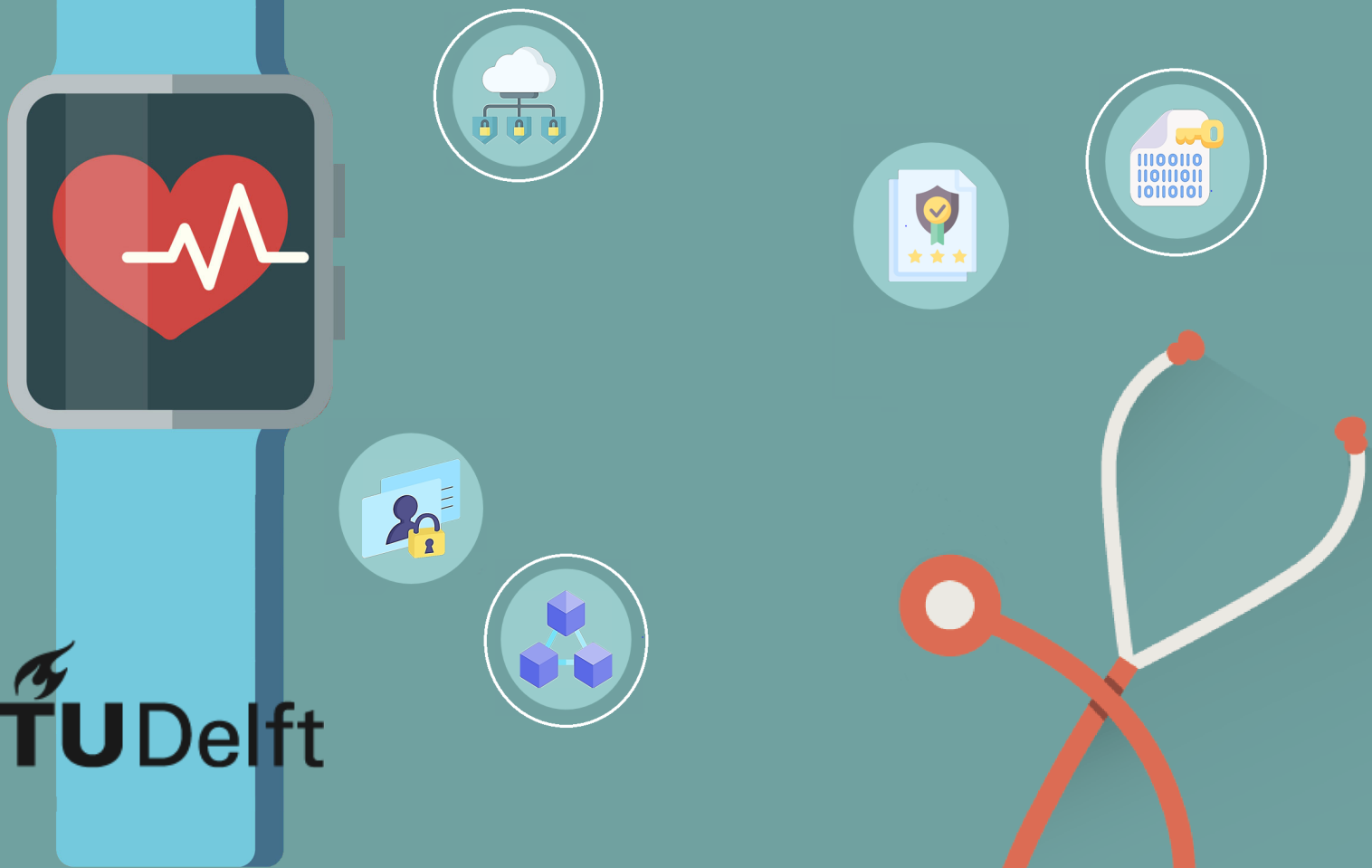
Enhancing the Cybersecurity and Privacy of Medical Wearables

A User-Centred Approach

P S



TU Delft

Enhancing the Cybersecurity and Privacy of Medical Wearables: A User-Centred Approach

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

P S

Student number: 5408601

To be defended in public on December 15th 2023

Graduation Committee

First Supervisor & Chair:	Dr. A.M.G. Zuiderwijk-van Eijk, Information & Communication Technology
Second Supervisor:	Dr. S. Hinrichs-Krapels, Policy Analysis
Advisor:	Dr. C.A. Figueroa, Information & Communication Technology

Acknowledgements

This thesis is my final graduation project for the Management of Technology Master's program at the Delft University of Technology. I pursued this master's degree in an attempt to combine my experience in applied physics with a broader interest in management. I was especially interested in analysing opportunities for technological innovation in dynamic and interactive environments. A specialisation track in cybersecurity further sparked my interest. Writing this thesis on human-centric cybersecurity, considering users' needs and limitations in managerial-level system design, has proven to be a challenging but appropriate fit for me.

The thesis would not have been what it is today if it was not for the involvement of several people. First, I would like to express my deepest gratitude to the members of my graduation committee. Their support and guidance in the formation of this thesis greatly improved the quality of the thesis. I want to thank Dr. Caroline Figueroa, for allowing me to work under her guidance. Her constructive feedback and engagement with the thesis helped me to think critically about choices that presented themselves during the process. Our meetings helped me to keep moving forward in the process. Furthermore, I would like to thank first supervisor and chair Dr. Anneke Zuiderwijk-van Eijk for always being available for valuable feedback and for her efforts to keep the thesis on track. Finally, the guidance of my second supervisor Dr. Saba Hinrichs-Krapels in the choice of a suitable scope for the thesis and her continued involvement with the thesis was much appreciated. Overall, I would like to thank the entire graduation committee for their time, compassion, and scheduling skills.

I want to thank Kathleen Guan and Wirawan Agahari, for participating in a review of the survey research on short notice. They provided valuable insights into possible further analysis and opportunities for future studies. The review allowed for a different take on the material and substantially added to the trajectory of the thesis.

Moreover, the research would not have been successful without the contribution of those who participated in the questionnaire. Their willingness to take time out of their day to help me and fill in the questionnaire is much appreciated. A lot of people even offered to spread the questionnaire themselves, involving family and friends. I got many enthusiastic responses and feedback, which helped to inform the data analysis and made me even more motivated.

Finally, I would like to thank my family and friends for their unwavering support during the last few months. Their contribution to the formation of this thesis is undeniable, and something I am forever grateful for.

P.

November 2023

Executive Summary

Recent advancements in healthcare have transformed the way clinical care is provided to patients. Remote healthcare has become a significant trend in the healthcare sector. The COVID-19 crisis has further propelled this trend as the healthcare system became less accessible and people gained more interest in health autonomy. The Dutch healthcare system faces sustainability challenges due to decentralisation and an ageing and individualistic population. Consumer-grade wearables (e.g., smartwatches and activity trackers) have been moving towards providing clinical care functionality (e.g., enabling diagnostics, treatment, prevention, and monitoring and alleviation of diseases). The use of consumer-grade wearables for clinical purposes can help the sustainability of the Dutch healthcare system and provide consumers with more health autonomy. However, vulnerabilities leave the wearables susceptible to cybersecurity and privacy risks. When they gain clinical care functionality (i.e., becoming medical wearables), the impact and probability of these risks are increased and problematic for the success of this technology.

The cybersecurity and privacy system of medical wearables deal with frequent social engineering attacks and non-malicious non-secure behaviour by users. Existing research presents a knowledge gap in the practical and thorough application of human-centric cybersecurity with a focus on system design. This research fills this knowledge gap by looking into user-centred cybersecurity and privacy for medical wearables, considering both user needs and limitations in the system design and system environment. The research shows its academic relevance with the closing of this gap and the combination of the fields of behavioural science and cybersecurity research. The following main research question is answered;

How can a user-centred approach to cybersecurity and privacy contribute to the successful use of consumer-grade wearables for clinical care purposes?

To answer the research question, first the role of users in the cybersecurity and privacy environment of medical wearables was examined with a literature review. Challenges and risks were identified with the help of notions from the human-centric cybersecurity field. The findings show that device constraints, large amounts of sensitive data, the remote and highly mobile nature of the device, and the heterogeneity of the device and software as a medical device (SaMD) are relevant challenges in the cybersecurity and privacy environment of medical wearables. Attacker-oriented risks include attacks such as man-in-the-middle attacks, eavesdropping, and replay attacks, which often use vulnerabilities due to device constraints. Social engineering attacks (e.g., phishing and spoofing) combine vulnerabilities due to device constraints and human factors. The impact of when attacks are successful is detrimental to users. Wrong diagnoses and treatment from faulty data can be devastating for patients and the healthcare sector (e.g., regulatory fines and loss of reputation). Human factors cause user-oriented risks. Consumer-grade wearable end-users have an incentive for non-malicious non-secure behaviour in the form of privacy calculus. Also, lack of knowledge and awareness were found to be prominent causes of user-oriented risks. Various examples of non-malicious non-secure behaviours of end-users of consumer-grade wearables were found (e.g., leaving default privacy settings, exhibiting bad password management, falling for social engineering attacks, and sharing sensitive information).

To establish a user-centred approach to the cybersecurity and privacy of medical wearables, tackling the user-oriented risks, and consequently also the attacker-oriented risks, the user needs and limitations need to be known. These were considered with the end-user perception regarding the adoption intention and were examined with quantitative survey research. A web-based questionnaire was shared with adult potential end-users of medical wearables in the Netherlands. The user needs of the system were asked out directly, represented by the impact of attacker-oriented risks. The user limitations are the human factors which hinder the user from secure involvement in the cybersecurity and privacy system. These were asked out as a lack of changes in the importance of concerns due to clinical care functionality (i.e., the main reason for the risk increase in the environment). One study was performed for consumer-grade wearables with clinical care functionality, and another study was conducted for those without. The 155 responses were subjected to data analysis in the form of PLS-SEM in combination with MGA, IPMA and cluster analysis.

The findings of the survey research show the presence of a privacy calculus in the end-user adoption intention considerations. The privacy concern mainly trades off with social influence in the adoption intention of potential end-users. Privacy concern (in its relation to adoption intention) was mainly defined by concerns about data collection and control. Security concern was found to be an important causal factor in the relationship between privacy concerns and the adoption intention. Of the different types of security concern, concern about data integrity loss was found to be the most contributing causal factor. No significant differences were found in the relationships of the conceptual research model based on clinical care functionality. This was found to be problematic as there is no adjusting of non-malicious non-secure behaviour when accessing the clinical care functionality. Furthermore, it was found that three

user segments in the data were defined by different security and privacy concerns, but had no response to clinical care functionality. These user segments could be linked to whether users had experience with consumer-grade wearables or not. Potential end-users familiar with the use of consumer-grade wearables were found to have significantly fewer cybersecurity and privacy concerns than inexperienced potential end-users. Possible underlying justifications for the findings on the conceptual research model were found in existing literature, however, further qualitative research has to be performed to gain more insight.

Based on these results on user needs and limitations and the human-centric components of user, usage, and usability, guidelines for the user-centred approach were formulated. These guidelines were subsequently linked with the challenges and attacker-oriented and user-oriented risks to establish recommendations for medical wearable providers to steer the design of the cybersecurity and privacy system and the structuring of the system environment:

1. To account for different levels of non-malicious non-secure behaviour of end-users, provide experience-based nudging and techno-regulation
2. To account for non-malicious non-secure behaviour of end-users of medical wearables, differentiate behavioural change techniques for SaMD and non-SaMD on the wearable
3. To account for the cybersecurity concern of end-users, focus on functional measures tackling the loss of data integrity
4. To account for the privacy concern of end-users, focus on technical measures and legislation, regulation, and policies tackling improper data collection and loss of data control
5. To ensure the usability of the cybersecurity and privacy system, design the system and structure the system environment with social influences in mind

The research presents a theoretical contribution in the form of a proven relevant conceptual research model for looking into end-user needs and limitations of medical wearables, including differences due to clinical care functionality. Moreover, the research integrates theories by combining the human-centric components of user, usage, and usability with user needs and limitations identified from quantitative survey research. Also, the research integrates the resulting guidelines of a user-centred approach with challenges and risks identified with a literature review. Finally, the research presents a paradigm shift from the traditional technology-centric paradigm where human interaction is seen as problematic to a paradigm where users are considered in the design of the cybersecurity and privacy system and its environment. The research presents practical contributions with its identification of best practices of the human-centric cybersecurity field, guidelines for a user-centred approach and corresponding practical recommendations for medical wearable providers.

By taking into account the limitations and needs of users, the cybersecurity and privacy system and system environment become more equipped for tackling user-oriented risks. Therefore, it helps adverse effects of cybersecurity and privacy breaches (e.g., regulatory fines for medical wearable providers, wrongful treatment and diagnosis of patients, and lawsuits in the healthcare sector). Ultimately, the research helps to alleviate the healthcare sector, provides business opportunities for medical wearable providers (e.g., increased customer satisfaction and increased adoption) and results in benefits for users (e.g., personalised and accurate healthcare and health autonomy). When taking on the recommendations of this research, the established limitations of the research model should be taken into account. Future studies could help the limitations of the research by performing qualitative research on types of non-malicious non-secure behaviour displayed by end-users and corresponding human factors. Furthermore, more data can be collected to be able to conduct analyses based on the 70-year-old or older user segment and to gain a more generalisable sample. A longitudinal study could help to see the effects of the recommendations on the adoption intention and risks over time.

