therefore, it is necessary to improve facilitating

										conditions and provide solid privacy protection.
26	Zhu et al. (2022)	Smart wearable devices	Privacy concerns reflect an individual's sense of boundary, self-protection, and control. Users' concerns about the violation of their ability to control their personal information have also become increasingly severe.	Privacy concerns	N/A	N/A	UTAUT	Quantitative	Individuals (Not specified)	Privacy concerns of consumers have a negative effect on smart wearable devices usage, while health consciousness positively impacts consumers' usage of smart wearable devices.

Appendix Table C. 2

Appropriateness of a developmental mixed-methods design (Adapted from Venkatesh et al. (2016))

Steps in mixed-methods inquiry	Property of mixed-methods research	Decision consideration	Other design decision(s) likely to affect the current decision	Design decision
Step 1: Decide on the appropriateness of a mixed-methods design	Research questions	A mixed-method design was used as we intend to provide a holistic understanding of the value of privacy in health information technology (HIT) use, by developing and testing a SHMS health empowerment model. Neither the quantitative nor qualitative method alone is sufficient to answer the research question of this study.	Research goals and objectives	Research question: This study aims to answer the following question: *How do users' value perceptions of health empowerment and privacy evolve in the context of SHMSs, and what factors influence these changes?*
	Purposes of mixed-methods research	One of the main purposes of a mixed methods research is to ensure that the questions from one strands emerge from the conclusions of a previous strands, or to use one strands to develop hypotheses to be tested in the next. Given the lack of our understanding on users' value perceptions of health empowerment and privacy in the SHMSs context, a mixed-methods approach helps to develop hypotheses within the SHMS health empowerment model and empirically test them. It matches a developmental purpose.	Research question	The purpose of the present mixed-methods research is to develop and then test a SHMS health empowerment model. This 'developmental' purpose involves using the findings of a qualitative study to develop a suitable set of constructs, establish relationships among these constructs in the form of a model, and propose a corresponding set of hypotheses, and then test the hypotheses through a quantitative method.
	Paradigmatic view	The present research seeks answers to the research questions, following a post-positivist research paradigm. It posits that the reality of privacy phenomena and their impact on health empowerment in the context of SHMSs have imperfectly been explored, but grants such reality can be discovered as accurately as possible.	Research question, purpose of mixed methods	Overall, we followed a post-positivist research paradigm to uncover multiple perspectives (Creswell & Poth, 2018). For the qualitative strand, we followed an interpretive phenomenological approach (IPA) for understanding participants experiences and thinking about the privacy phenomenon in relation to health empowerment in SHMS contexts through the perspective of participants (SHMS users or potential users), rather than the researcher (Cohen et al., 2013). Quantitative strand: we adopted the post-positivist perspective where there are a priori fixed hypotheses in the form of the causal relationships between the phenomenon that are investigated with the structured instruments. The data analysis approach is deductive. The hypotheses are either supported or rejected based on the results of statistical analysis (Cohen et al., 2013).
	Epistemological perspective	Qualitative and quantitative components of the study used the different paradigmatic assumptions. The present research investigates epistemologies by way of assumptions about knowledge. It explores privacy issues in relation to health empowerment in SHMSs, striving for objectivity beyond just the facts.	Research question, purposes of mixed methods	Single paradigm stance.

Step 2: Develop strategies for mixed-methods approach	Design investigation strategy	This research was intended to develop and test a model and associated hypotheses.	Research question, paradigmatic assumption	Study 1 (Qualitative) Study 2 (Quantitative)
	Strands of research	This research involved two stages of studies.	Purpose of mixed-methods research	Multistrand design
	Mixing strategy	The qualitative and quantitative components of the study are mixed in that the qualitative results informed the quantitative design.	Purposes of mixed-methods research, strands/phases of research	Sequentially mixed methods
	Time orientation	The data collection was conducted sequentially, starting with the qualitative strand, followed by the quantitative strand.	Research questions, strands of research	Sequential design
	Priority of methodological approach	The qualitative and quantitative components are equally important.	Research question, strands of research	Equivalent status design
Step 3: Develop strategies for collecting and analysing mixed-methods data	Sampling design strategies	The samples for the quantitative and qualitative components of the study were from Australia, New Zealand, and the United States.	Design investigation strategy, time orientation	We implemented sequential mixed-methods sampling strategy with parallel samples to collect the qualitative and quantitative data. A purposive random sampling strategy was employed in the qualitative strand, targeting participants with knowledge and experience in specific SHMSs. These systems ranged from those used in clinical trials to surveillance-based monitoring products available in the local market. The quantitative strand used a probability sampling strategy where individuals were randomly selected from the population, who was claiming to be able to understand what is a smart health monitoring system (SHMS).
	Data collection strategies	Qualitative data were collected in Study 1. Quantitative data were collected in Study 2.	Sampling design strategies, time orientation, strands of research	Study 1 were based on semi-structured interviews with open-ended questions using an interview transcript. The participants' voice was recorded for this strand. Study 2 were based on an online questionnaire survey with closed-ended questions adapted from the previously validated measurement items.
	Data analysis strategy	Qualitative data were firstly analyzed, followed by quantitative data analysis.	Time orientation, data collection strategy, strands of research	A sequential qualitative-quantitative analysis design was used.
Step 4: Draw meta-inferences from mixed methods findings	Type of reasoning	The data analysis included developing and testing/ confirming hypotheses.	Design investigation strategy	Inductive and deductive theoretical reasoning.
Step 5: Assess the quality of meta-inferences	Inference quality	The qualitative and quantitative inferences met the standards.	Research question, design strategy, sampling design, data collection and data	We maintained a primary focus on the research purpose and research question throughout all data analysis, interpretations, and discussions.

			analysis strategies, type of reasoning	In Study 1, we used different types of validity checks, including design validity, analytical validity, and inferential validity (Venkatesh et al., 2013). ● We adhered to descriptive validity to ensure the accuracy of our (the researchers') reports. ● For credibility and transparency ensuring that the results of qualitative strand are credible and believable, we collected data from a purposive random sample of participants with knowledge and experience in specific SHMSs. ● To ensure analytical validity, we employed well-designed protocol for data collection. The interview protocol was pre-tested to finetune the questions based on feedback and suggestions from respondents. During the interviews, we asked every question in the prescribed order according to the interview protocol. ● Moreover, inferential validity was evaluated to ensure we can accurately understand participants' experiences, views, and intentions. This was achieved by obtaining participants' feedback during the interviews. We also coded and reported data as closely as possible to participants' interview transcripts and notes. In Study 2, we assessed the statistical results. As reported, the statistical validity criteria including construct validity, internal validity, discriminant validity and statistical conclusion validity also confirmed that the quantitative inference met the criteria (Venkatesh et al., 2013).
Step 6: Discuss potential threats and remedies	Inference quality	Potential issues were discussed and addressed with appropriate remedies.	Data collection strategies, data analysis strategies	We have taken several remedial actions to address the data collection and data analysis threats. ● To avoid unequal sample sizes for the data collection, both qualitative and quantitative studies had a fairly large sample size. ● To avoid potential bias in the data collection, a specific interview protocol/script was used in Study 1 for all interviewees. A third-party agency data collection platform was used in Study 2 for the participant recruitment and quantitative data collection. ● To remove threat(s) to data conversion, we analyzed the qualitative data by creating codes and then counting codes and evaluating their weights. ● We also assessed and discussed the validity of both studies to address threats to multiple validates (as discussed above).

Appendix Table C. 3

Interview participants' profiles

Participant#	Age	Gender	Industry	Occupation	Education	Familiarity with SHMSs	End-user?
1*	35	Female	Government	Director of Clinical Digital Governance	Postgraduate diploma	Very familiar	No
2	45	Male	Government	Manager of Data Governance	Master's degree	Familiar	No
3*	78	Female	N/A	Retired	N/A	Very familiar	Yes
4*	34	Female	Government	Staff	Master's degree	Very familiar	Yes
5	47	Female	Healthcare	Caregiver	High school	Familiar	No
6	38	Female	Healthcare	Nurse	Bachelor's degree	Very familiar	No
7	45	Female	Healthcare	Caregiver	Bachelor's degree	Familiar	No
8	33	Male	Technology	Technical manager	Doctorate degree	Very familiar	No
9	35	Female	Healthcare	Nurse	Postgraduate diploma	Very familiar	No
10*	51	Female	Healthcare	Project manager	Doctorate degree	Very familiar	No
11	30	Male	Technology	Developer	Doctorate degree	Very familiar	No
12	43	Female	Healthcare	Caregiver	High school	Familiar	No
13*	52	Female	Education	Lecturer	Doctorate degree	Not familiar	Yes
14	77	Female	Education	Retired	High school	Not familiar	Yes
15	34	Male	Technology	Staff	Bachelor's degree	Familiar	Yes
16	25	Female	Education	Student	Master's degree	Not familiar	Yes
17	38	Male	Technology	Unemployed	Master's degree	Not familiar	Yes
18	37	Female	Marketing	Staff	Bachelor's degree	Not familiar	Yes
19	49	Male	Technology	Staff	Bachelor's degree	Familiar	Yes
20	50	Female	Education	Staff	Master's degree	Familiar	Yes

Appendix Table C. 4

Selected quotes by respondents

Constructs and descriptions	Selected quotes supporting each construct (1st order)	Themes (2nd order)	Aggregated aspects
Legislation of data privacy protection includes the right to information, provisions prohibiting or restricting the use of mechanisms of data governance, rules on IT-security-legislation, provisions supporting the use of mechanisms, and so on (Weber, 2010).	● *"We definitely take legality very seriously. We know what our obligations are when it comes to privacy through privacy law, through privacy codes"* (participant#2). ● *"I'm not as familiar as I should be…I guess in New Zealand where generally people are pretty well protected it's an area that's really difficult to make sure it's well covered in law."* (participant#3). ● *"I think I am very familiar with the existing privacy acts and codes …not so much in-depth…we were repeatedly mentioned all those acts when we have nursing courses"* (participant#5).	Legislative protection	Regulatory and sociocultural
Transparency refers to ensuring everything is visible, denoting one's openness or open communication to pursue trustworthiness (Kim et al., 2014).	● *"Many people have privacy concerns based on assumptions and once we educate them and attempt to manage health data in a more transparent way, they are gonna have more concerns"* (participant#1). ● *"You [government health authorities] can also be very clear in your privacy-related materials about what the information will be used for… you can provide what we call a layered privacy statement…if you want more information go to this 3 pages, 5 pages, 10 pages, whatever it is that gives you the full explanation of the system. We wrote a probably 60 or 70-page privacy impact assessment associated with COVID tracer…so people who really wanted to know what's going on [can] go and read the full document…but for the relatively small number of people that could read that code and understand it, they could go there and confirm that"* (participant#2). ● *"At this point you will naturally think of saying I have to let him know [the patient] what I'm going to do first, and then, definitely explain to the person first and then talk to the person about what the reason is for having this test. And then the beginning is to understand that, well, if there are elderly people who have Alzheimer's, they will also call with the family and communicate with them first, then, I know what to do next"* (participant#6).	Transparency	

People with different cultural and religious backgrounds have different concepts of privacy (Smith et al., 2011). Cultural and religious factors influence people's attitudes and behaviors when they are involved in using healthcare monitoring devices (Karadag et al., 2019).	● *"Māori communities and their extended families have a different sense of data protection than a western concept"* (participant#1). ● *"For example, New Zealand has to respect Māori culture… we need to obey Māori data protection rights. But we don't bother about Indian or Asian or Chinese data rights at all, although India or China has a universal data policy. Asian differences or any other differences are not that much valued and we only talked about Māori data sovereignty"* (participant#8). ● *"We would get feedback from one of our cultural advisory groups before we go into these projects. We are just making sure that we're not completely missing the issue [since] the device could be linked with some ethical considerations"* (participant#10).	Cultural and religious differences	
Ethical considerations focus on managing ethical concerns. Concerns/considerations may include a loss of personal liberty, an increase in feelings of objectification and loss of control, deception and infantilization, and so on (Sharkey & Sharkey, 2012).	● *"We've got mechanisms around governance…we've got data ethicists… [it is] a real joint effort… on the ethics of data…as part of our program"* (participant#1). ● *"We are interested in the ethical space and we would call this social license, it's not so much what can you [we] do purely legally, but what would people expect you [us] to do and what is kind of good behavior and…trying not to do things that people wouldn't expect or might not be happy with, even if technically you [we] could do them legally"* (participant#2). ● *"Our sticking [monitoring] device could be linked with the usage of tracking devices in prison…but those are ankle bracelets…right? We need to make sure a device…well…it's not a device…it was a way to capture people's vitals by using the camera on users' phones… [therefore] we should be more careful about ethical when we recruited patient volunteers."* (participant#10).	Ethical considerations	Ethical aspect
Equity refers to the absence of avoidable or remediable differences between groups of people (Schaefer & Ballantyne, 2022). Health information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances (The Ministry of Health New Zealand, 2017).	● *"[Equity is] one of four main dimensions together with clinical safety, privacy, and security in terms of data protection scope in the healthcare sector"* (participant#1). ● *"Fairness is often called equity and we need to take into account different people in different situations can be affected in different ways"* (participant#2).	Equity/fairness	
Traceability is defined as the ability to identify and verify the chronology and components of events in all paces of a process (Arbabi et al., 2022). Traceability can either expose interactions between the devices and the associated data owners (e.g., unauthorized used, inappropriately shared, and insecurely processed), or transparently audit the streamed data for potential compromises in a healthcare system (DAMA International, 2009; Lomotey et al., 2017).	● *"They [Traceability] will be able to monitor improper data transfer processes…for example…staff members can be traced and recorded when they download large personal datasets such as excel files from the system to local USB sticks…this [traceability] can avoid or detected unauthorized behaviors and increases data protection ability of the system"* (participant#4). ● *"To be able to use that device within New Zealand, we have to switch off the voice recognition part…but there were questions such as can I be listened or can I be tracked…the nurses would inform their patients that the collected data is completely anonymous and no one will see their data…and we could never link that data back"* (participant#10).	Traceability	Technological

Security is defined as a condition that results from the maintenance and establishment of protective measures that safeguard a state of inviolability from influences or hostile acts (Al Ameen et al., 2012).	● *"Privacy is much more about individual control of identifiable information and security is much more about the mechanisms that you use in relation to the web and IT systems to stop people getting in from the outside or stop people from the inside who shouldn't see information from seeing it"* (participant#2). ● *"In the past, people have asked me for my password at the hospital, that clinic or whatever, and I've always been a bit hesitant…now in order to give my clinicians access…I have to go online and basically share my password with them… I've had to give him my password so he can access my data to be enabled to help me the best way...[However,] the provider should make a better means of password protection"* (participant#3).	Security	
Privacy concerns refer to the degree of an individual's concerns about the possible loss of privacy following voluntary or surreptitious information disclosure to application developers or providers (Trkman et al., 2023). These concerns are associated with uncertainties regarding new technologies, representing an individual's level of anxiety about the electronic transaction of private data (Trkman et al., 2023).	● *"There can be no movement along the journey towards self-empowerment unless they [we] feel confident that their [our] data is going to be protected and respected and they [we] can be confident their [our] data is not going to be used for any reason. I am sure the system means a lot to me because of its ability to offer knowledge further enhanced my confidence. For example, being able to view the daily data [glucose records] provided me with a consistent measure of my health condition, giving me a sense of safety and strength"* (participant#3). ● *"A lot of people know that if their blood saturation goes under a certain number, they are then in control of that they can either switch on their oxygen or they come back into hospital"* (participant#10). ● *"When I don't have as many privacy worries, I feel more sure about managing my health information, making it simpler for me to take charge of my well-being as I've got all my health documents and records that I need in one place"* (participant#15).	Privacy	Privacy concerns
Individual health empowerment in the context of SHMSs, is defined as individuals' perceptions of access to information, support, resources, and opportunities to learn and grow, enabling individuals to optimize their health and obtain a sense of competency, meaningfulness, self-determination, and impact on their lives (Spreitzer, 1995).	● *"Everyone becomes partners and they all contribute stuff of great value that can benefit the individual, but collectively also represent huge value for the community"* (participant#3). ● *"People may feel empowered after using the system as they can feel more in control over their health information"* (participant#10).	Individual health empowerment	Health empowerment
Community empowerment is a group phenomenon that includes a raised level of psychological empowerment among SHMS users, a political action part in which users have dynamically participated, and the achievement of some redistribution of resources or decision making beneficial to the community in question (Rissel, 1994). Israel et al. (1994) mentioned that "an empowered	● *"I think that individual health empowerment will positively affect the community empowerment although individuals are virtually connected in the system. By participating and interacting in the system, users are able to influence service providers and the service quality of the system that must benefit the overall community health status"* (participant#13). ● *"The system can increase our ability to participate in our health data management, in particular it allows us to coordinate with other people including other individuals that is definitely a great opportunity to empower the overall community members including me"* (participant#15).	Community health empowerment	