Contents

List of Figures

List of Tables

1 Introduction

In recent years, the medical world has seen rapid digitalisation. Patient files can be accessed in real-time by means of electronic health records (EHR) (Priyananadan & Brahm, 2016), doctor appointments can be carried out online (Stoumpos et al., 2023), and anonymised databases can help researchers scan for patterns in diseases to enhance diagnoses (Kumar et al., 2023). The COVID-19 crisis has further propelled the innovation of healthcare with an emphasis on remote patient monitoring. As doctor visits were discouraged and health anxiety became prominent in day-to-day life, people became more and more interested in the remote monitoring of their health. The increasing desire of people to monitor and maintain their health by themselves leads them to actively seek the tools to do so. At the same time, healthcare institutions realised the inaccessibility of the healthcare system and started to rely more on the technological innovations brought about by digitalisation (Baudier et al., 2022), including remote monitoring opportunities.

In the Netherlands, the trend of healthcare digitalisation comes at a time when the national healthcare system is experiencing sustainability challenges. Demographically, the population of the Netherlands is rapidly ageing. More and more people are becoming dependent on the healthcare system for the diagnosis, monitoring and treatment of their health problems (De Korver, F., 2019). This causes the healthcare system to become overloaded. Economically, the Dutch healthcare system has gone through several cuts and both general practitioners and hospital staff shortages are expected to become worse in the next six years (Linssen, L., 2022). A study of healthcare workers in the Netherlands in 2022 showed that almost all facets of the healthcare sector experience high pressure and burnout rates (Dirven & Gielen, 2022). Moreover, the healthcare system has been extensively decentralised since 2015 (Vermeulen, W., 2015). Healthcare institutions need to manage funding and policies themselves. In the approach of decentralisation of the Dutch healthcare system, there is a focus on the responsibilities of the individual. However, in the face of the older population, this poses a problem. People are reluctant to ask for help and/or suitable help is not available (Kromhout et al., 2020). The digitalisation of healthcare and remote monitoring can help to keep the Dutch healthcare system affordable and accessible in the face of these challenges.

A promising application for remote healthcare is the use of consumer-grade wearable devices for clinical care functionality. These wearable devices (e.g., smartwatches and activity trackers), are body-worn electronic devices that can track, analyse, and transmit personal data. They are often interconnected with apps and other technologies like smartphones and can measure biometric data such as heart rate, oxygen levels, and blood pressure. These so-called consumer-grade wearables are mostly used for personal health monitoring, giving the user insight into their fitness and letting them make healthy life choices. Consumer-grade wearables are different from medical devices (e.g., glucose meters and ECGs), as they are not designed for the purpose of diagnostics, treatment, prevention, monitoring, and alleviation of diseases. However, consumer-grade wearable providers have been making the transition to provide customers with this 'clinical care functionality' in an attempt to capitalise on the newly sparked remote monitoring interest and healthcare system shortcomings. The use of consumer-grade wearables for clinical care purposes can help the healthcare sector. These wearables allow for early detection, and possibly prevention, of adverse health issues (Caldwell, 2022). They collect data that provide a more accurate and/or complete picture of a person's health or lifestyle. This allows for healthcare to become more personalized and reduces the chances of misdiagnosis due to people providing false symptoms or failing to connect symptoms. The introduction of consumer-grade wearables into the healthcare system could relax the workload of healthcare professionals by having fewer check-ups, and they could provide convenience, by lowering manual effort and providing more at-home functionality. Additionally, consumer-grade wearables present an opportunity for other branches of healthcare, by providing easily obtained, noninvasive data collection which can be used in clinical trials and the pharmaceutical industry.

There are two routes providers of consumer-grade wearables can take to provide this clinical care functionality; by advertising their product as a medical device (hardware) or by providing the possibility of running software as a medical device (SaMD) on their product. Recently, companies like Apple, Google and Xiaomi have been pursuing the SaMD route, by gaining regulatory clearance for several clinical care tools on their wearable devices (Wetsman, N., 2020). The software route is often more favourable for existing consumer-grade wearable providers as the process of obtaining all the regulatory clearance needed to be considered a medical device (hardware) is long and tedious.

Besides the move of consumer-grade wearables into clinical care territory, actual medical devices have been moving towards the consumer-grade wearable market as well. Medical device providers have been trying to provide more user-friendly devices by including more functionalities, designing more attractive devices, and providing more freedom from healthcare institutions (Cangardel, K. and Volgina, D., 2023) (Kraudel, R., 2019). These new developments in medical devices can motivate patients to be more willing to use a medical device remotely and increase the value for healthcare providers by gaining more complete, easily obtained data. The result of these simultaneous developments is a converging of the functionalities and abilities of medical devices and consumer-grade wearables. If a consumer-grade wearable has clinical care functionality through SaMD (to varying levels), this thesis will use the term 'medical wearable'. A representation of the converging market of medical devices and consumer wearables can be seen in figure 1.

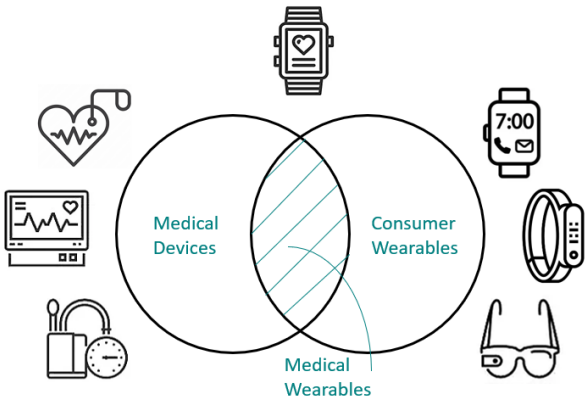


Figure 1: Converging wearable market

1.1 Problem Definition

The use of consumer-grade wearables for the purpose of clinical care is not without risks. In September of 2021, 61 million fitness tracker records from both Apple and Fitbit were exposed online in a wearable device data breach (McKeon, J., 2021). The exposed data belonged to wearable device users around the world and contained names, birthdates, weight, height, gender, and geographical location. The database was not password-protected, and the information was identifiable in plain text. More recently, Strava and other fitness apps have been shown to leak sensitive location information of users like home addresses, even when users used features to set up privacy zones (Montalbano, E., 2023) (Toulas, B., 2023). In 2018, Strava even allowed for the derivation of secret military basis locations in the US utilising a heat map (Hern, A., 2018).

When these types of devices provide clinical care functionality, cybersecurity and privacy threats are detrimental to stakeholders. Sensitive personal health data of users is compromised and the healthcare sector and medical wearable providers face reputation damage, loss of trust, and financial loss. Moreover, if healthcare professionals make wrong diagnoses or treatment decisions based on incomplete or incorrect data due to cybersecurity and privacy attacks, this can have disastrous effects on end-users (Ponemon Institute, 2023). In the grand scheme of things, this also causes a loss of trust in healthcare and medical wearables as a technology. Additionally, inaccurate data due to attacks can cause increased health anxiety (Rosman et al., 2021) and can subsequently have a counteracting effect on the aspired lowering of the workload of healthcare professionals. For attackers, health data, personal identifiable information, and financial information make medical wearables an attractive target.

The increase in cybersecurity and privacy risks (in both impact and probability) of consumer-grade wearables due to clinical care functionality is problematic for the success of medical wearables.

Users play an important role in the cybersecurity and privacy system of consumer-grade wearables. They have a large responsibility in keeping the system safe. Social engineering attacks of malicious attackers are prominent and non-malicious non-secure behaviour of users undermines the system. Users have different privacy and security concerns for consumer-grade wearables and medical devices and thus different needs and limitations (Gao et al., 2015). When the functionalities of these devices are combined in medical wearables, this can be problematic for the cybersecurity and privacy system. A more user-centred approach to cybersecurity and privacy could potentially help the system.

1.2 Knowledge Gap & Research Objective

The practice of taking a user-centred approach to cybersecurity and privacy is promoted by the field of human-centric cybersecurity. Human-centric cybersecurity steps away from traditional technology-centric cybersecurity where the cybersecurity system is focused on tackling technological vulnerabilities and where human involvement in the system is seen as purely problematic. Human-centric cybersecurity looks at how a cybersecurity system can work in tandem with human needs and limitations. There is a lack of practical research into the application of human-centric cybersecurity in a system design context (Zimmermann & Renaud, 2019) (Gutfleisch et al., 2022). This research fills the gap by applying insights from the human-centric cybersecurity field to the cybersecurity and privacy system of medical wearables. Existing related research on the cybersecurity and privacy of medical wearables is mostly focused on technology-centric cybersecurity (e.g., Silva-Trujillo et al. (2023); Fuster et al. (2023)). Although there is related research on the cybersecurity and privacy behaviour and needs of end-users, this is mostly performed solely in the consumer-grade wearable context (e.g., Gabriele & Chiasson (2020)). Additionally, related existing research into the user perception on the cybersecurity and privacy of medical wearables does not combine both user limitations and needs (e.g., Thapa et al. (2023)).

The objective of this thesis is to examine how the adoption of consumer-grade wearables for clinical purposes can be enhanced by taking a user-centred approach to the design of the cybersecurity and privacy system of medical wearables. First, the role of the user in the cybersecurity and privacy environment of medical wearables needs to be clear. To this end, the risks due to both malicious attackers and the involvement of valid users with the system need to be assessed. After this, it is important to establish the user perception on the cybersecurity and privacy environment to determine user needs and limitations. Based on such a user-centred environment analysis, recommendations for the design of the cybersecurity and privacy system can be provided. This shows how the user-centred approach can be applied in the design of the security and privacy system of medical wearables. Concluding, to accomplish the research objective, the following three deliverables are pursued:

- A human-centric overview of cybersecurity and privacy challenges and risks of medical wearables
- An understanding of the end-user needs and limitations in their involvement with the cybersecurity and privacy system of medical wearables
- Recommendations for a user-centred cybersecurity and privacy system

1.3 Research Questions & Research Design

Based on the knowledge gap of user-centred cybersecurity and privacy of medical wearables analysis and the objective of the research, the main research question of this thesis is as follows:

> *RQ: How can a user-centred approach to cybersecurity and privacy contribute to the successful use of consumer-grade wearables for clinical care purposes?*

The research is of a descriptive nature. In order to gather sufficient information and data to answer the main research question, the following subquestions are formulated to steer the research:

SQ1: What are the cybersecurity and privacy challenges and risks of medical wearables?

SQ2: How do users' privacy and cybersecurity concerns influence their intention to adopt consumer-grade wearables for clinical care purposes?

SQ3: What are user-centred cybersecurity and privacy recommendations for medical wearable providers to be able to capitalise on clinical care functionality?

SQ1 helps to establish the user-centred cybersecurity and privacy environment of medical wearables, examining the role of users in the environment. This is done based on human-centric cybersecurity and privacy risk assessment, with the help of two orientations; attacker and user. The attacker orientation focuses on malicious attackers and the user orientation on intentional and unintentional non-malicious non-secure behaviour of valid users. The answering of SQ1 is done with a literature review of existing literature on the topics of human-centric cybersecurity and privacy, as well as that of medical wearable challenges and vulnerabilities. From this, important notions of human-centric cybersecurity are identified which can be used in the design recommendations. Additionally, this question helps to set out the existing risks in the environment and human involvement in these risks. This subquestion thus helps to establish the possible roots of cybersecurity and privacy concerns of end-users and the negative effects of their involvement with the system.

SQ2 is answered to develop more insight into the involvement of end-users with the cybersecurity and privacy system and their limitations and needs. By answering this subquestion, the analysis of the cybersecurity and privacy environment of this thesis is completed. This is done with the development of a conceptual research model in combination with subsequent survey research. The conceptual research model is based on existing literature on technology adoption and research into the user perspective on the cybersecurity and privacy of consumer-grade wearables. Hypotheses are formed based on theory to establish expected relationships and corresponding directions. To answer the subquestion, data analysis is performed according to theories and practices in partial least squares structural equation modelling (PLS-SEM). An expert review of the results of this subquestion is done in the form of a brainstorming session, to establish further interpretation and analysis suggestions.

SQ3 is answered to establish user-centred cybersecurity and privacy recommendations for medical wearable providers. These recommendations explain how the user-centred approach would influence the cybersecurity and privacy system of medical wearables and the existing risks in the environment. Medical wearable providers make managerial decisions which steer the design of the cybersecurity and privacy system and they have a large influence on the system environment. The recommendations for the providers are based on the findings of the first and second research subquestion.

By answering these subquestions, the potential contribution of users' limitations and needs to the cybersecurity and privacy of medical wearables is examined and recommendations are provided to take these into account. This together builds the answer to the main research question.

1.4 Research Relevance

1.4.1 Academic Relevance

From an academic perspective, the research contributes to the literature on human-centric cybersecurity by providing insights into user limitations and needs and their contribution to the cybersecurity and privacy system of medical wearables. Important notions of human-centric cybersecurity literature are combined and used in a human-centric risk assessment, containing both attacker and user orientations. The research takes a new approach to human-centric cybersecurity, combining both literature on cybersecurity and privacy risks and the risk perception of end-users, tackling both user limitations and needs. In this sense, the thesis seeks to combine cybersecurity and privacy environment analysis with notions from the field of behavioural science in a novel, meaningful way.

1.4.2 Corporate & Societal Relevance

The research helps providers of medical wearables guide managerial decisions regarding effective cybersecurity and privacy system design by taking a user-centred approach. The success of medical wearables as a technology stands and falls with the adoption of end-users, Providers can face reputational damage, regulatory fines, loss of consumer trust, and damaged business relationships due to breaches. More importantly, it can harm the trust in and adoption of medical wearables. When the adoption of end-users goes down, Dutch society loses a promising technological opportunity in healthcare. Medical wearables can help to relieve the workload and stress of healthcare professionals

and the government can incentivise the use of this technology to counteract the problems due to the decentralisation of the healthcare system. End-users gain a more personalised, convenient and well-rounded way of diagnosis, treatment, and monitoring and can have more autonomy over their health. By providing user-centred recommendations for medical wearable providers, providers can take into account the risks due to the involvement of valid users with the system. This way, the cybersecurity and privacy environment is built around end-users. Ultimately, the research helps the successful use of consumer-grade wearables for clinical purposes.