community has the ability to influence decisions and changes in the larger social system" (p. 5).		
Trust management deals with security policies, credentials, and trust relationships. Trust management has emerged as a promising technology to facilitate collaboration among entities in a digital environment where traditional security paradigms cannot be enforced due to a lack of centralized control and incomplete knowledge of the environment (Yan et al., 2011).	● *"Trust is very fragile but critical and we need to make sure that we've got enough data protection mechanisms in place to maintain that trust. Within the community framework shaped by a monitoring system, trust is often regarded as a relational basis that can influence the overall community health development"* (participant#1). ● *"Overall, trust is an extremely important thing. It can even have a direct impact on the health index of the elderly. For example, if I run to take a patient's temperature, or if you want to enter an elderly person's room, they may be taking a lunch break. However, if you trust each other, the person will not feel disturbed and will not have a privacy concern"* (participant#7). ● *"As these are essential documents that we have to keep for a long time, so the PIAS [Privacy Impact Assessment] and those cloud risk assessments I have to say that I've presented those to that they were approved. I then have to tell so the executive leadership team if those things haven't happened, I won't get approval. So there's lots of trust and cross checks and they trust that the process is happening. If I say it's happening, then they trust that we've got the approval and that we can move forward"* (participant#10). ● *"Everybody has to be able to trust a service system and its new technology before being willing to try it"* (participant#9). ● *"There are lots of trust and cross checks and people live in the community must trust in each other then we can move forward. It would mean that the community has to be trustworthy before we can call it a powerful community"* (participant#10).	Trust

Appendix Table C. 5

Survey respondents' demographic information

Items	Category	Frequency	Ratio
Age	18-24	63	17%
	25-34	97	26%
	35-44	59	16%
	45-54	36	10%
	55-64	13	3%
	Over 65	109	29%
Gender	Female	209	55%
	Male	163	43%
	Others	5	1%
Education	Some school, no degree	3	1%
	High school graduate	44	12%
	Some college, no degree	70	19%
	Bachelor's degree	163	43%
	Master's degree	49	13%
	Professional degree	17	5%
	Doctorate degree	19	5%
	Others	12	3%
Health literacy skills	Not at all	2	1%
	A little bit	16	4%
	Somewhat	53	14%
	Quite a bit	170	45%
	Extremely	136	36%
Income	Less than $30,000	67	18%
	$30,000-$50,000	34	9%
	$50,001-$70,000	48	13%
	$70,001-$100,000	120	32%
	$100,001-$140,000	70	19%
	Over $140,001	21	6%
	Others	17	5%
Traumatic experience	Yes	79	21%
	No	298	79%
Racial/ethnic background	European	251	67%
	Māori	3	1%
	Pacific Peoples	3	1%
	Asian	76	20%
	Latino	7	2%
	Middle Eastern/Latin American/ African	12	3%
	Australian Aboriginal	3	1%
	Others	22	6%

Appendix Table C. 6

Measurement items of constructs

Construct	Adapted items	Original items	Reference
Legislative protection	LEGP1: I think the existing laws in my living country are sufficient to protect my health data privacy.	The existing laws in my country are sufficient to protect consumers' online privacy.	Lwin et al. (2007)
	LEGP2: I think there are stringent international laws to protect my personal information that I share in the SHMS.	There are stringent international laws to protect personal information of individuals on the Internet.	
	LEGP3: I think the government is doing enough to ensure that I am protected against data privacy violations.	The government is doing enough to ensure that consumers are protected against online privacy violations.	
Transparency	TRAN1: I believe the SHMS should allow me to find out my health information that the SHMS keeps in their databases.	Whether health informatics as a service will allow me to find out what information about me they keep in their databases.	Xu (2019)
	TRAN2: I believe the SHMS service providers should tell me how long they will keep information they collect from me.	Whether health informatics as a service tells me how long they will retain information they collect from.	
	TRAN3: I believe the purpose that the SHMS collect my health data should be clear.	The purpose for which health informatics as a service applications want to collect from me.	
Cultural and religious differences	CURE1: I think I would be uncomfortable using the SHMS due to privacy while sharing my health data and interacting with people in the opposite gender who are providing the service to me.	Being uncomfortable due to privacy while giving care to patients in the opposite gender.	Karadag et al. (2019)
	CURE2: I think I may not use the SHMS and share my health data and interact with involved people of service providers in the opposite gender who are providing the service to me.	Not being able to give sufficient physical care to patients in the opposite gender.	
	CURE3: I think I may have difficulty in communicating with others in the systems who cannot speak English.	Having difficulty in meeting patients and their relatives who can't speak Turkish.	
	CURE4: I think I may have difficulty in explaining or understanding while sharing my health data and interacting with other people due to differences in religious belief.	Having difficulty in explaining or understanding while giving care due to difference in religious belief.	
Ethical considerations	ETCO1: I believe that the actions in the SHMS should be always ethical.	Makes sure that his/her actions are always ethical.	De Hoogh and Den Hartog (2008)
	ETCO2: I believe that the SHMS should be earnest.	Means what he/she says, is earnest.	

	ETCO3: I believe that the SHMS deserves trust and can be relied upon. ETCO4: I believe that the SHMS can be trusted to serve my interests (rather than its own benefits). ETCO5: I believe that the SHMS do not pursue own best interest at the expense of me.	Deserves trust, can be believed and relied upon to keep his/her word. Can be trusted to serve the interests of his/her subordinates rather than him/herself. Pursues own best interest at the expense of others (reverse coded). Does not criticize subordinates without good reason.	
Equity/fairness	EQFA1: I believe that what users receive from using the SHMS is fair with regard to the profit smart health service providers of the SHMS receive. EQFA2: I believe that the ratio between what users get out of using the SHMS and the profit the smart health service providers make is fair. EQFA3: I think what the smart health service providers earn with users' using of this device is fair in comparison to what it offers to users. EQFA4: I believe services that the SHMS offers users is commensurate with what they earn with it EQFA5: I believe the profit that the SHMS makes is fair, given the service users receive from the SHMS.	What I receive from using the services of the company is fair with regard to their profit. The ratio between what I get out of using the service provided by the company and the profit the firm makes with me is fair. I think what the company earns with me is fair in comparison to what they offer me. The service the company offers me is commensurate with what they earn with it. The profit the company makes is fair, given the service I receive.	A. Wagner et al. (2021)
Security	SECU1: I think the risk of an unauthorized third party overseeing the SHMS is low. SECU2: I think the risk of abuse of my health information is low when using the SHMS. SECU3: I think the SHMS is secure in conducting my health information management.	The risk of an unauthorized third party overseeing this system is low. The risk of abuse of my health information (e.g. case reports) is low when using this system. I would find this system secure in conducting my health management.	Hsu et al. (2013)
Privacy concerns	PRIV1: I am concerned that the information gathered through the SHMS could be misused. PRIV2: I am concerned that the SHMS service providers (e.g., technology providers) can find my private health information through the system.	I am concerned that the information I submit through the proximity tracing app could be misused. I am concerned that the developers or the proximity tracing application provider can find private information about me through the app.	Trkman et al. (2023)

	PRIV3: I am concerned about my captured information through the SHMS because of what others might do with it.	I am concerned about submitting information through the proximity tracing app because of what others might do with it.	
	PRIV4: I am concerned about my captured information. through the SHMS because it could be used in a way I did not foresee.	I am concerned about submitting information through the proximity tracing app because it could be used in a way I did not foresee.	
Individual health empowerment			
– *Competence of user*	COMP1: I have mastered the skills necessary for using an SHMS.	I have mastered the skills necessary for using the system.	Kim and Gupta (2014)
	COMP2: I am self-assured about my capabilities to use an SHMS	I am self-assured about my capabilities to use the system.	
	COMP3: I am confident about my ability to use an SHMS.	I am confident about my ability to use the system.	
– *Meaning of system usage*	MEAN1: The SHMS that I may use, would be very important to me in relation to my personal health goals.	The system I use is very important to me.	Kim and Gupta (2014)
	MEAN 2: The SHMS that I may use, would be meaningful to me in relation to my personal health goals.	The system I use is meaningful to me.	
	MEAN 3: My SHMS activities would be personally meaningful to me in relation to my personal health goals.	My system activities are personally meaningful to me.	
– *Self-determination of user*	SELD1: I think I would have significant autonomy in determining how I may use the SHMS for setting up my health goals.	I have significant autonomy in determining how I use the system for work.	Kim and Gupta (2014)
	SELD2: I think I would have considerable opportunity for independence and freedom in how I may use SHMS for setting up my health goals.	I have considerable opportunity for independence and freedom in how I use the system for work.	
	SELD3: I think I could decide on my own how to go about using SHMS for setting up my health goals.	I can decide on my own how to go about using the system for work.	
– *Impact of system usage*	IMPA1: I think if I use an SHMS, my impact on what happens to my health status would be large.	Based on system usage, my impact on what happens at work is large.	Kim and Gupta (2014)
	IMPA2: I think if I use an SHMS, I will have significant influence over what happens to my health status	Based on system usage, I have significant influence over what happens at work.	
	IMPA3: I think if I use an SHMS, I will have a great deal of control over what could happen to my health.	Based on system usage, I have a great deal of control over what happens at work.	
Community health empowerment	COME1: I believe the community members should have influence over decisions that affect the community health.	My community has over decisions that affect my life.	Israel et al. (1994)

	COME2: I believe the community members should influence decisions that affect the community's health status. COME3: I believe, by working together, people in the community can influence decisions that affect the community's health status. COME4: I believe people in the community should work together to influence health-related decisions on the state or national level. COME5: Overall, I am satisfied with the amount of influence I have over decisions that affect the community's health status.	I can influence decisions that affect my community. By working together, people in my community can influence decisions that affect the community. People in my community work together to influence decisions on the state or national level. I am satisfied with the amount of influence I have over decisions that affect my community.	
Trust	TRUS1: I believe the SHMS should operate in a highly reliable manner. TRUS2: I believe the SHMS should promote my benefits as well as its own. TRUS3: I believe the SHMS does not engage in any kind of exploitive and damaging behavior to me. TRUS4: I feel confident and assured in using the SHMS.	This e-vendor will operate its business in a highly dependable and reliable manner. This e-vendor will promote customers' benefits as well as its own. This e-vendor will not engage in any kinds of exploitive and damaging behavior to customers. When browsing this site, I feel confident and assured.	Chang and Fang (2013)

Appendix Table C. 7

Procedural and statistical remedies

Techniques	Actions
Procedural remedies (Podsakoff et al., 2003)	
Protecting anonymity of respondents and alleviating evaluation apprehension	Before the participants engaged in the survey, we guaranteed their anonymity. We reassured the participants that there were no correct or incorrect answers and encouraged them to answer the questions truthfully.
Enhancing scale items	We utilized measurement items from existing literature that had been pre-validated and deemed reliable.
Statistical remedies	
Harman's single factor test (Harman, 1976; Podsakoff & Organ, 1986)	To examine the unrotated solution, all measurement items were loaded into an exploratory factor analysis. The analysis revealed forty factors from the dataset with the first factor explaining 24.6% of the variance, and no factor contributed to the majority of the variance. It suggests that CMB is not considered a significant issue for our findings.
Lindell and Whitney's (2001) marker variable test	This test uses a theoretically unrelated construct as a control on dependent variables. In this study, we adopted a fantasy construct from the field of psychology, specifically focusing on respondents' attitude while watching an enjoyable movie. No distinction was observed between the comparative models, one lacking the marker variable and the other incorporating it. Additionally, all the significant paths remained significant, confirming that CMB is not a major issue.

Appendix Table C. 8

HTMT values for discriminant validity

	Community health empowerment	Competence of user	Cultural and religious differences	Equity/fairness	Ethical considerations	Health literacy skill	Impact of system usage	Legislation protection	Meaning of system usage	Privacy concerns	Security	Self-determination of user	Traceability	Transparency
Competence of user	0.192													
Cultural and religious differences	0.081	0.168												
Equity/fairness	0.100	0.096	0.061											
Ethical considerations	0.070	0.169	0.063	0.603										
Health literacy skill	0.183	0.453	0.149	0.059	0.084									
Impact of system usage	0.181	0.325	0.090	0.275	0.240	0.251								
Legislation protection	0.067	0.048	0.048	0.441	0.617	0.043	0.274							
Meaning of system usage	0.264	0.405	0.200	0.241	0.272	0.257	0.567	0.165						
Privacy concerns	0.137	0.142	0.282	0.312	0.402	0.088	0.222	0.416	0.157					
Security	0.126	0.234	0.177	0.567	0.652	0.124	0.288	0.561	0.209	0.583				
Self-determination of user	0.091	0.372	0.128	0.352	0.306	0.206	0.606	0.283	0.448	0.285	0.331			
Traceability	0.142	0.181	0.295	0.255	0.241	0.223	0.286	0.060	0.381	0.099	0.237	0.131		
Transparency	0.112	0.153	0.310	0.093	0.100	0.166	0.054	0.185	0.157	0.204	0.084	0.064	0.498	
Trust in SHMS	0.095	0.311	0.213	0.613	0.695	0.159	0.422	0.573	0.426	0.489	0.705	0.380	0.343	0.051

Appendix D: Ethics Approval Letters

Letter for Qualitative Data Collection (Study 1, Chapter 3)

Auckland University of Technology Ethics Committee (AUTEC)

Auckland University of Technology
D-88, Private Bag 92006, Auckland 1142, NZ
T: +64 9 921 9999 ext. 8316
E: ethics@aut.ac.nz
www.aut.ac.nz/researchethics

13 September 2022

Farkhondeh Hassandoust
Faculty of Business Economics and Law

Dear Farkhondeh

Re Ethics Application: **22/156 An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective**

Thank you for providing evidence as requested, which satisfies the points raised by the Auckland University of Technology Ethics Committee (AUTEC).

Your ethics application has been **approved in stages** for three years until 13 September 2025.

Standard Conditions of Approval

1. The research is to be undertaken in accordance with the Auckland University of Technology Code of Conduct for Research and as approved by AUTEC in this application.
2. A progress report is due annually on the anniversary of the approval date, using the EA2 form.
3. A final report is due at the expiration of the approval period, or, upon completion of project, using the EA3 form.
4. Any amendments to the project must be approved by AUTEC prior to being implemented. Amendments can be requested using the EA2 form.
5. Any serious or unexpected adverse events must be reported to AUTEC Secretariat as a matter of priority.
6. Any unforeseen events that might affect continued ethical acceptability of the project should also be reported to the AUTEC Secretariat as a matter of priority.
7. It is your responsibility to ensure that the spelling and grammar of documents being provided to participants or external organisations is of a high standard and that all the dates on the documents are updated.
8. AUTEC grants ethical approval only. You are responsible for obtaining management approval for access for your research from any institution or organisation at which your research is being conducted and you need to meet all ethical, legal, public health, and locality obligations or requirements for the jurisdictions in which the research is being undertaken.

Please quote the application number and title on all future correspondence related to this project.

For any enquiries please contact ethics@aut.ac.nz. The forms mentioned above are available online through http://www.aut.ac.nz/research/researchethics

(This is a computer-generated letter for which no signature is required)

The AUTEC Secretariat
Auckland University of Technology Ethics Committee

Cc: jingjing.zhang@autuni.ac.nz; angsana@aut.ac.nz

Letter for the Amendment to Extend Recruitment of Interview Participants in Australia (Study 1, Chapter 3)

Auckland University of Technology Ethics Committee (AUTEC)

2 February 2023

Farkhondeh Hassandoust
Faculty of Business Economics and Law

Dear Farkhondeh

Re: Ethics Application: **22/156 An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective**

Thank you for your responses to the conditions for the amendments to your ethics application.

The amendment to extend recruitment of participants in Australia is approved.

Non-Standard Conditions of Approval

1. Please increase length of time to follow up invitation from 1 to 2 weeks.
2. Please insert AUTEC approval number on the advertisement.
3. Please provide AUTEC with a signed copy of the data sharing agreement (this is for the overseas based supervisors not the Australian participants).

Non-standard conditions do not need to be reviewed by AUTEC unless requested but must be completed before commencing your study. Please send through any requested documents for file.