1.5 Thesis Structure

The contribution of the research, as explained in section 1.2, will be handled in the different chapters of the thesis. A visualisation of the chapters and their contributions to the overall user-centred cybersecurity and privacy approach can be seen in figure 2.

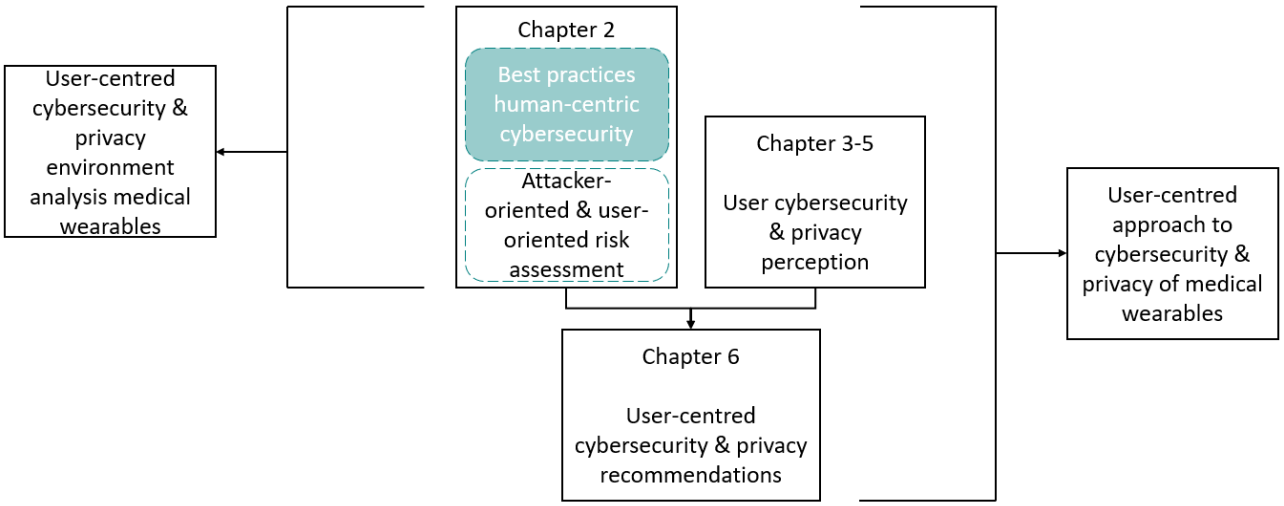


Figure 2: Research overview

Chapter 2 constitutes the establishment of human-centric cybersecurity best practices and a human-centric cybersecurity and privacy risk assessment of medical wearables, consisting of an attacker orientation and user orientation. Chapter 3 looks into the needs and limitations of end-users by examining their cybersecurity and privacy risk perception in relation to their adoption intention. After the results of this end-user perception are concluded in chapter 5, the user-centred cybersecurity and privacy environment analysis of this thesis is complete. In chapter 6, recommendations for medical wearable providers to steer the system design and the structuring of the system environment are formed, based on the environment analysis. Chapter 2 to chapter 6 cover the user-centred approach to the cybersecurity and privacy of medical wearables.

The thesis is structured into four main parts; the research justification, environment analysis, data collection and analysis, and finally, the evaluation and conclusion. The environment analysis is built by the literature review on the human-centric risks and the survey research on the end-user needs and limitations. An overview of the methodological structure of the thesis (including the answering of the research questions) can be seen in figure 3. As stated above, the total of the cybersecurity and privacy environment analysis contains chapters 2 to 6.

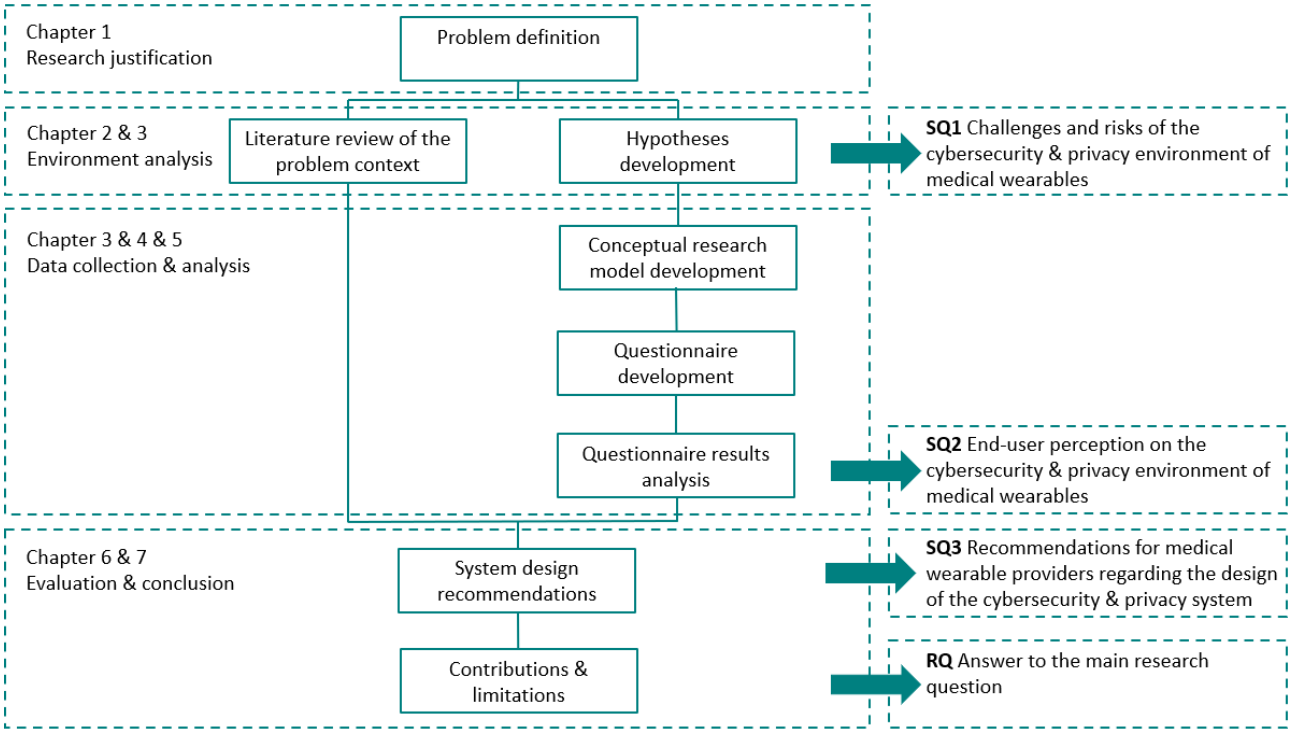


Figure 3: Methodological structure overview

2

Literature Review

This chapter outlines the underlying theories and literature relevant to the user-centred approach to the cybersecurity and privacy of medical wearables. First, a theoretical background regarding cybersecurity is set out. In section 2.1, literature on human-centric cybersecurity is examined to establish important notions of the field that will be used in the research. In section 2.1.4, the system and environment characteristics of medical wearables are set out. Subsequently, in section 2.2, a human-centric risk assessment for the cybersecurity and privacy of medical wearables is performed with the help of existing literature. Challenges and vulnerabilities of medical wearables are examined, by taking into account the general system and environment characteristics and that of the cybersecurity and privacy system. After this, attacker-orientated risks and user-oriented risks are established. With the results of the risk assessment, subquestion 1; 'What are the cybersecurity and privacy challenges and risks of medical wearables?' is answered. The part of the user-centred cybersecurity and privacy environment of medical wearables tackled in this chapter can be seen in the black-lined box in figure 4 below.

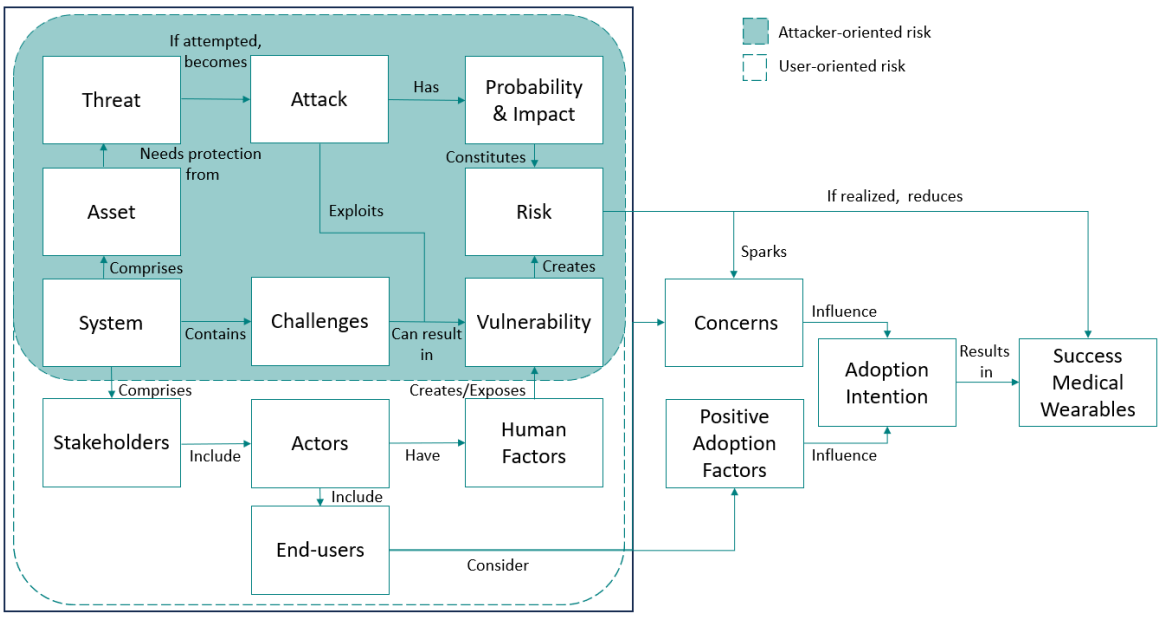


Figure 4: User-centred cybersecurity and privacy environment analysis: human-centric risk assessment

The sources in this literature review were acquired by performing a computerised search of scientific literature in Scopus and Web of Science databases, based on the guidelines of the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) (Page et al., 2021). The literature review consists of two different parts; the theoretical background and a medical wearable risk assessment. There is a focus on the combination of human behaviour and (cyber)security and privacy aspects of wearables. Entries are only included if the search terms are included in the title of the article, the provided keywords or in the abstract. The search is repeated for other terms related to combinations of words or synonyms (e.g., information and data). The search is started with the following search terms:

((cyber* OR security OR privacy) AND (human* OR user)) OR wearable
Within the results, a further search is executed with the search terms Health* and Behaviour.

Because of the lack of closely related articles on the subject and the combination of two fields; behavioural science and cybersecurity, the search is further refined in two ways. Search terms are added that include aspects of technology-centric cybersecurity. Therefore the search is limited to the subject area of computer sciences and the results were searched by the main keywords human, cybersecurity, device, and data privacy. On the other hand, the search is limited to the subject area of social sciences and the results are searched by the keywords privacy, data collection, and motivation. The resulting papers are again checked for title and abstract in terms of relevance. A full-text check results in articles being removed for not covering the subject of the research and through the snowball effect specific other articles are found.

2.1 Theoretical Background

2.1.1 Cybersecurity

To be able to perform a cybersecurity and privacy analysis, it is important to first understand the concepts of cybersecurity which will be used in this research. Cybersecurity is defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's asset" (Von Solms & Van Niekerk, 2013, p. 97). NIST (2015) defines cybersecurity as "the prevention of damage to, unauthorised use of, exploitation of, and – if needed – the restoration of electronic information and communications systems and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems" (p. 41). These three dimensions form the pillars of information security, which is a significant aspect of cybersecurity (NIST, 2008, p. 7);

- Confidentiality: is "the property that data or information is not made available or disclosed to unauthorised persons or processes."
- Integrity is "the property that data or information have not been altered or destroyed in an unauthorized manner."
- Availability is "the property that data or information is accessible and useable upon demand by an authorized person."

Cybersecurity differs from information security most importantly in the assets they protect. In cybersecurity, the protection goes beyond just information and includes the whole of cyberspace, e.g., people, critical infrastructures, and society. The main goal of cybersecurity is to implement policies and use technological tools to secure systems and networks, preventing cyber threats from occurring. Cyber threats are possible cyberattacks which exploit vulnerabilities in the system. These threats comprise a risk (probability and impact), if not properly mitigated (Khan, N., 2023).

The cybersecurity field is technology-centric by nature, with technology being viewed as the ultimate solution to security problems (Haney, 2022). Technology-centric cybersecurity and privacy assessment focuses on risks occurring due to vulnerabilities in the technology. These risks are considered potential cyberattacks. In technology-centric assessments, concepts such as attack goal, source, target/assets, method, probability, and impact are considered (Mancuso et al., 2014). There are several techniques for this assessment of technology-centric cybersecurity and privacy risk. Most prominently, some sort of threat modelling is performed. One relevant example of a threat modelling approach (for the scope of this thesis) is that of the STRIDE model (table 1), where attack purposes have been classified into six categories (Kohnfelder, L. and Grag, P., 1999). The STRIDE model is often linked to the impact based on the information security pillars (including the concepts of non-repudiation and authentication).