Standard Conditions of Approval

1. The research is to be undertaken in accordance with the Auckland University of Technology Code of Conduct for Research and as approved by AUTEC.
2. All public facing documents must have the AUTEC approval number and be of a high standard of spelling and grammar. Dates on the Information Sheet(s) and Consent Form(s) must be consistent.
3. Any amendments to the project must be approved by AUTEC prior to being implemented.
4. A progress report is due annually on the anniversary of the approval date.
5. A final report is due at the expiration of the approval period, or, upon completion of project.
6. Any serious or adverse events must be reported to AUTEC, this includes unforeseen issues that might affect continued ethical acceptability of the project.
7. AUTEC grants ethical approval only. You are responsible for obtaining management permission for access from any institution or organisation at which your research is being conducted and you need to meet all ethical, legal, public health, and locality obligations or requirements for the jurisdictions in which the research is being undertaken.

The application number and title need to be referenced on all correspondence related to this project.

All forms are available online http://www.aut.ac.nz/research/researchethics

For any enquiries, please contact ethics@aut.ac.nz

(This is a computer-generated letter for which no signature is required)

The AUTEC Secretariat
Auckland University of Technology Ethics Committee

Cc: jingjing.zhang@autuni.ac.nz; ajohnston@cba.ua.edu; harminder.singh@aut.ac.nz

Auckland University of Technology, D-88, Private Bag 92006, Auckland 1142, New Zealand
T: +64 9 921 9999 ext. 8316: E: ethics@aut.ac.nz: www.aut.ac.nz/researchethics

Letter for Quantitative Data Collection (Study 2, Chapter 3)

Auckland University of Technology Ethics Committee
(AUTEC)

14 September 2023

Farkhondeh Hassandoust
Faculty of Business Economics and Law

Dear Farkhondeh

Re Ethics Application: **22/156 An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective**

Thank you for your responses to the conditions for the amendment to your ethics application.

An online survey to complete the second stage of the research has been approved.

Non-Standard Conditions of Approval

1. Removal of the repetition of the contact details of the Executive Secretary from the information sheet and Kate O'Connor's name. Please refer to the current Information Sheet exemplar on the website.

Non-standard conditions do not need to be submitted to or reviewed by AUTEC unless requested but must be completed before commencing your study.

Standard Conditions of Approval

1. The research is to be undertaken in accordance with the Auckland University of Technology Code of Conduct for Research and as approved by AUTEC.
2. All public facing documents must have the AUTEC approval number and be of a high standard of spelling and grammar. Dates on the Information Sheet(s) and Consent Form(s) must be consistent.
3. Any amendments to the project must be approved by AUTEC prior to being implemented.
4. A progress report is due annually on the anniversary of the approval date.
5. A final report is due at the expiration of the approval period, or, upon completion of project.
6. Any serious or adverse events must be reported to AUTEC, this includes unforeseen issues that might affect continued ethical acceptability of the project.
7. AUTEC grants ethical approval only. You are responsible for obtaining management permission for access from any institution or organisation at which your research is being conducted and you need to meet all ethical, legal, public health, and locality obligations or requirements for the jurisdictions in which the research is being undertaken.

The application number and title need to be referenced on all correspondence related to this project.

All forms are available online http://www.aut.ac.nz/research/researchethics

For any enquiries, please contact ethics@aut.ac.nz

(This is a computer-generated letter for which no signature is required)

The AUTEC Secretariat
Auckland University of Technology Ethics Committee

Cc: jingjing.zhang@autuni.ac.nz; ajohnston@cba.ua.edu; harminder.singh@aut.ac.nz

Appendix E: Participant Information Sheet

Qualitative Stage (Study 1, Chapter 3)

Participant Information Sheet

This Information Sheet is prepared for the participants from individual volunteer users.

Date Information Sheet Produced:

9 March 2023

Project Title

An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective

An Invitation

Tena koe! Greetings. I am Jingjing Zhang, a PhD student in the department of Business Information Systems at Auckland University of Technology (AUT). To complete my PhD research in the above project title, I would like to invite you to participate in an interview and share your opinions from the individual user perspective. You would be asked about, for example, your experience with your health data privacy protection and the usage of a smart health monitoring device and service. The interview will take around 60 minutes, face-to-face or via a video conferencing platform, such as Zoom or Microsoft Teams, on a date and time most convenient to you in the following weeks.

Your participation in this research is voluntary (it is your choice), and whether or not you choose to participate will neither advantage nor disadvantage you. Moreover, please be assured that you will not be identified in any way. This project is under the supervision of Dr Farkhondeh (Ferry) Hassandoust from AUT (New Zealand) and Professor Allen Johnston from the University of Alabama (United States).

What is the purpose of this research?

This research is in two stages. In the first stage or current stage, the research aims to investigate how data governance mechanisms have been developed by stakeholders (e.g., government authorities, decision-makers or managers from smart technology providers, healthcare providers, and individual users) toward managing surveillance and privacy concerns. In the second stage, the research aims to investigate the effects of the implemented data governance mechanisms on individuals' use of smart health monitoring devices and services, understanding individuals' experiences and perceptions of their surveillance and privacy concerns.

Individual users are defined as part of key stakeholders in this research. In the current stage (Stage 1). As an individual stakeholder representative, you are invited to participate in an interview. Please be aware that I will conduct other interviews with participants from different stakeholder groups. The outputs of this research will be a thesis and academic publications.

How was I identified and why am I being invited to participate in this research?

You have been identified from one of the following channels: 1) Some potential participants are asked to pass on the details about the study to you, and you decide to contact me. Therefore, your contact details have been identified to me. 2) You have responded to one of the social media advertisements.

Because you are identified as an individual user who is using or has the potential to use a specific smart health monitoring device, you may have some perceptions and opinions when you communicate with other stakeholders (such as healthcare providers, smart technology providers, and government authorities) and share your health data with them through the device. Your perceptions and opinions will be valuable in investigating how data governance is developed to manage surveillance and privacy concerns in a smart health monitoring system.

How do I agree to participate in this research?

To agree to participate in this research, you can complete a Consent Form, which is attached to this document. You can consent by emailing the signed Consent Form to me at jingjing.zhang@autuni.ac.nz. The Consent Form will also be handed to you before the interview when the interview is arranged offline and you wish to complete it face-to-face.

Your participation in this research is voluntary (it is your choice), and whether or not you choose to participate will neither advantage nor disadvantage you. You can withdraw from the study at any time. If you decide to withdraw from the study, you will be offered the choice between having any data identifiable as belonging to you removed or allowing it to continue to be used. However, removing your data may not be possible once the findings have been produced.

What will happen in this research?

The interview will take around 60 minutes via a video conferencing platform, such as Zoom or Microsoft Teams. The location for a face-to-face interview can be arranged in the researcher's office at AUT or other public areas (e.g., cafés).

Before the interview, we will ask for your consent to participate in this study and to audio-record the conversation; it is your choice to agree or not agree to the recording. The recordings will be transcribed into a written document and shared with my supervisors. The involved researchers (my supervisors and me) will use the transcribed data for this research, and the data will be kept securely, not allowing third parties to access them.

During the interview, you will be asked about your experiences related to the data governance field, particularly surveillance and privacy protection concerns that may be risks when you share your health data through your smart health monitoring device. Your answers will be recorded, collected, and analysed in this research.

What are the discomforts and risks?

I do not anticipate any discomforts or risks with your participation in this study. You can refuse to answer some questions if you regard them as intrusive or are unwilling to answer them. You can choose to withdraw from this study at any time.

How will these discomforts and risks be alleviated?

You can ask me to stop the interview if you feel discomfort or risk. Your participation in this study is voluntary. If you choose not to continue participating in this study, your decision will not disadvantage you in any way.

What are the benefits?

The benefit of this research is that the student researcher obtains a doctoral degree.

Moreover, this research will allow participants to reflect on their data governance mechanisms and use the findings to discuss how to better collaborate with other stakeholders to develop effective data governance mechanisms that can better manage user personal and healthcare data in a smart health monitoring context.

How will my privacy be protected?

Your personal data, like your name and your background, will be protected and managed by the de-identification procedure (i.e., pseudonymisation). It means I will not use identifiable information about you. Instead, any identifiable information will be coded using numbers in the data analysis process, in disseminating findings, and in the resulting publications. For instance, if we quote your comments directly, the quote will only be attributed to a pseudonym title, such as Participant 1, not to you personally.

Confidentiality might be affected if you choose to be interviewed on the premises of your organisation. If you have any questions during the interview, please ask anytime.

Your contact details are stored on the hard drives of the researcher's computer only for the purpose of feeding back the insights of this research. Data will be stored securely for six years and then will be deleted.

What are the costs of participating in this research?

There is almost no cost to participate in this research other than approximately 60 minutes of your time, which is much appreciated. Your Internet access available during the interview may be considered a monetary cost when the interview is arranged online, as you suggest.

What opportunity do I have to consider this invitation?

Please respond to this invitation within four weeks so I can schedule an interview at a date and time of your convenience. The interview can occur at AUT or other public locations such as a café or other indoor public facilities. If needed, an online interview can be arranged via a video conferencing platform such as Zoom or Microsoft Teams.

Will I receive feedback on the results of this research?

If you would like to receive a summary of the research findings, please make sure you tick the appropriate box in the Consent Form and provide your contact details, and we will be happy to share a one or two-page summary of the findings with you.

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor, Dr Farkhondeh (Ferry) Hassandoust, ferry@aut.ac.nz, (+649) 921 9999 ext. 5419.

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTEC, ethics@aut.ac.nz, (+649) 921 9999 ext. 6038.

Whom do I contact for further information about this research?

Please keep this Participant Information Sheet and a copy of the Consent Form for your future reference. You are also able to contact the research team as follows:

Researcher Contact Details:

Jingjing Zhang

jingjing.zhang@autuni.ac.nz | (+649) 921 9999 ext. 26995

Project Supervisor Contact Details:

Dr Farkhondeh (Ferry) Hassandoust

ferry@aut.ac.nz | (+649) 921 9999 ext. 5419

Approved by the Auckland University of Technology Ethics Committee on *2 February 2023*, AUTEC Reference number *22/156*.

Quantitative Stage (Study 2 in Chapter 3)

Participant Information Sheet

Date Information Sheet Produced:

XX September 2023

Project Title

An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective

An Invitation

Greetings. I am Jingjing Zhang, a PhD student in Business Information Systems at Auckland University of Technology (AUT), New Zealand. To complete my PhD research in the above project title, I invite you to participate in a survey and share your ideas and experiences about the use of smart health monitoring devices (or services), your concerns about surveillance and privacy (if any), and data governance mechanisms implemented by service providers to address you concerns. You can withdraw from the survey by closing the browser. However, please be informed that once data is submitted it is unable to be withdrawn as it is anonymous. Please be informed that whether you choose to participate will neither advantage nor disadvantage you.

What is the purpose of this research?

The research aims to investigate the effects of the implemented data governance mechanisms on individuals' perceptions of surveillance and privacy concerns and their effects on the use of smart health monitoring devices (or services). The outputs of this research will be a thesis and academic publications.

How was I identified and why am I being invited to participate in this research?

You have been invited to participate in this research through a third-party panel data service, Prolific. Your input will be invaluable in helping to understand the effects of the data governance mechanisms on customer perceptions of surveillance and privacy concerns and their effects on the use of smart health monitoring devices (or services).

How do I agree to participate in this research?

By completing this web survey, you are indicating your consent to participate in the research.

Your participation in this research is voluntary (it is your choice), and whether or not you choose to participate will neither advantage nor disadvantage you. You can withdraw from the survey by closing the browser. However, please be informed that once data is submitted it is unable to be withdrawn as it is anonymous.

What will happen in this research?

You will be given a survey link. The survey will ask demographic questions such as your age and education. You will also be asked about your concerns associated with surveillance and privacy in the context of smart health monitoring systems, your perceptions of the data governance mechanisms implemented for surveillance and privacy protection, your perceived benefits of data sharing in the context, and your willingness to use smart health monitoring devices (services). You can email the primary researcher and request a copy of the collated results.

What are the discomforts and risks?

There will not be any discomfort or risk, as the level that the participants may experience discomfort or embarrassment will be minimal. Your participation is anonymous and voluntary.

How will these discomforts and risks be alleviated?

We will not share your information and survey responses with anyone outside this research team.

What are the benefits?

The benefit of this research is that the student researcher obtains a doctoral degree.

Moreover, this research will allow participants to reflect on the important data governance mechanisms for managing surveillance and privacy concerns and use the findings to promote better data governance mechanisms that benefit individual users and other stakeholders in smart health monitoring systems.

How will my privacy be protected?

The survey is anonymous. No party other than us will have access to the data. All data will be securely destroyed after a period of six years.

What are the costs of participating in this research?

There are no costs to you for participating in this study except for approximately 10-15 minutes of your time answering survey questions, which is much appreciated.

What opportunity do I have to consider this invitation?

You will have two weeks to fill in the web survey since you have received a link to the survey.

Will I receive feedback on the results of this research?

Yes. You are welcome to email Jingjing Zhang (jingjing.zhang@autuni.ac.nz) if you wish to receive a summary of the research findings.

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor, Farkhondeh (Ferry) Hassandoust, ferry@aut.ac.nz. (+649) 921 9999 ext. 5419.

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTEC, *ethics@aut.ac.nz*, (+649) 921 9999 ext. 6038.

Whom do I contact for further information about this research?

Please keep this Information Sheet for your future reference. You are also able to contact the research team as follows:

Researcher Contact Details:

Jingjing Zhang, jingjing.zhang@autuni.ac.nz

Farkhondeh (Ferry) Hassandoust, ferry@aut.ac.nz,

Allen C. Johnston, acjohnston5@ua.edu

Project Supervisor Contact Details:

Dr Farkhondeh Hassandoust

ferry@aut.ac.nz | (+649) 921 9999 ext. 5419

Approved by the Auckland University of Technology Ethics Committee on *14 September 2024*, AUTEC Reference number *22/156*.

Appendix F: Consent Form

Consent Form for the Qualitative Data Collection (Study 1, Chapter 3)

Consent Form

Project title:	***An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective***
Project supervisor:	***Dr Farkhondeh Hassandoust, Professor Allen Johnston***
Researcher:	***Jingjing Zhang***

- ○ I have read and understood the information provided about this research project in the Information Sheet dated 9 March 2023.
- ○ I have had an opportunity to ask questions and to have them answered.
- ○ I understand that notes will be taken during the interviews and that they will also be audio-taped and transcribed.
- ○ I understand that taking part in this study is voluntary (my choice) and that I may withdraw from the study at any time without being disadvantaged in any way.
- ○ I understand that if I withdraw from the study then I will be offered the choice between having any data that is identifiable as belonging to me removed or allowing it to continue to be used. However, once the findings have been produced, removal of my data may not be possible.
- ○ I agree to take part in this research.
- ○ I wish to receive a summary of the research findings (please tick one): Yes○ No○

Participant's signature: .....

Participant's name: .....

Participant's Contact Details (if appropriate):

.....

.....

.....

.....

Date:

Approved by the Auckland University of Technology Ethics Committee on 2 February 2023 AUTEC Reference number 22/156

Note: The Participant should retain a copy of this form.

Oral Consent Protocol

For use when interviews are being conducted by videoconference.

Project title:	***An investigation of surveillance and privacy-protective data governance and their impacts on smart health monitoring systems use: A collaborative stakeholder perspective***
Project Supervisor:	***Dr Farkhondeh Hassandoust, Professor Allen Johnston***
Researcher:	***Jingjing Zhang***

The participant joins the videoconference

- ○ Do you agree to my recording your consent to participate?

If they agree, then the record function will be activated and they will be asked the following:

- ○ Have you read and understood the information provided about this research project in the Information Sheet dated 9 March 2023?
- ○ Do you have any questions about the research?
- ○ Do you understand that notes will be taken during the interviews and that the interview will also be audio-recorded and transcribed?
- ○ Do you understand that taking part in this study is voluntary (your choice) and that you may withdraw from the study at any time without being disadvantaged in any way?
- ○ Do you understand that if you withdraw from the study then you will be offered the choice between having any data that is identifiable as belonging to you removed or allowing it to continue to be used? However, once the findings have been produced, removal of your data may not be possible.
- ○ Do you agree to take part in this research?
- ○ Do you wish to receive a summary of the research findings? (please tick one): Yes○ No○
- ○ Do you want me to send you a copy of the audio recording for this consent? Yes○ No○
- ○ Please confirm you name and contact details

Participant's name: .....

Participant's Contact Details (if appropriate):

.....

.....

.....

.....

I will now turn off the recording of the Consent and then will start a separate recording for the interview.