Attack type	**Description**
Spoofing Identity	Attacker pretends to be someone else, intending to steal data or gain unauthorised access
Tampering	Attacker maliciously modifies data
Information Disclosure	Attacker gains access to confidential data
Repudiation	Attacker denies involvement in malicious activity; no way to prove it
Denial of service	Attackers denies service to valid users
Elevated Privilege	Attacker gains privileged access to the device/service

Table 1: STRIDE model
(Kohnfelder, L. and Grag, P., 1999)

Technology-centric cybersecurity approaches focus on tackling vulnerabilities of the system by having technological mitigation and prevention techniques. In technology-centric approaches to cybersecurity, humans are often perceived as the 'weakest link', displaying human errors and undermining the security system. In reality, socio-technical systems are complex, highly interactive and unpredictable, and adverse events have multiple contributing factors. Moreover, contrary to being the primary source of all problems, humans can be crucial players in defending against attacks (Zimmermann & Renaud, 2019). In human-centric cybersecurity, the focus of cybersecurity is shifted to taking into account people's limitations and needs. A human-centric approach emphasizes the significance of the human element in designing, implementing, and managing cybersecurity systems. Grobler et al. (2021) define human-centric cybersecurity as "involving all aspects of cyber security, with a particular focus on the human involvement in the system and processes. That is, understanding how humans represent value, but also risk to an organization; understanding how humans and computer interact and what risks are introduced as a result of these interactions" (p. 2).

Human-centric cybersecurity is relatively underexposed in the cybersecurity literature and there has been advocating for more research being done on this approach (Zimmermann & Renaud, 2019) (Gutfleisch et al., 2022). Several papers state the importance of considering a human-centric approach when designing for cybersecurity; not just imposing more and stricter security measures, but measures that are adaptive to users and designing security with users in mind (Herley, 2014) (Adams & Sasse, 1999). As stated in the introduction, the relevance of this orientation for medical wearables is high. As consumer-grade wearables gain clinical care functionality, end-users have a prominent role in keeping personal health data safe and private. Additionally, the consumer-grade wearable system is implemented in the healthcare sector. This adds another human element (organisation) to the system. A purely technology-centric approach to cybersecurity undermines the success of medical wearables. The following sections dive deeper into the human-centric approach to cybersecurity.

2.1.2 Human-Centric Cybersecurity

Human-centric cybersecurity mainly involves understanding human behaviour and designing systems that consider underlying limitations and needs. Most literature in this field takes an integrated approach, combining environmental dimensions and focusing on differentiation. For the environmental dimensions, often organisational, individual, and technical dimensions are considered. Pollini et al. (2021) take an integrated human-centric approach to analysing computer and information security (CIS) systems. The authors establish the individual factor, where they mention several psychological theories for the individual reasoning behind cybersecurity behaviour. Within the organisational factor, contextual and situational knowledge of an organisation, culture, and maturity levels are considered. The technological factor looks at the underlying justification that users experience a usability-security trade-off, actively avoiding security mechanisms that are difficult to use. Security design with users' needs in mind is stated to be effective for increasing users' comprehension of the security system properties and thus increasing security itself.

As stated in the knowledge gap, in terms of practical human-centric cybersecurity design approaches, the literature is not extensive. Grobler et al. (2021) present a human-centric cybersecurity design approach by defining user, usage, and usability (3U's) as three essential components for considerations of cybersecurity systems. The user component is defined by the concepts of demography and culture, situational awareness, psychology and behaviour, and cognitive factors. The paper advocates considering different user groups and behaviours (linked to human factors) and their corresponding expectations and incentives. The usage component is established by looking at how functional, technical measures and legislation, policies can be designed and/or implemented with a human-centric approach to assure effectiveness. The paper suggests designing cybersecurity systems based on different security levels for the technological and non-technological dimension. The technological dimension consists of functional and technical measures. Functional measures are broad cybersecurity measures with a specific security function in mind (e.g., access controls and security awareness and training). Technical measures are specific technological or software-based cybersecurity techniques which are transparent to users (e.g., firewalls and encryption algorithms). Legislation, regulation, and policies are non-technological measures to support the cybersecurity system. The paper advocates establishing measures which are not overly restrictive, are transparent, and minimal. For the usability component, the authors state the importance of looking at factors influencing the usability perception of users regarding the cybersecurity system. They provide experience and interaction factors as two aspects influencing the perception of usable security. The focus on the three components of user, usage, and usability is further affirmed by other research in the human-centric cybersecurity field (Haney, 2022) (Rahman et al., 2021). These three components are seen as pillars of human-centric cybersecurity and will be considered for the user-centred approach of this research.

2.1.2.1 Risk Assessment

As stated above, an important part of human-centric cybersecurity is understanding that users' limitations play an important role in the cybersecurity environment of technologies. Thus it is important to understand the causes and nature of non-malicious non-secure behaviour or a lack of 'cyber hygiene' of users. Vishwanatha et al. (2020) define cyber hygiene as "the cybersecurity practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyber-attack" (p. 2). There are two types of non-malicious non-secure behaviour regularly mentioned in literature; intentional and unintentional (Lahcen et al., 2020). Chowdhury et al. (2019) classify it as non-malicious informed disregard (non-prompted and prompted). They also consider uninformed behaviour and misinformed behaviour while Pollini et al. (2021) call it accidental and non-deliberate actions determining a violation of a security rule or a violating procedure and deliberate actions determining an unwanted violation of a security rule. In general, this research considers non-malicious non-secure behaviour as 'user-oriented risks'. The risks are considered as both intentional and unintentional. Underlying reasons for non-malicious non-secure behaviour are so-called 'human factors' (Hilowle et al., 2023) (Lahcen et al., 2020). An important part of designing for human-centric cybersecurity is to assess underlying causes of not displaying secure behaviour by users. Risk assessment thus involves the examination of the human factors.

Risk assessments of user-oriented risks and associated human factors mostly take their approach from traditional risk assessment approaches in technology-centric cybersecurity (Henshel et al., 2015) (The Chartered Institute of Ergonomics & Human Factors (CIEHF), 2022). Human factors are often defined in terms of individual human factors and environmental factors (Lahcen et al., 2020). The Human Factors Framework of Cybersecurity Risk Assessment (HFF) of Henshel et al. (2015), divides the human factors into inherent and situational characteristics. Inherent characteristics are comprised of behavioural characteristics and knowledge/skill characteristics while situational characteristics include circumstances such as insider access. Another important concept in human factor literature is the interactive and dynamic nature of human factors. Young et al. (2018) establishes three actors that influence human factors in the system; humans, organisations, and technology. Human factors are seen as evolving in time and dependent on each other.

The user-oriented risks in these types of frameworks are often linked to the risks due to malicious attackers (Ferro et al., 2021). Mancuso et al. (2014) combine a technology-centric cybersecurity approach with human factors and present a thorough framework to identify risks. They describe a waterfall framework to consecutively consider, the adversarial, methodological, and operational dimensions of malicious informed attacks (figure 5). The adversarial dimension looks into the goal and source of the attack. The methodological dimension looks at the attack vector (method used) and the target of the attack, which can include system components as well as specific data. The operational dimension looks at the impact, which can be further divided into the technological impact, human impact, and socio-organisational impact. Within each of the dimensions, the human factor considerations are made.

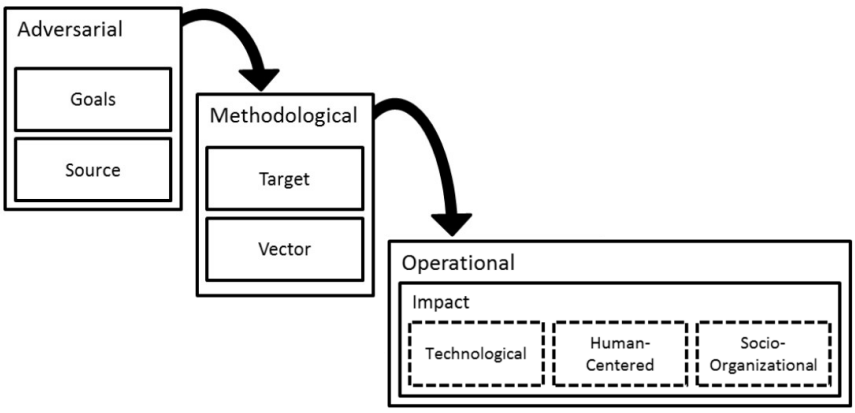


Figure 5: Three-dimensional Waterfall framework human-centric approach
Adapted from Mancuso et al. (2014)

2.1.2.2 Behavioural Change Theory

After the risks are identified, it is important to know how these risks can best be mitigated or prevented. In human-centric cybersecurity literature, there is a focus on the combination of usable security design and behavioural change techniques. To this end, the literature on behavioural change theory is examined for relevant theories and best practices for its application in the cybersecurity field. The theories are further checked for alignment with the components of human-centric cybersecurity; user, usage, and usability.

Michie et al. (2011) developed the capability-opportunity-motivation-behaviour (COM-B) model (figure 6). Within COM-B, capability is considered as physical and psychological capabilities. Physical capability focuses on the skills and abilities of people, while physiological capability focuses on knowledge, memory and attention. Within opportunity, physical (e.g., environmental context and resources) and social opportunities are considered (e.g., social influence, pressure, and norms). Motivation is classified into reflective and automatic motivation. Reflective motivation considers beliefs about capabilities and consequences, goals, identity, and roles. Automatic motivation considers emotions, reinforcements, and incentives.

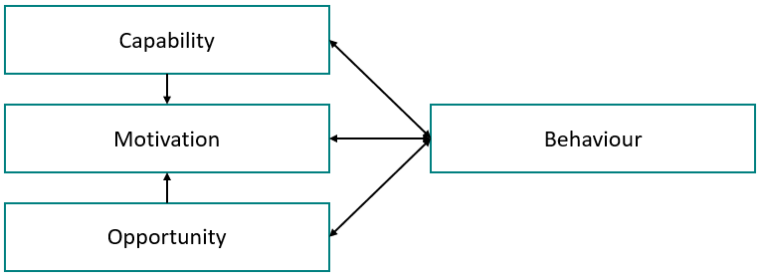


Figure 6: COM-B model
Adapted from Michie et al. (2011)

The model essentially presents a classification of human factors. The authors of the model further developed COM-B into the Behavioural Change Wheel, for guiding behavioural change strategies (interventions and policies) based on the different components. In the behavioural wheel, the COM-B model components are directly linked to mitigation strategies in the form of education, training, coercion, enablement, environmental restructuring, incentivisation, persuasion, restrictions, and modelling. Additionally, the wheel looks at suiting policy options for these intervention strategies; marketing/communication, guidelines, fiscal, regulation, legislation, environmental/social planning, and service provision.

The COM-B model has been proven relevant in existing literature regarding the tackling of unwanted cybersecurity behaviour (Van der Kleij, 2022) (Alshaikh et al., 2019). When it is determined which behavioural change strategy would work best for the relevant human factor, a technique of delivery/presentation regarding the system design has to be chosen. Van Steen (2022) looks into the possibility of specifically improving cybersecurity behaviour by taking a closer look at the way systems present options and choices to end-users. The authors categorize behavioural change strategies under two techniques: nudging and techno-regulation. The former aims to gently push end-users towards a preferred (safer) course of action, while the latter forcefully removes any unwanted (riskier) options, thereby improving cybersecurity at the cost of freedom of choice. The authors suggest that behaviour that merely needs to be increased or decreased or that users are familiar with and needs to be done only once, could be addressed using nudging techniques. For behaviours that need to be changed permanently or that involve systems which are new to users, techno-regulation might be more sensible.

When designing nudges and techno-regulation it is important to rely on proven effective strategies for influencing human behaviour. Dolan et al. (2012) developed the MINDSPACE framework (table 2), to describe a number of the 'influencing factors' that have been identified across different economic and psychological models of behaviour change. The MINDSPACE framework is effective for designing strategies for unwanted human behaviour (Coventry, Briggs, Jeske, & Van Moorsel, 2014).

Influences	Nudges description
Messenger	We are influenced by the person and/or method by which the message is delivered
Incentives	We are influenced by the rewards and punishments (losses) we receive. This includes our evaluation of the cost of behaving appropriately and the cost of the consequences if we do not
Norms	We are influenced by the behaviours demonstrated by influencial others, such as senior managers, colleagues and family
Defaults	We go with the flow of preset options. The default option will be chosen more often
Salience	We are attracted by what is either novel or particularly relevant to ourselves
Priming	Our acts are influenced by sub-conscious cues
Affect	Our emotional associations influence our behaviour
Commitments	We seek to be consistent with our public statements and reciprocate the acts of others
Ego	We act in ways that make us feel better about ourselves

Table 2: MINDSPACE framework
(Coventry, Briggs, Jeske, & Van Moorsel, 2014)

Coventry, Briggs, Blythe, & Tran (2014) state the relevance of the MINDSPACE framework for tackling the risky cybersecurity behaviour of users. Van der Kleij (2022) looked into the deployment of behavioural change techniques tackling non-malicious non-secure behaviour and found that nudges in cybersecurity need to be transparent, sources need to be trustworthy, and they need to appear only occasionally.

Literature on behavioural change theories in cybersecurity and privacy also stresses the opportunity of adapting techniques to user segments. Qu et al. (2021) performed research on nudging based on user segments and found that only individuals who are deeply concerned about the future consequences of their actions will be affected by a so-called 'promotion-based' nudge, which speaks to people's notion of their ideal self. Qua et al. (2022) also finds that nudges work better if matched to specific user characteristics. The authors set up profiles that capture user characteristics (e.g., personality traits) related to nudge effects.

2.1.3 Privacy

The NIST defines privacy as "the right of a party to maintain control over and confidentiality of information about itself" (NIST, 1992, p. 43). Westin (1968) defines privacy 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. 3). Privacy, although closely related, differs from confidentiality in that confidentiality controls protect data against the unauthorized use of information which is present in the data flow, whereas privacy protects the rights of an individual to control the information that is collected, maintained, and shared with others. Thus, intentional non-malicious non-secure behaviour of users is an important concept within the privacy environment.

When considering user-oriented risks to privacy, it is important to understand the theories concerning user behaviour around privacy. One of the relevant leading theories is that of the privacy calculus (Kim et al., 2019) (Princi & Kramer, 2020). Privacy calculus theory regards privacy risk as a trade-off of actions with various other beneficial factors of information disclosure (Zhang et al., 2018). An individual's privacy decisions depend on the outcomes of a calculation of the privacy risks and benefits that they would incur for disclosing the information (Sun et al., 2020). People then only disclose personal information when the benefit of sharing outweighs the risk of sharing. This privacy calculus informs the privacy concern, which constitutes individuals' beliefs about privacy risks (Zhang et al., 2018). Related to this is the theory of hyperbolic discounting, where people are considered to be near-sighted in their assessment of privacy risks and benefits, trading long-term risks for short-term gain (Acquisti & Grossklags, 2004). In the 'extended privacy calculus', this theory is extended from information disclosure to the effect of the calculus on the adoption intention regarding a technology (Schomakers et al., 2022).

The theory of the privacy paradox, further indicates that even if people state high privacy concerns, they often do not behave accordingly. The privacy paradox shows that people disclose personal information despite reporting high concerns about privacy or showing low sharing intentions (Sun et al., 2020). The privacy paradox focuses on a concern-behaviour gap, which describes that people share their personal information despite their high privacy concerns. This means there are discrepancies between actual and self-reported behaviour in research on non-malicious non-secure behaviour.

Considering the human-centric background of this research, it is useful to look at theories which consider differences in privacy due to user characteristics. Louis-Harris & Associates & Westin, A. F. (1995) found three ideological-interest positions of privacy; privacy fundamentalists, pragmatists, and unconcerned. Privacy Fundamentalists "rejected consumer-benefit or societal-protection claims for data uses and sought legal-regulatory privacy measures" (Westin, 2003, p. 445). Westin equates the Privacy Unconcerned with the low concern group. The Privacy Unconcerned "were generally ready to supply their personal information to business and government and rejected what was seen as too much privacy fuss" (p. 445). Westin equates Privacy Pragmatists with the Moderate Concern group. Westin regards Privacy Pragmatists as holding a more balanced view of privacy because they "examined the benefits to them or society of the data collection and use" (p. 445).

2.1.4 Medical Wearables: System & Environment Characteristics

To set out human-centric cybersecurity and privacy challenges and vulnerabilities, it is crucial to have an overview of the general system characteristics of medical wearables. System characteristics of medical wearables are different for different types of wearables. However, they do often share the same type of architecture components, stakeholder environment, and acting legislation.

Medical wearables comprise of consumer-grade wearable hardware with software as a medical device (SaMD) applications. Recently, European regulation on medical devices, the medical device regulation (MDR), has increased the classification of SaMD from class I medical devices to class IIa, which means it poses a moderate risk to the health of users if not functioning properly. SaMD now requires a conformity assessment by a Notified Body, and manufacturers must provide more detailed technical documentation. Moreover, SaMD has to be proven as accurate (and thus effective) by clinical research (Tziouras, 2022). The data collected by medical wearables falls under the general data protection regulation (GDPR) and is considered health data. This means that stricter rules are enforced on the data regarding data sharing practices and data usage. However, there is no standardisation regarding the protocols and measures used in the system. The regulatory and legislative environment of medical wearables focuses on technology-centric cybersecurity and places a lot of responsibility on the end-user to maintain their privacy.

Medical wearables operate under the principle of the internet of things (IoT). IoT devices are an outcome of combining the worlds of information technology (IT) and operational technology (OT). IoT devices can collect a large amount of data, and have a large number of device connections. Many IoT devices include technological advances such as cloud computing, mobile computing, embedded systems, big data, and low-price hardware. IoT devices can provide computing functionality, data storage, and network connectivity for equipment that previously lacked them, enabling new efficiencies and technological capabilities, such as remote monitoring. When IoT is used in the healthcare sector it is called the internet of medical things (IoMT) or wearable internet of medical things (WIoMT) for wearable devices. IoT devices typically comprise of four layers;

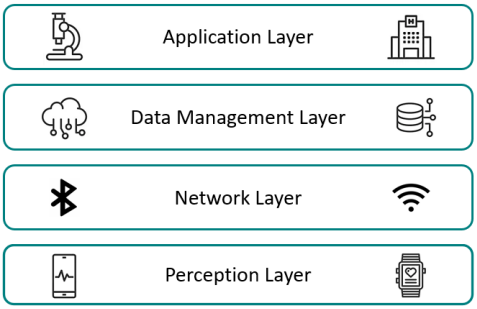


Figure 7: IoMT data layers
Adapted from Rizk et al. (2019)

- Application layer
  The application layer is a presentation and service layer where the data collected by the devices are employed, understood, and shared. This is the layer where the results of the data interpretation can be observed. The application layer in IoMT consists of health professionals diagnosing, treating or remote monitoring, and other healthcare applications such as clinical trials and medical research.

- Data management layer
  The data management layer is the layer comprising data storage, management, computing, and processing units. Here, cloud services and databases store the data that is sent through the network layer. In the case of IoMT, connections with electronic health record (EHR) databases and machine learning techniques come into play in this layer.

- Network layer
  The network layer is the layer comprising the communication between IoT objects and IoT application servers. The layer includes both wired and wireless communication. This layer processes the data coming from the perception layer and transmits them to the higher data management layer. IoT gateways help this connection by guiding data traffic between different networks and protocols. In some cases, mobile phones act as the IoT gateway. Wireless communication standards in this layer include Bluetooth low energy (BLE), Zigbee, Wi-Fi, and 5G.

- Perception layer
  The perception layer is the layer in which data are produced and collected through devices that can be directly communicated with by the end-user. This layer is examined in two object classes such as IoT devices that detect in itself (wearable) and IoT hub nodes acting as gateways (e.g., mobile phone). The data are acquired through the detection nodes such as sensors, while the gateway nodes are used for transmitting and checking the obtained data. The detection nodes have computing (e.g., microcontroller (MCU)), sensing, and communication functionalities. The mobile phone also acts as an end-user interface, using its connection with the cloud to run applications such as SaMD.

When consumer-grade wearables start to provide clinical care functionality, they operate in an environment with increased stakeholders and actors. Actors are considered those stakeholders who have a direct effect on or interact with the data flow. An overview of the stakeholder environment based on the data flow regarding the primary clinical care functionality (catered to consumers/patients) of medical wearables can be seen in figure 8.

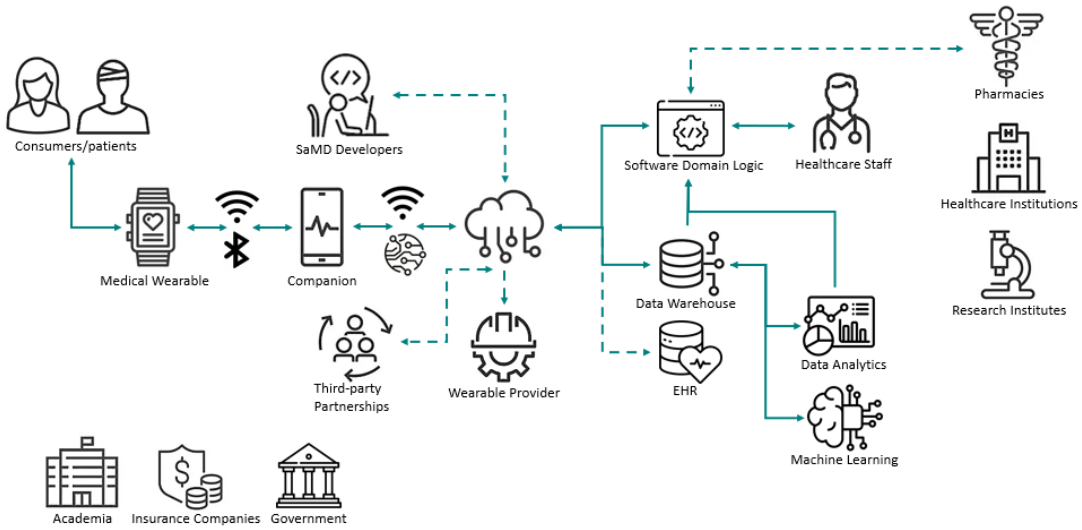


Figure 8: Medical wearables stakeholder and data flow overview
Adapted from Smart Medical Devices (n.d.) Fuster et al. (2023)

The data flow starts with the collection of data at the end-user through the sensory equipment of the detection and hub nodes. Once collected, the data is stored in the service cloud of the wearable provider. SaMD developers use this cloud to get their software applications across. Relevant data for the clinical care functionality is then transferred from the cloud into a data warehouse. This warehouse is accessed for the purpose of data analytics and machine learning. The analysed and raw data is accessed by healthcare staff through software domain logic. This converts the data for the purpose of connection with the software used by the healthcare staff. Less direct data flows, but still relevant to end-users, are the data flows with the wearable provider and associated third-party partnerships (e.g., advertisements), the access of the data by pharmacies (e.g., medication intake tracking and ordering), and the connection with other healthcare databases (e.g., EHR databases).

An important stakeholder in this environment is that of the healthcare institution. As stated before, healthcare institutions like hospitals benefit from the lower workload for healthcare staff and increased information quality and quality of care. Research institutions or clinical trials can benefit from the data flow by using medical wearables for their data collection (Tu & Gao, 2021). Moreover, the government benefits as the data enables more efficient, personal healthcare, leading to increased welfare and relief of necessary financial investment in the healthcare sector. The data collection of consumer-grade wearables can also be used by insurance companies to set accurate premiums for healthcare insurance (Neumann et al., 2022). Pharmacies can effectively adjust prescriptions and order medication on the basis of the collected data. Academia is a less involved stakeholder, interested in all kinds of aspects of the process of research and development.

2.1.5 Conclusions Theoretical Background

In the theoretical background section of the literature review, important aspects regarding human-centric cybersecurity and the privacy environment were examined. Human-centric design of the cybersecurity and privacy system and its environment need to take into account the components of user, usage, and usability. These components will form the basis for the user-centred approach of the research. Other authors recognize the importance of environmental dimensions (e.g., organisational, individual, and technical) and their interactive nature in the considerations regarding the cybersecurity environment. This is important to take into account when considering the cybersecurity and privacy system in terms of challenges and vulnerabilities. Literature on human factors can both be individual or environmental and user-oriented risks can best be identified with a traditional technology-centric approach to risk assessment.

Once the environment analysis is completed (chapter 5), the best practices of behavioural change techniques will come into play. Which techniques to use is best determined by using the COM-B model and Behavioural Change Wheel combination and the techniques are best designed according to the MINDSPACE framework. In the user-centred approach, nudges should be transparent, sources need to be trustworthy and they should not be overly restrictive or happen too often. Furthermore, behavioural change techniques are more effective when they account for the components of user, usage and/or usability.

The system and environment characteristics of the medical wearable show that there is an interconnected data flow which covers different layers of IoT, comprises several protocols and policies and has an extensive stakeholder network.

2.2 Human-Centric Cybersecurity & Privacy Risk Assessment Medical Wearables

With the necessary background known, this section will aim to answer research subquestion 1. In this section, a human-centric risk assessment of the cybersecurity and privacy of medical wearables will be performed by examining existing literature. To this end, notions from the literature review on human-centric risk assessment are used. First, a human-centric analysis of the system environment is performed by considering organisational and technological factors. Subsequently, cybersecurity challenges and vulnerabilities will be identified. The framework of figure 5 is used to establish a human-centric risk assessment approach which allows for the benefits of technology-centric assessments. Moreover, both the attacker-oriented and user-oriented risks are considered on the adversarial, methodological and, operational dimensions, to allow for a thorough, user-centred overview. The attack-oriented risks consider any type of malicious behaviour, while user-oriented risks consider both intentional and unintentional non-secure non-malicious behaviour.

2.2.1 Challenges & vulnerabilities

In human-centric risk assessment, it is important to consider the interactive nature of the cybersecurity environment. In the stakeholder environment, each actor has its role and responsibilities in establishing a proper cybersecurity and privacy environment. All actors display calculi which contribute to the overall level of cybersecurity and privacy in the system. The different actors consider the 'costs' of appropriate practices with other incentives. It is important to establish human-centric considerations in the system based on individual, organisational, and technological factors. Individual incentives will be examined in the user-oriented risk section (2.2.3). Pertinent incentive trade-offs in the system include;

- Organisational incentives healthcare versus cybersecurity and privacy
  The organisational environment of the healthcare sector requires timeliness to ensure the quality of care. This cultural aspect is an important human-centric element in the cybersecurity and privacy environment of medical wearables. Timeliness in operating IT healthcare systems undermines the importance of cybersecurity practices. The culture of the healthcare sector also affects human factors in employees such as workload, stress, and distraction. Coventry et al. (2020) investigated the security behaviour of healthcare staff and found that they perceived the organisational culture as "understaffed and overworked" (p. 117), where staff is too busy and under major time constraints, leading to non-malicious non-secure behaviour.

- Business incentives providers versus cybersecurity and privacy
  The business environment that medical wearable providers operate in, means that decisions are made for the success of the business. End-users of wearables sometimes only have limited options in displaying secure behaviour or maintaining privacy due to these decisions. Medical wearable providers then value incentives for non-secure practices over incentives for secure practices. Bauer & Van Eeten (2009) looked into incentives of software and hardware vendors and identified the incentives for non-secure practices of costs, time to market, partnerships, and quality of service. Gutfleisch et al. (2022) looked at the influence of contextual factors on the level of usable security in the development of software. They found that the security system in software is influenced by budget, time, and a 'functionality first' mantra. All these aspects bring in revenue (directly or via customer satisfaction) and establish the direct success of a company.