Approved by the Auckland University of Technology Ethics Committee on 2 February 2023, AUTEC Reference number 22/156.

Note: The Participant should retain a copy of this form.

Appendix G: Interview Questions (Study 1, Chapter 3)

Student researcher	Jingjing Zhang
Project supervisor	Dr Farkhondeh (Ferry) Hassandoust, Professor Allen C. Johnston
Participants	Volunteer individual users

Warm-up questions

1. Are you familiar with any smart healthcare monitoring devices[4]? Where did you hear about it?
2. Do you use it? If so, how often? And for how long have you used it?
3. What motivated you the most to use it?
4. You may not yet use the smart health monitoring system, but I learned that you are interested in using it in the future. Could you talk about your idea of such kinds of devices or services? Such as any advantages and disadvantages of using it.

Research-focused questions

Part 1: privacy and surveillance concerns

We have discussed that the smart health monitoring system (or the XXX system) can record your health-related data and share the data with other parties (such as your doctors, nurses, and the device provider who produced this device) when necessary for better healthcare management. For example, Freestyle Libre is a continuous glucose monitoring system with a sensor and mobile app. You can stick the sensor to your skin (on the back of the upper arm), and the system will be able to record your blood glucose readings and monitor your glucose trends for you. Through this sensor-based system, your glucose information can also be shared with others, such as your doctor or the provider of the Freestyle Libre product.

5. When you recognise that the device is going to monitoring your health information, will you have some potential concerns about data protection? For example, you think you are a bit difficult to share your health data with service parties through the system? Could you explain
    a. Whom did you worry about? For example, it could be your healthcare provider (e.g., doctor, nurse) who can access your health data through the device, or the device provider (the company who produced this device) if you think they may use some method you are uncertain about to visit your data remotely without your permission.
    b. Is anyone else you worried about?
    c. What kind of activities by those stakeholders will make you worry about your data privacy/protection? Are there any specific behaviors that you dislike regarding the privacy aspect?
6. How important is your health data protection/privacy to you? Do you realise the availability of information privacy policies that can protect your privacy? Is it important if you are required to read and accept (or reject) those policies before you can use it?
7. Besides privacy concerns, do you have other concerns or undesired feelings when you know that device could probably monitor your health information? For example, you might be concerned that someone behind the system could learn when you eat or sleep since your glucose information or heart working condition can be shared with others through the device. (This question is related to surveillance concerns.)

Part 2: Antecedent factors impacting individuals' privacy concerns with SHMSs

[4] During the interview, XXX will be replaced with a specific smart health monitoring device or service. For example, the FreeStyle Libre Flash, Dexcom G6 glucose monitoring system, or KardiaMobile Personal EKG Monitor etc., that can be found in the local market.

8. If you had data privacy or related concerns when being monitored by a device, how do you consider addressing those concerns?
9. What do you think of the importance of "responsibility" in the reporting structure of data governance? For example, the "responsibility" allows the system to tell the truth about how they collect and use your health information.
10. What do you think of the importance of the "decision-making authority" in the reporting structure of data governance? For example, the "decision-making authority" allows the system to improve the process and better protect your health data.
11. Several aspects of health data protection are involved when a smart health monitoring system collects and manages your health data. For example: security, confidentiality, fairness, efficiency, accuracy, transparency, reliability, effectiveness, traceability, ethnicity (ethical consideration), legality (legislative protection), appropriateness etc. In your opinion, what are the main important factors (characters) (mentioned above) to manage your surveillance- and privacy-related concerns caused by the monitoring device? Why? Why are these factors important to you?
12. How familiar are you with the following acts?
    a. Privacy Act 2020[5]
    b. Search and S Surveillance Act 2012[6]
    c. Others (for example, Health Information Privacy Code 2003, Health Practitioners Competence Assurance Act 2003, Health and Disability Commissioner Act 1994, Good Medical Practice, etc.)
13. Data privacy protection unavoidably involves a larger group of stakeholders due to the resource-independent, context-dependent, and organizational-boundary-crossing nature of the information. To improve stakeholders' collaboration for better data governance in terms of privacy and relative management, several three aspects are often involved into discussion: communication, training and the coordination of decision making among stakeholders.
14. What do you think of the term collaboration?
15. What do you think of the impact of stakeholders' collaboration on your health data protection in terms of communication, training, and coordination? For example, how do you value the communication among different stakeholders such as doctors, government, smart technology providers of this device, and representatives from individual users (e.g., you) that could help to manage and address privacy and surveillance-related issues in terms of customers' health data protection?
16. You are welcome to share more if you recognise other critical points or aspects regarding the rational governance mechanisms, which should be considered to address data protection concerns.

Part 3: Privacy and health empowerment

Individual Health empowerment is defined as individuals' perceptions of access to information, support, resources, and opportunities to learn and grow, enabling individuals to optimize their health and obtain a sense of competency, meaningfulness, self-determination, and impact on their lives.

Community Health Empowerment is a group phenomenon that includes a raised level of psychological empowerment among SHMS users, a political action part in which users have dynamically participated,

[5] New Zealand's Privacy Act 2020 is a framework in New Zealand that protect an individual's right to privacy of personal information, including the right of an individual to access their personal information.
Please visit https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23223 for more information.

[6] New Zealand's Search and Surveillance Act 2012 facilitates the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values.
Please visit https://www.legislation.govt.nz/act/public/2012/0024/latest/whole.html for more information.

and the achievement of some redistribution of resources or decision making beneficial to the community in question. An empowered community has the ability to influence decisions and changes in the larger social system.

17. Can you describe any concerns you have regarding using Smart Health Monitoring Systems (SHMS)?
18. How do you balance the need for your concerns (e.g., privacy concerns) with the potential health benefits provided by SHMS? Let's assume A as a confident and proficient user of SHMS, what do you think about how A could contribute to improving the health and well-being of their community? (In our study, we term this phenomenon Community Health Empowerment.)
19. Does your perspective differ when comparing A's age, specifically whether they are under 65 or over 65 years old?
20. What do you think of the importance of a high level of trust among various stakeholders of the system?

Last question: What do you think of the future of smart health devices? To what extent do privacy concerns deter individuals from using these devices to improve (empower) their health and community health promotion?

-End-

Appendix H: Online Questionnaire (Study 2, Chapter 3)

A survey about using smart health monitoring systems

In this study, we are seeking participants aged 18 and above who have an understanding of what a smart health monitoring system (SHMS) is after viewing the given introduction at the beginning of this survey.

The participants will be asked about their ideas and experiences about smart health monitoring systems and devices, thoughts or concerns about monitoring technology, health data protection, and health data management activities implemented by service providers to provide better customer service.
<<Participant Information Sheet>> (See Appendix E)

Please provide information about your background below.

Filtering question: Age: What is your age? (End of Survey if Below 18 is Selected)
1) Below 18
2) 18-24
3) 25–34
4) 35–44
5) 45–54
6) 55–64
7) Over 65

Please provide information about your background below.

Gender: What is your gender?
1) Female
2) Male
3) Gender variant/Non-conforming
4) Prefer not to say

Education: What is the highest degree or level of school you have completed?
1) Some school, no degree
2) High school graduate
3) Some college, no degree
4) Bachelor's degree
5) Master's degree
6) Professional degree
7) Doctorate degree
8) Other: Please specify_____
9) Prefer not to say

Health literacy skills: How confident are you filling out medical forms by yourself?
1) Not at all 2) A little bit 3) Somewhat 4) Quite a bit 5) Extremely

Traumatic experience: Did you experience a traumatic event? (e.g., lose a parent(s) during your childhood)?
1) Yes
2) No

Income: Which income level describes you? In either Australian dollars (AUS), New Zealand dollars (NZ), or United States dollars (US)
1) Less than $30,000
2) $30,000-$50,000
3) $50,001-$70,000
4) $70,001-$100,000
5) $100,001-$140,000
6) Over $140,001
7) Unknown

8) Refused to answer

Cultural background: What racial or ethnic groups describe you?

1) European
2) Māori
3) Pacific Peoples
4) Asian
5) Latino
6) Middle Eastern/Latin American/ African
7) Australian Aboriginal
8) Native Hawaiian/Other pacific islander
9) Other ethnicity. Please specify_____

Please read the following scenario very carefully.