The combination of the actor incentive trade-offs with the system and environment characteristics of medical wearables (section 2.1.4), leads to several challenges and vulnerabilities. Once these challenges are not properly addressed and an attacker exploits them, the consequences are severe. Relevant challenges and vulnerabilities for medical wearables and corresponding literary sources can be seen in table 3.

Challenges	**Vulnerabilities**	**Literature**
Device constraints (e.g., computational power and memory)	Weak authentication controls Unsecure wireless personal area networks (WPANs) Weak encryption Cloud computing	(Silva-Trujillo et al., 2023) (Fuster et al., 2023) (Cartwright, 2023) (Shah, 2019)
Large amount of sensitive data	Healthcare organisational infrastructure Medical database linkage Healthcare technological infrastructure	(Coventry et al., 2020) (Zeadally et al., 2019) (Williams & Woodward, 2015)
Remote and highly mobile device	Human factors Dynamic updating/patching	(Silva-Trujillo et al., 2023) (Cartwright, 2023)
Heterogeneous devices and SaMD	Lack of standards security and privacy Third-party connections Data storage connections	(Thapa et al., 2023) (Silva-Trujillo et al., 2023) (Piwek et al., 2016)

Table 3: Challenges consumer-grade wearables for clinical care purposes

First of all, wearables have device constraints which make them vulnerable. Power, memory, computational power, and device costs all affect the suitability of cybersecurity measures. When choices have to be made for the use of technological resources, cybersecurity is often undermined (revenue trade-off). Unsecure networks are used for easy communication functionality and authentication controls are limited by storage ability. In the case of sensitive health data, the absence of proper cybersecurity measures due to device constraints becomes a major problem. Silva-Trujillo et al. (2023) and Blow et al. (2020) further looked into the vulnerability of BLE, which has been adopted as the standard for wireless personal area networks (WPANs) in consumer-grade wearables. BLE often uses unsecured pairing methods, static addresses, no end-to-end security, and weak authentication. Additionally, BLE connections are stored

in the device, thus if the device is lost or stolen this makes them vulnerable to data breaches. Business incentives of medical wearable providers play an important role in the challenge of device constraints for cybersecurity and privacy.

Another challenge of medical wearables is the large amount of data they collect that enters the healthcare system. This causes vulnerabilities in the form of linkage of data with other medical databases such as EHR, which increases the amount of sensitive data in the system. Moreover, technological infrastructure in the healthcare sector includes non-secure nodes (e.g., outdated software and medical devices). The large amount of data also means that data handling mistakes by healthcare professionals are more frequent (Ponemon Institute, 2023). Hilbel & Frey (2023) found that healthcare professionals will experience an information burden from consumer-grade wearables, especially due to false positive findings, which means an excess referral burden on doctors. Several sources state that barriers for healthcare professionals, regarding the use of medical wearables, include accuracy and relevance of data, both related to data burden. These healthcare sector vulnerabilities are related to the human-centric element of organisational culture and the corresponding trade-off between quality of care and cybersecurity and privacy.

The remote use of medical wearables and their high mobility means end-users become an important part of the cybersecurity and privacy environment. Their human factors result in a significant vulnerability that malicious attackers can exploit, or valid users become attackers themselves. Here, the trade-off with other individual incentives of users such as functionality versus cybersecurity and privacy comes into play. Apart from human factors, the remote and highly mobile nature of medical wearables also has its effects on the updating and patching process. These processes are performed in consumer-grade wearables with the use of HTTP connections. These can be easily intercepted which hinders the security of new vulnerability patches (Fuster et al., 2023).

The heterogeneity of medical devices and SaMD lead to several vulnerabilities. The many types of consumer-grade wearables and SaMD currently on the market and the constant addition of new types make that there is a lack of standardisation of cybersecurity and privacy within the hardware/software. Therefore, there is no interoperability between consumer-grade wearables and SaMD from different manufacturers/software developers. Within healthcare, this means that data flow protocols are different for different types of medical wearables (Hilbel & Frey, 2023). Even though the GDPR for health data is active, the MDR only applies to the SaMD. The hardware of the medical wearable is considered to provide a wellness purpose. Some wearable providers do obtain medical device classification and others keep from this, to mitigate the regulatory requirements that medical devices belong to. This can cause data handling issues for healthcare organisations both in technology and human interaction. Moreover, there are different types of informed consent for users by different types of medical wearables and SaMD.

Additionally, the amount of stakeholders who have access to the data flow in the system is problematic. Third-party partnerships of medical providers for advertisements and other database connections (e.g., via cloud services), leave for a large attack service. These types of unsecured connections can be used to target even a properly secured primary data flow.

2.2.2 Attacker-Oriented Risk (Malicious Intention)

2.2.2.1 Adversarial Dimension

Mancuso et al. (2014) mentions that for the attacker-oriented adversarial dimension, the source and the goals of the attack are combined because these constructs are often difficult to consider independently in practice. Cyberattacks on medical wearables can be targeted at the individual or the healthcare organisations that are involved. Attacker goals of consumer-grade wearables regarding the individual include sensitive information in the form of locations, behavioural patterns, personal identifiable information (PII) (identity theft), and financial information. Cyberattacks focusing on the healthcare sector, are mostly financially motivated, by taking data or infrastructure hostage, and making ransom demands (Williams & Woodward, 2015). The sensitivity of data in the healthcare sector allows for steep demands. Additional motivations for attacks on the healthcare sector include the identification of a particular individual's information or influencing decision-making.

2.2.2.2 Methodological Dimension

The methodological dimension consists of the attack target and the attack vector. The attack target is considered to be the assets of the system. The targets are considered as the vulnerabilities as established in table 3. The attack vector in this orientation includes the particular type of attack used to complete the goal of the attack. For the attack vector, common attacks on consumer-grade wearables and the healthcare sector are considered.

Attackers often use the vulnerabilities associated with the challenge of device constraints. Unsecure WPANs, cloud services, encryption, and authentication controls, allow for a variety of attacks. Prevalent attacks for consumer-grade wearables mentioned in the literature include man-in-the-middle (MITM) attacks, replay attacks, and eavesdropping (Elhoseny et al., 2021). The vulnerability of human factors leads to social engineering attacks being prevalent in the environment (Simonjan et al., 2020) (Ching & Singh, 2016). Ponemon Institute (2023) mention that one of the most prevalent attacks in the healthcare sector is email spoofing of healthcare staff. Kioskli et al. (2023) also finds that social engineering attacks are prevalent in the healthcare sector and examples of frequently used techniques are shoulder surfing, diversion theft, 'dumpster diving', impersonation of help desk calls, phishing, and/or personal blackmailing.

For medical wearables, the data flow is connected to a large supply chain. Attackers use weakly protected third-party partnerships and data storage connections to access the data. In the healthcare sector, supply chain attacks and cloud compromises are prominent (Ponemon Institute, 2023). Supply chain attacks use newly acquired third-party connections and data storage connection vulnerabilities. There is also data inference by malicious attackers from combining information from different database linkages. Attackers can get access to other medical databases and alter/steal medical records. Moreover, inferences from the collected health data like pregnancy, drugs and alcohol use, religion (from location data), and future health problems and mortality, are common (Kounoudes et al., 2023).

2.2.2.3 Operational Dimension

The operational dimension, or the impact of the attacker-oriented risk is further divided into technological, human, and socio-organisational impact. Malicious attacks directly compromise the information security pillars of confidentiality, integrity, and availability. Technologies become inoperable or data inaccessible, the technology runs on faulty data, or the data is unknowingly compromised. The impact when looking at the human dimension includes wrong diagnoses or treatment (resulting in complications or death), delay of treatment, device unavailability, stress, and anxiety (e.g., due to identity theft), financial loss, and loss of privacy (Awotunde et al., 2021) (Ponemon Institute, 2023). The loss of privacy is considered as a loss of control over the data (where and what it is used for) and as too much or unwanted data being collected. For the organisational dimension of healthcare, cyberattacks can cause operational disruptions (patient care), reputational damages, regulatory fines, lawsuits, financial losses due to ransom payments, and loss of trust in the healthcare system (Ponemon Institute, 2023). Additionally, attacks hurt the technology providers as intellectual property (IP) can be lost, possibly resulting in more attacks, and reputation loss and lawsuits can result (Vakhter et al., 2022).

2.2.3 User-Oriented Risk (Non-malicious Intention)

2.2.3.1 Adversarial Dimension

In the adversarial dimension the source of user-oriented risk, human factors are considered. From the literature review, types of human factors include individual and environmental factors. Human factors of users of consumer-grade wearables include lack of awareness, lack of knowledge, and carelessness. Zufferey et al. (2023) examined third-party data sharing in consumer-grade wearables and found that end-users do not have sufficient knowledge about the data flow processes. Zimmer et al. (2020) looked into privacy management of fitness tracker users and found users tend to have a careless attitude towards maintaining data privacy. With the presence of medical jargon and multiple functions in consumer-grade wearables, users' lack of knowledge and awareness are important human factors to consider. Gabriele & Chiasson (2020) looked at fitness tracker users' security and privacy knowledge, attitudes and behaviours. The results show how users behave differently according to the type of information, seeing some types of information as more acceptable for the device to collect and share than others. Users differentiate between more acceptable data such as steps, sleep, and general fitness data, as opposed to personal identifiers or location data. The paper further states that trust in wearable providers is a factor influencing non-secure behaviour in end-users.

Another aspect of human factors is incentives for intentional non-malicious non-secure behaviour by end-users. As stated in section 2.1.3, people often consider the benefits of information sharing/disclosing over their privacy. Literature on consumer-grade wearables shows that an extended privacy calculus exists for the end-user adoption intention considerations (Gao et al., 2015) (Von Kalckreuth & Feufel, 2021) (Schomakers et al., 2022). End-users can consider different benefits of privacy loss. Providing personal information can help to get more accurate results for health monitoring. In addition, sharing information with different applications and devices can increase social benefits for the end-user by adhering to social norms (Rising et al., 2021). Zimmer et al. (2020) found that consumer-grade wearables provide limited privacy features. Furthermore, a lack of motivation in the form of risk underestimation

was found to be present in smartwatch users (Udoh & Alkharashi, 2016). Lupton (2021) found similar results, with end-users of fitness trackers stating that they did simply not expect to be attacked.

2.2.3.2 Methodological Dimension

In the methodological dimension, the 'attack' vector is the non-malicious non-secure behaviour exhibited by valid end-users. From the human-centric risk assessment literature, examples of non-malicious non-secure behaviour are presented in the frameworks of The Chartered Institute of Ergonomics & Human Factors (CIEHF) (2022) and Ferro et al. (2021). Anderson et al. (2023) researched the cyber hygiene of IoT device users by examining the literature on best practices and risky behaviour. He identified relevant behaviour such as choosing weak passwords, disabling security features, not changing the default password, not changing the default settings on devices, not installing software updates, password re-use, placing convenience before security, sharing of too much personal data, and visiting risky websites (such as torrent websites) (Coventry, Briggs, Blythe, & Tran, 2014).

Tu & Gao (2021) state that users of consumer-grade wearables may unknowingly provide informed consent for secondary sharing of information when they sign up for accounts. Gabriele & Chiasson (2020) found that a large amount of fitness wearable end-users do not take proper steps to protect their data against security and privacy threats. Moreover, the paper finds that a large amount of end-users left default privacy settings untouched. Also, they predominantly did not read privacy policies or terms and conditions. A more nuanced view was given on the secure behaviour of setting sharing preferences. End-users were found to be comfortable sharing information with the fitness tracker itself and with friends. Zufferey et al. (2023) found similar results, with end-users not checking privacy settings after setting them up upon the first use of the wearable. This behaviour disregards the dynamic nature of privacy protection. Alqhatani & Lipford (2019) also found that end-users predominantly share data with friends and use social media networks to do so.

2.2.3.3 Operational Dimension

The impact of non-malicious non-secure behaviour includes that attacks are becoming easier and/or have more impact. There is thus extra strain on the security and privacy goals. Sharing of sensitive information leaves digital traces, which can be used by attackers for inferences of data (Piwek et al., 2016). Moreover, data-sharing practices can help to give malicious attackers information to undermine confidentiality, integrity, and availability. For instance, insecure passwords, updating, and patch management leave systems open for attacks. Non-malicious users thus help malicious attackers gain access to the system more easily, or the end-users become the attackers themselves. The latter happens, for instance, when users unintentionally overload systems or improperly dispose of important data.

3

Theoretical Framework

The research now shifts its focus towards establishing the end-user limitations and needs. This chapter outlines the hypotheses and corresponding conceptual research model (section 3.2 for research into the end-user perception of the cybersecurity and privacy system of medical wearables. In the figure 9 below, the focus of this chapter is presented by the black-lined box. 'Concerns' is made up of cybersecurity concern and privacy concern and trades off with positive adoption factors in the adoption intention considerations of end-users.

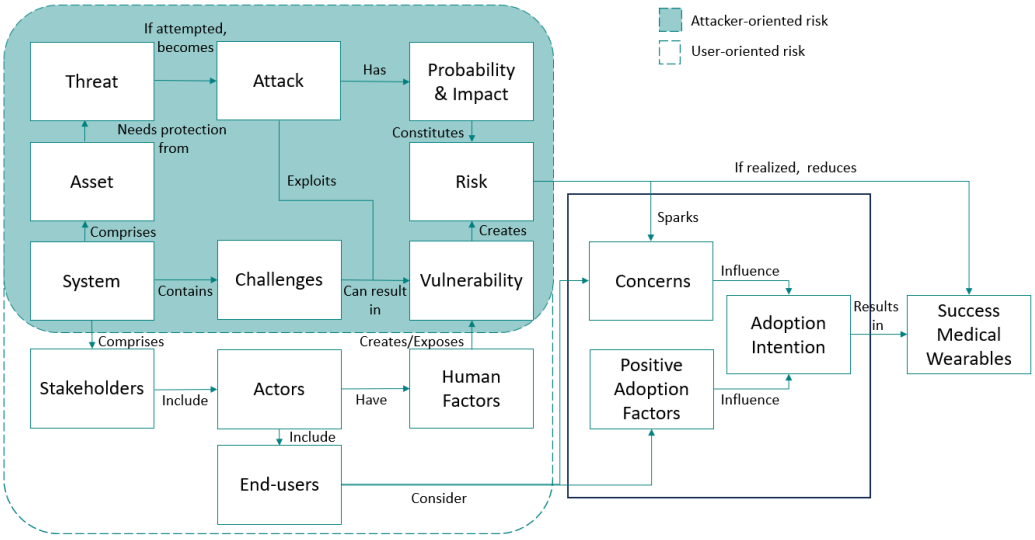


Figure 9: User-centred cybersecurity and privacy environment analysis: user cybersecurity and privacy perception

The user needs are those factors that are important in users' adoption intention considerations. In this research, the needs of end-users for the cybersecurity and privacy system are considered as the impact of attacker-oriented risks. The user limitations are those factors which hinder the user from secure involvement in the cybersecurity and privacy system. As existing literature on consumer-grade wearables points out the existence of a privacy paradox in users' behaviour, the user limitations are not asked out directly. Instead, they will be extracted from the differences between the user needs due to clinical care functionality. In this research, the cybersecurity system is seen as underlying the privacy system, with which end-users directly interact.

The relevant constructs in this chapter are defined with the help of existing literature on privacy calculus and technology adoption theories. The search strategy is mostly equivalent to that of chapter 2. Underlying theories for the constructs are identified while reading literature sources of chapter 2. Literature which helps to inform the relationships and corresponding directions between the different constructs are found with the following search paths:

(UTAUT OR adoption intention OR "privacy calculus") AND ("fitness tracker" OR wearable OR smartwatch OR "medical wearable")

(IUIPC OR trust) AND ("fitness tracker" OR wearable OR smartwatch)

("perceived risk" OR security risk) AND (UTAUT OR "adoption intention") AND ("fitness tracker" OR wearable OR smartwatch OR "medical wearable")

3.1 Research Hypotheses Development

3.1.1 Trust Development

An important factor within the realm of the cybersecurity and privacy environment is the concept of trust. Trust is a psychological state that involves an intention to accept vulnerability based on positive expectations about someone else's intentions or behaviour (Rousseau et al., 1998). In the context of wearables, trust is found to be relevant in the form of trust in the device, trust in the wearable provider and trust in the healthcare system (Bhatt & Chakraborty, 2020). Trust in the provider denotes the willingness of the user to allow a vulnerability in relation to the actions of the provider with the positive expectation that he will transparently carry out a certain action that is important for the user. When a provider fulfils a user's needs, user trust increases (Von Kalckreuth & Feufel, 2021). Increased trust in the provider, can lead to a reduction in the user's uncertainty regarding the (mis)use of personal data and thus increase acceptance of the provider's services and disclosure of their data. Literature on the existing privacy calculus for consumer-grade wearable adoption intention shows that trust in the provider significantly affects the calculus. Thus, the construct of Trust is considered to be relevant for the conceptual research model.

3.1.2 Positive Adoption Factors Development

The positive, traditional adoption factors in the trade-off of figure 9 will be examined by the construct 'Adoption Factors'. The motivation of this construct is end-users' adoption incentives other than cybersecurity and privacy, which influence the cybersecurity and privacy system involvement of users. The basis of this construct comes from research on technology adoption research models. The design of technology adoption theories, in general, is to predict the behaviour of expected users and their acceptance of using new technologies and their usage applications for personal purposes or in working environments. An overview of different research models, based on the scientific field and development method, can be found in table 21 in Appendix A. Both the TAM and UTAUT models are considered suitable models for this construct. Scholars have expressed the existence of a move from TAM to UTAUT in research due to the inherent limitation in the TAM as compared to the UTAUT. The Adoption Factors construct will be based on the UTAUT model, which combines several technology adoption research models, and also has been widely used in privacy calculus and medical wearable adoption research (Schomakers et al., 2022) (Gao et al., 2015) (Hassan et al., 2022) (Enaizan et al., 2020) (Lee & Lee, 2020).

- The unified theory of acceptance and use of technology (UTAUT)
  The wide variety of technology acceptance models led Venkatesh et al. (2003) to combine several of them in the unified theory of acceptance and use of technology (UTAUT) model. This model takes from eight older models of technology acceptance and addresses their limitations. The UTAUT model sees the behavioural intention of the user as the link to actual user behaviour. The model can be seen in figure 10 below. The UTAUT model was further extended by Venkatesh et al. (2012) to include the constructs of Hedonic Motivation, Price Value, and Habit.

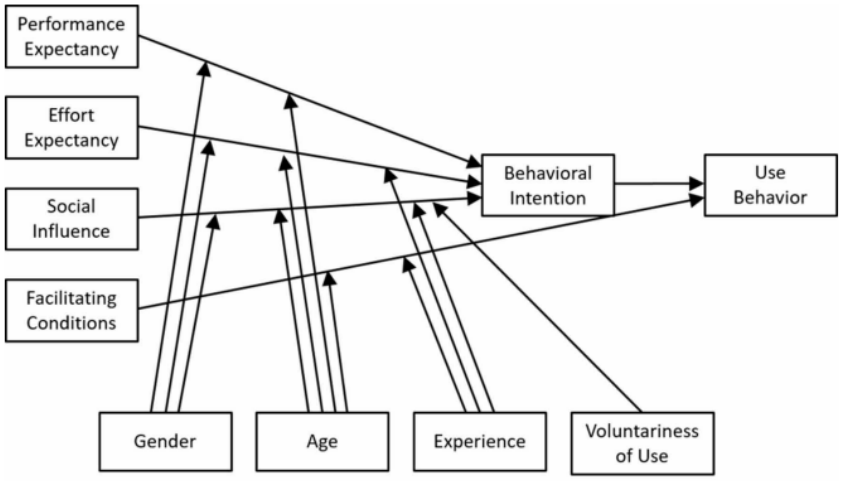


Figure 10: UTAUT adoption model
(Venkatesh et al., 2003)

As the research scope is more focused on the cybersecurity and privacy environment, the 'Adoption Factors' construct is not set out as extensively as in the UTAUT model and its extensions. To still gain insight into the type of positive adoption factors working in the considerations of end-users, the UTAUT factors are considered as separate indicators of the first-order construct 'Adoption Factors'. Performance Expectancy, Effort Expectancy, Facilitating Conditions and Social Influence (human-oriented and brand-oriented) are considered (Beke et al., 2022). Prior research into electronic medical record adoption has considered the constructs of the UTAUT model as 'Individual Factors' that work as a trade-off with cybersecurity and privacy concerns in user perception and found a significant positive relation with the concept of trust and adoption intention (Enaizan et al., 2020). Ben Arfi et al. (2021) looked into the effect of UTAUT and Trust on behavioural intention in the use of IoT in eHealth and found significant positive effects for all factors but Performance Expectancy. Trust was perceived as having an indirect effect on behavioural intention via Perceived Risk. In several research sources, Effort Expectancy is not related to trust (Tanga et al., 2021). However, as it is asked out as an indicator, this research will consider this relation. Consequently, regarding the 'Adoption Factors' construct, the following hypotheses are formed:

H1a: Adoption Factors (AF) will have a direct positive effect on Behavioural Intention (BI)
H1b: Adoption Factors (AF) will have a direct positive effect on Trust (TR)

3.1.3 Concerns About Risk Development

3.1.3.1 Privacy Concern Antecedents

The privacy concern is based on the operational dimension of the attacker-oriented risks and considers the human impact of privacy loss. To be able to measure the privacy concerns of potential end-users of consumer and medical wearables, different theories are considered in the relevant literature. An overview of popular theories of consumer privacy concern can be seen in table 4. The general information privacy concern (GIPC) is a general scale for privacy concern, developed on the basis of strategic theory to capture individuals' concerns about organizational information privacy practices. The concern For information privacy (CFIP) was developed by Smith et al. (1996) to capture the organisations' responsibility in handling customer information by looking into the concepts of collection, improper access, unauthorized secondary use and error. Malhotra et al. (2004) developed the internet users' information privacy concerns (IUIPC) on the basis of the CFIP for application in a network environment. Using this scale, it is easy to demonstrate how end-users' privacy concerns negatively influence their willingness to build relationships with companies based on online practices (Wang et al., 2022). IUIPC is a useful tool for analysing the privacy concerns of online consumers and their reactions to privacy threats when dealing with online practices. The coverage of IUIPC includes and extends that of CFIP. As the scope of the research is end-users' individual privacy perception of a highly network-dependent technology, which functions in the context of a trade-off with positive adoption factors, the decision is made to use the IUIPC. The dimensions of Collection, Control, and Awareness constitute the second-order construct of Privacy Concern.

Criteria	**GIPC**	**CFIP**	**IUIPC**
Purpose	To reflect the level of information privacy concerns in general	To reflect individuals' concerns about organisational privacy practices	To reflect Internet users' concern about information privacy
Focus	No particular focus	Organisations' responsibilities for the proper handling of customer information	Individual's perceptions of fairness/justice in the context of information privacy
Context	Context-independent	Mostly offline or traditional marketing	Mostly online environment
Communication	One-way and two-way communication	Mostly one-way communication	Mostly two-way communication
Dimensions	One-dimensional construct	Collection, improper access, unauthorized secondary use, and error	Collection, control, and awareness
Representations	Single latent variable	Correlated first-order constructs	Second-order construct

Table 4: Privacy concern theories
(Malhotra et al., 2004)

Von Kalckreuth & Feufel (2021) looked at consumer-grade wearables in the extended privacy calculus context and found a negative effect of privacy concern on the intention to use. Enaizan et al. (2020) found privacy concern to have a significantly negative effect on trust and adoption intention of EHR use under healthcare professionals. Schuster & Habibipour (2022) mentions the low trust in wearable providers of consumer-grade wearables as an important factor affecting adoption. Yuchao et al. (2020) looked into health information disclosure practices in mobile health environments and found trust in doctors to have a significant negative effect on privacy concerns. Blagodarny (2017) performed qualitative research into privacy concern and found a positive effect of trust in applications or providers on lack of privacy concern; "One of the explanations given by participants, why they do not have privacy concerns, is trust in company or developer behind the service or application. They did not see a reason why the company would leak their location information to the malicious parties" (p. 39). Because of the ambiguity in the literature about the relation direction between trust and privacy concern, the relation will be examined in both directions and decided on after analysis. The following hypotheses are formed regarding Privacy Concern (PC);

H2a: Privacy Concern (PC) will have a direct negative relationship with Trust (TR)
H2b: Privacy Concern (PC) will have a direct negative effect on Behavioural Intention (BI)

3.1.3.2 Security Concern Antecedents

The other dimension of the 'concern about risk' is security concern. The security concern is based on the operational dimension of the attacker-oriented risks and considers the technological impact. Security Concern as a construct is based on the information security pillars explained in section 2.1.1; confidentiality, integrity, and availability. The concern about these concepts will be used as lower-order constructs to obtain more depth in the findings. Security concern is expected to causally influence the concepts of trust and privacy concern in their contribution to the adoption intention. Namahoot & Jantasri (2022) considered cybersecurity risk as Perceived Risk and found a significant negative effect on trust. The following hypotheses are formed regarding the second-order construct Security Concern;

H3a: Security Concern (SC) will have a direct positive effect on Privacy Concern (PC)
H3b: Security Concern (SC) will have a direct negative effect on Trust (TR)

3.1.4 Clinical Care Functionality

Research has shown that the sensitivity of the data handled by wearables has a positive effect on privacy concern (Bansal et al., 2010) (Eysenbach & Buis, 2021) and influences the privacy calculus. Motti (2015) found that the sensitivity of the data is an important factor in privacy concern. Schomakers et al. (2022) looked at the extended privacy calculus theory in the context of smart technologies and found a significant positive effect of information sensitivity on privacy concern. Gao et al. (2015) compared fitness wearables and medical device user perceptions and found that perceived privacy concern had a significantly positive effect on the negative relation with behavioural intention. In the conceptual research model, it is thus expected that clinical care functionality will significantly positively affect the negative relationship between Privacy Concern and Behavioural Intention. On the other hand, clinical care functionality adds another layer to consumer-grade wearables and thus also affects the Adoption Factors construct. Gao et al. (2015) found that performance and effort expectancy were significantly more important in the adoption intention in the medical device group compared to the fitness device group. However, facilitating conditions and social influence were found to be less important for the adoption intention of medical wearable users. When looking at the respective differences between the two groups, these two factors are considered to have more effect on the differences in the importance of the Adoption Factors construct in the adoption intention. The relationships regarding the Trust construct are not expected to change. Bansal et al. (2010) found no relation between privacy concern and trust based on information sensitivity.

H4a: Clinical care functionality will have a significant positive effect on the negative relationship between Privacy Concern (PC) and Behavioural Intention (BI)
H4b: Clinical care functionality will have a significant negative effect on the positive relationship between Adoption Factors (AF) and Behavioural Intention (BI)

3.2 Conceptual Research Model

The hypotheses on the relationships between the constructs form the basis of the research into the end-user perception of the importance of cybersecurity and privacy concerns for the adoption intention regarding medical wearables. Furthermore, the clinical care hypotheses form the basis of the research into the effect of clinical care functionality on the end-user perception. The resulting conceptual research model can be seen in figure 11 below. The model is leading for the following chapters 4 and 5.