Smart health monitoring systems (SHMS) are intelligent surveillance systems that employ smart health monitoring devices to monitor changes in the vital signs of individual customers. In the system, the monitoring devices are used to collect health information from customers. Meanwhile, multiple smart health service providers, such as healthcare providers (e.g., clinics, hospitals), smart technology providers, government authorities, and so on, who are connected with the SHMS use the collected health information to deliver services to customers.

Here is a video about a glucose-monitoring wearable device. It would be a good example for you to understand better how a smart health monitoring device interacts with customers and relevant healthcare providers to offer services to customers. In the video, the sensor of the glucose monitoring device is linked to an iPhone or Android-based app. It can measure customers' glucose every minute. By wearing the device, customers can scan and share their readings at any time from anywhere. These readings provide customers and their healthcare providers with valuable information. Sharing glucose readings with healthcare providers allows for easier and more productive conversations about customers' diabetes management. Healthcare providers can access to the SHMS which is secure and cloud-based. By doing this, healthcare providers can review the glucose readings of customers and provide treatment support in person or remotely. It means that healthcare providers can quickly help customers identify patterns and trends in glucose levels and discuss possible changes to a diabetes management plan for customers. You can click the video for more details about this example.

Filtering question: Based on the introduction above, I have an understanding of what is a smart health monitoring system (SHMS). **(End of Survey if No is Selected)**

1) Yes
2) No

Do you believe you are presently using a smart health monitoring device (similar to the given example shown in the video)?

1) Yes. Please identify
2) No
3) Maybe in the near future

Please pay attention to the below points:

Please note that "**SHMS**" refers to **Smart Health Monitoring Systems**.

Smart health monitoring systems (SHMS) are intelligent surveillance systems that employ smart health monitoring devices, to monitor the changes in the vital signs of individual customers. In the system, the monitoring devices are used to collect health information from customers. Meanwhile, multiple smart health service providers, such as healthcare providers (e.g., clinics, doctors, hospitals), smart technology

providers, government authorities, and so on, who are connected with the SHMS use the collected health information to deliver services to patients/customers.

If you are not currently using a Smart Health Monitoring Service (SHMS), **please <u>assume using a SHMS</u>**, sharing your health information with service providers (e.g., your doctor, nurses) in the system, while answering the following questions.

You may come across <u>similar questions</u> in the next sections. We need to include similar questions to establish statistical reliability and validity.

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Legislative protection**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I think, the existing laws in my living country are sufficient to protect my health data privacy. ● I think, there are stringent international laws to protect my personal information that I share in the SHMS. ● I think the government is doing enough to ensure that I am protected against data privacy violations.					

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Transparency**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I believe the SHMS should allow me to find out my health information that the SHMS keeps in their databases. ● I believe the SHMS service providers should tell me how long they will keep information they collect from me. ● I believe the purpose that the SHMS collect my health data should be clear.					

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Cultural and religious differences**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I think I would be uncomfortable using the SHMS due to privacy while sharing my health data and interacting with people in the opposite gender who are providing the service to me. ● I think I may not use the SHMS and share my health data and interact with involved people of service providers in the opposite gender who are providing the service to me. ● I think I may have difficulty in communicating with others in the systems who cannot speak English. ● I think I may have difficulty in explaining or understanding while sharing my health data and interacting with other people due to differences in religious belief.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Ethical consideration**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I believe that the actions in the SHMS should be always ethical. ● I believe that the SHMS should be earnest. ● I believe that the SHMS deserves trust, and can be relied upon. ● I believe that the SHMS can be trusted to serve my interests (rather than its own benefits). ● I believe that the SHMS do not pursue own best interest at the expense of me.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Equity/fairness**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I believe that what users receive from using the SHMS is fair with regard to the profit smart health service providers of the SHMS receive.					

● I believe that the ratio between what users get out of using the SHMS and the profit the smart health service providers make is fair. ● I think what the smart health service providers earn with users' using of this device is fair in comparison to what it offers to users. ● I believe services that the SHMS offers users is commensurate with what they earn with it. ● I believe the profit that the SHMS makes is fair, given the service users receive from the SHMS.

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Traceability**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I expect the SHMS to help me carefully trace and evaluate my health condition (e.g., blood glucose). ● I expect traceability of the SHMS gives me quick and easy access to large and integrated volumes of information I need. ● I expect traceable information the SHMS provides is trustworthy.					

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Security**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I think the risk of an unauthorised third party overseeing the SHMS is low. ● I think the risk of abuse of my health information is low when using the SHMS. ● I think the SHMS is secure in conducting my health information management.					

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Privacy concerns**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I am concerned that the information gathered through the SHMS could be misused. ● I am concerned that the SHMS service providers (e.g., technology providers) can find my private health information through the system. ● I am concerned about my captured information through the SHMS because of what others might do with it. ● I am concerned about my captured information through the SHMS because it could be used in a way I did not foresee.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Individual health empowerment – Competence of user (sub-dimension)**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I have mastered the skills necessary for using a SHMS. ● I am self-assured about my capabilities to use a SHMS. ● I am confident about my ability to use a SHMS.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Individual health empowerment – Meaning of system usage (sub-dimension)**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● The SHMS that I may use, would be very important to me in relation to my personal health goals. ● The SHMS that I may use, would be meaningful to me in relation to my personal health goals. ● My SHMS activities would be personally meaningful to me in relation to my personal health goals.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Individual health empowerment – Self-determination of user (sub-dimension)**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I think I would have significant autonomy in determining how I may use the SHMS for setting up my health goals. ● I think I would have considerable opportunity for independence and freedom in how I may use SHMS for setting up my health goals. ● I think I could decide on my own how to go about using SHMS for setting up my health goals.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Individual health empowerment – Impact of system usage (sub-dimension)**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I think if I use a SHMS, my impact on what happens to my health status would be large. ● I think if I use a SHMS, I would have significant influence over what happens to my health status. ● I think if I use a SHMS, I would have a great deal of control over what could happen to my health.					

How much do you agree with each of the following statements? “SHMS” refers to Smart Health Monitoring Systems.

Construct: **Community empowerment**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I believe the community members should have influence over decisions that affect the community health. ● I believe the community members should influence decisions that affect the community’s health status. ● I believe, by working together, people in the community can influence decisions that affect the community’s health status.					

● I believe people in the community should work together to influence health-related decisions on the state or national level. ● Overall, I am satisfied with the amount of influence I have over decisions that affect the community's health status.

How much do you agree with each of the following statements? "SHMS" refers to Smart Health Monitoring Systems.

Construct: **Trust**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● I believe the SHMS should operate in a highly reliable manner.					
● I believe the SHMS should promote my benefits as well as its own.					
● I believe the SHMS does not engage in any kind of exploitive and damaging behavior to me.					
● I feel confident and assured in using the SHMS.					

Attention Check 1:

Please read the follow text attentively, as it pertains to an Attention Check. The colour test you are about to take part in is very simple, when asking for your favourite colour you must select 'Brown'. This is an Attention Check.

Based on the text you read above, what colour have you been asked to enter? 1) Blue 2) Green 3) Orange 4) Brown

Attention Check 2:

How much do you agree or disagree with the following statement? Please indicate your agreement with the statement below. This is an Attention Check.

I swim across the Pacific Ocean to get to work every morning. 1) Strongly disagree 2) Disagree 3) Neither agree nor disagree 4) Agree 5) Strongly agree

Marker Variable:

Please be patient and assist us by answering the following set of questions. They refer to your feelings when watching a good movie. Please answer these questions based on your 'gut' feeling. The exact answer is not important to us – but it is required for statistical calibration of the earlier questions.

How much do you agree or disagree with each of the following statements about your feelings when you watch a good movie?

Construct: **Fantasy**	1 - Strongly disagree	2 - Disagree	3 - Neither agree nor disagree	4 - Agree	5 - Strongly agree
● When I am watching an interesting movie, I imagine how I would feel if the events in the movie were happening to me.					
● I really get involved with the feelings of the characters in a movie.					
● I am usually objective when I watch a movie or play, and I don't often get completely caught up in it.					
After seeing a play or movie, I have felt as though I were one of the characters.					
● I daydream and fantasise, with some regularity, about things that might happen to me.					
● Becoming extremely involved in a good movie is somewhat rare for me.					
● When I watch a good movie, I can very easily put myself in the place of a leading character.					

Thank You for Completing Our Survey!

To submit this survey, click the 'Next' button on the bottom right side of your screen.

Your response has been recorded while you click the 'Next' button.

We thank you for your time spent taking this survey.

-End-