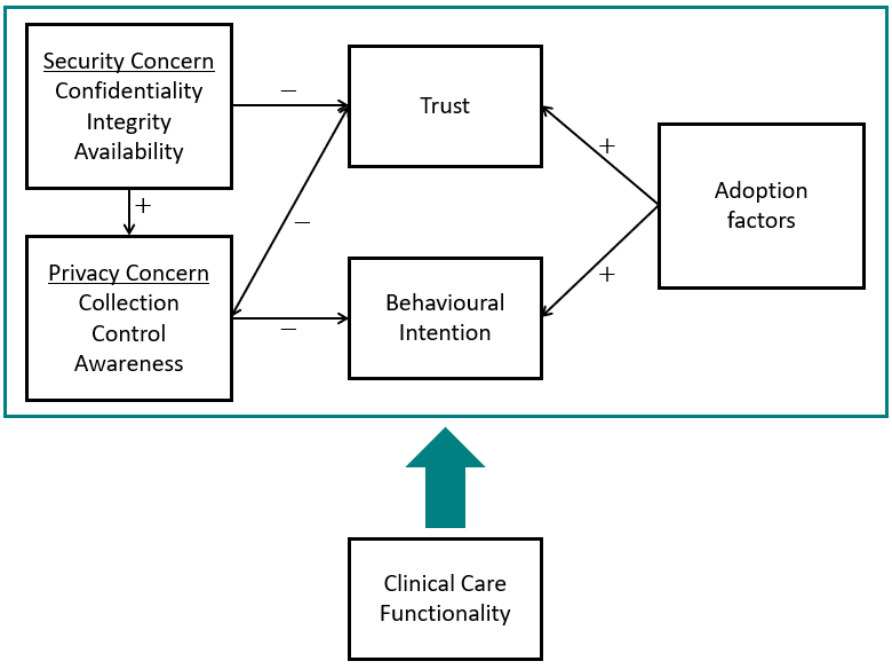


Figure 11: Conceptual research model

4

Methodology

In this chapter, the methodology of the research looking into the relationships of the conceptual research model of chapter 3, is outlined. In section 4.1 the research approach is considered, where the conceptual research model presented in figure 11 is leading. The section establishes the use of a quantitative survey method in the form of a web-based electronic questionnaire carried out under potential adult end-users of medical wearables in the Netherlands. Section 4.2 states the data analysis methods the research uses. The section explains the use of structural equation modeling (SEM), multigroup analysis (MGA) and importance-performance mapping analysis (IPMA). Moreover, it includes justifications for several choices made in SEM. After consideration of various methods, an aspired sample size of 146 was established. The sampling strategy is outlined in section 4.3. The results of a pre-test of the questionnaire are examined in section 4.4.

4.1 Research Approach

4.1.1 Quantitative Research Approach

To conduct the research on the conceptual research model established in section 3.2, a quantitative research approach is chosen. Aliaga & Gunderson (2002) define quantitative research as the explaining of an issue or phenomenon by gathering data in numerical form and analysing with the aid of mathematical methods, particularly statistics. The purpose of quantitative research is to test hypotheses, look at cause and effect, and make predictions (Johnson & Christensen, 2008). The research strategy chosen is survey research. Survey research is a suitable and scalable method to gain insight into people's behaviour. The unit of analysis of the research is individuals and the research is non-contrived. As we are interested in the user perception of medical wearables, the target population of the survey research is potential adult end-users of medical wearables in the Netherlands.

4.1.2 Questionnaire

A web-based electronic questionnaire is used as the data collection method, collecting information on the relationships between the different constructs in the conceptual research model. Due to the limited amount of time, a cross-sectional questionnaire is the best type of research method for this research, since the data can be gathered at one moment in time and from one group (Sekeran & Bougie, 2016). The items of the questionnaire are on an interval and rating scale; the Likert scale. The Likert scale is designed to examine how strongly subjects agree or disagree with statements on a five-point scale. This scale allows for measuring attitudes, beliefs, and perceptions. Advantages of web-based electronic questionnaires include fastness of delivery, the ability to reach wide geographic regions, and low costs. Disadvantages to keep in mind during the research are a low response rate, an inability to clarify questions, and the fact that web-based electronic questionnaires are often perceived as spam.

The introduction of the questionnaire contains information about the background, purpose and data-handling practices of the questionnaire. Firstly, the questions regarding demographic variables are presented. These questions allow for the assessment of the representativeness of the collected sample, as well as give insight into significant differences based on age, gender, and experience with consumer-grade wearables. After the introductory section, the research model items are asked out. The research model will be asked out twice (items will have a general 'wearable' variant and a 'wearable with a clinical care purpose' variant), which substantially increases the number of potential items to be considered. The amount of items for the lower-order constructs is therefore taken to be minimal (2 per construct) to keep a reasonable completion time for the questionnaire of approximately 7 minutes. To still keep some depth of the 'Adoption Factors' construct, based on the UTAUT model, the 5 items mentioned in section 3.1.2 are kept. The 21 unique items of the questionnaire can be seen in the Appendix B. The items are randomized throughout the questionnaire to reduce the correlation of error terms and increase overall reliability (D. Goodhue & Loiacono, 2002).

To further reduce bias, the items for clinical care functionality and without are also randomized. Several items are put in a negative form to reduce the chance of repeat bias (Sekeran & Bougie, 2016). The questionnaire was first written in English and subsequently translated into Dutch. The risk assessment and informed consent of the questionnaire were approved by the Human Research Ethics Committee (HREC).

4.2 Data Analysis

After the data is collected from the questionnaire, data analysis is performed. The data analysis of quantitative research is done to identify statistical relationships. The collected data will be analysed with the use of the software packages SPSS Statistics and SmartPLS 4.0. The survey data will be divided into Study 1 which examines the consumer-grade wearable perception and Study 2 which examines the medical wearable perception.

4.2.1 Structural Equation Modeling

One of the most suitable methods of processing non-parametric data to test hypotheses is structural equation modeling (SEM) (Hair et al., 2013). This technique is a combination of factor analysis and multiple regression analysis and is used to analyse the structural relationship between measured variables and latent constructs. The SEM technique employed in the research is based on the two-step approach (Henseler et al., 2009). First, a lower-order measurement model is established, which includes the first-order constructs. The first-order constructs presented in the conceptual research model are analysed by factor analysis to obtain reliability and validity of the relation between items and constructs. Hereafter, the second-order constructs are checked for reliability and validity. This concludes the steps taken to assess the measurement model. After this, structural modelling is performed on the higher-order model by assessing the path coefficients, variance explained, and predictive relevance.

4.2.1.1 Factor Analysis

In SEM, there are two ways of carrying out the factor analysis; exploratory factor analysis (EFA) and confirmatory factor Analysis (CFA). The details of both methods are set out in table 5 below. The most suitable method for this research is CFA, as the conceptual research model includes prespecified constructs and seeks to confirm a preconceived theory (Chapter 3). In the case of low factor loadings of items, EFA could give some insight into the root of this. CFA will be performed in SmartPLS 4.0.

Criteria	**EFA**	**CFA**
Research goal	Explores the data and provides the researcher with information about how many factors are needed to best represent the data	Tests whether the theoretical pattern of factor loadings on prespecified constructs (variables loading on specific constructs) represents the actual data
Construct building	All measured variables are related to every factor by a factor loading estimation by statistical software	A theory is used to associate variables with the corresponding construct
Preconceived theory	The researcher does not know how many factors/constructs and set of variables exist	The researcher knows how many factors/ constructs and set of variables exist
Results	It does not confirm the preconceived theory	It confirms the preconceived theory
Cross-loading	Cross-loadings are potential	There are no cross-loadings

Table 5: Factor analysis techniques
Adapted from Hair et al. (2013)

To determine if the sample is appropriate for factory analysis, both a Kaiser-Meyer-Olkin (KMO) analysis (Tabachnick & Fidell, 2014) and Bartlett's test of sphericity (Hair et al., 2013) are performed on the survey data to indicate the acceptance level of sampling adequacy. This is done for both the consumer-grade wearable study and the medical wearable study. The KMO measure is a test to assess the appropriateness of using factor analysis on the data set. It ranges from 0 to 1 and 0.60 is suggested as a minimum for good factor analysis. Bartlett's test of sphericity is used to test the null hypothesis that the variables in the population correlation matrix are uncorrelated. The significance value of this test should be <0.05.

4.2.1.2 Mulitple Regression Analysis

The other dimension of SEM is multiple regression analysis. The objective of multiple regression analysis is to predict the changes in the dependent variable in response to changes in the independent variables. This technique generally consists of two possible approaches which are presented in table 6 below.

Criteria	PLS-SEM	CB-SEM
Research goal	Predicting key target constructs or identifying key 'driver' constructs. To test the prediction effects and model hypotheses through constructs or latent variables	Theory testing, theory confirmation, or comparison of alternative theories. To understand the model in order to measure the accuracy level of model representation by its measured indicators.
Data characteristics	No assumption on normality data and robustness can be achieved with missing values	Requires normally distributed data and is sensitive to missing data
Constructs	Reflective and formative	Mainly reflective
Sample size	Small (min. 30-100)	Large (min. 200-800)

Table 6: Multiple regression analysis techniques
Adapted from Clement (2019)

The research aims to predict and explain the variance in key target constructs and the conceptual research model has a certain level of complexity. Using PLS-SEM will allow the research to adopt the advantages of the method in terms of less rigorous requirements of restrictive assumptions (Hair, Sarstedt, et al., 2014). PLS-SEM does not make any assumptions regarding the distribution of the data, which allows for analysis of non-normally distributed data. In addition, the time constraint of the research will have an effect on the possible sample size of the research. Therefore, the research will be done on the basis of PLS-SEM with the program SmartPLS 4.0.

4.2.2 Measurement Model: Reflective Constructs

The data analysis of the measurement model is different for formative and reflectively-formed constructs (Sarstedt et al., 2019). Reflective constructs are constructs that are made up of interchangeable indicators. Behavioural Intention and Trust are measured in this way. Privacy Concern is by definition of the IUIPC a reflective-reflective second-order construct. Formative constructs contain indicators that are not interchangeable and each establishes a different aspect of the construct. The research considers both the indicators of 'Adoption Factors' and those of the second-order 'Security Concern' construct to be defined in this way. Reflective constructs are assessed by checking individual item reliability, internal item consistency, and establishing convergent and discriminant validity. Formative constructs are assessed by establishing convergent validity, assessing multicollinearity issues, and checking the significance and relevance of outer weights. SmartPLS 4.0 includes confirmatory tetrad analysis (CTA) which can be used to check whether constructs are better defined formatively or reflectively. However, as the formation of the constructs in the conceptual research model is based on preconceived theory, this will not be part of the initial data analysis.

4.2.2.1 Reliability Testing

The reliability of a measure indicates the extent to which it is without bias and hence ensures consistent measurement across the various items (Sekeran & Bougie, 2016). It is an indication of the stability with which the survey measures concepts and helps to assess the 'goodness' of a measure, in this case, of the constructs. To this end, individual item reliability and internal item consistency can be checked.

- Individual item reliability is established by checking factor loadings of items. Hair, Hult, et al. (2014) recommend factor loadings of individual items higher than 0.5. If the individual item factor loading is higher than 0.4 but smaller than 0.5, the internal item consistency and convergent validity can be checked to look whether dropping the item increases reliability and/or validity.
- Internal item consistency can be tested with a Cronbach's coefficient alpha test for the constructs (Cronbach, 1946). Another method is to examine composite reliability (CR) (Hair, Hult, et al., 2014). This measure of reliability takes into account the different outer loadings of the indicator variables, as not all items are expected to affect constructs the same way.

Cronbach's alpha is a conservative measure of reliability (i.e., it results in relatively low-reliability values), while CR tends to overestimate internal consistency reliability. When analyzing and assessing the measures' internal consistency reliability, the true reliability usually lies between the two criteria (Hair, Hult, et al., 2014). Both criteria have a threshold value of 0.6 being acceptable and 0.7 for good reliability. As the questionnaire randomization is expected to substantially decrease Cronbach's alpha coefficients for the constructs but increase overall structural reliability (D. Goodhue & Loiacono, 2002), the internal item consistency will be established with the CR criterion.

4.2.2.2 Validity Testing

The validity of a measure indicates the extent to which it is measuring the concept we set out to measure and not something else (Sekeran & Bougie, 2016). Content validity is defined as the extent to which a measure includes an adequate and representative set of items that tap the concept. The more the scale items represent the domain or universe of the concept being measured, the greater the content validity. Construct validity is defined as the extent to which the results obtained from the use of the measure fit the theories around which the test is designed. There are two types of construct validity; convergent and discriminant validity. Convergent validity is established when the scores obtained with two different instruments (indicators/items) measuring the same construct are highly correlated. Discriminant validity is the extent to which a construct is truly distinct from other constructs by empirical standards. Discriminant validity thus establishes that a construct is unique and captures phenomena not represented by other constructs in the model.

- To ensure content validity, a pre-test of the questionnaire with 6 people from the target population will be carried out. There is no prescribed sample size for pre-testing, but often sizes of 15-30 are advised (Burns & Grove, 2005). Due to the time constraint and robust underlying theories, a smaller pre-test sample size is taken. Based on the feedback, modifications will be made to make the questionnaire clearer and possibly items lacking relevance will be deleted. This helps to identify inadequacies before conducting the questionnaire with the real sample and helps to reduce bias.
- Convergent validity is established with the average variance extracted (AVE). This criterion is defined as the grand mean value of the squared loadings of the indicators associated with the construct (i.e., the sum of the squared loadings divided by the number of indicators). A construct having an AVE value of 0.5 or higher, establishes the construct's convergent validity. The AVE is often considered together with CR for an overall view of the appropriateness of variables. The AVE criterion is used for both the reflective and formative construct convergent validity.
- Discriminant validity can be assessed with the use of the Fornell-Larcker criterion, checking cross-loadings, and the heterotait-monotrait (HTMT) criterion. The Fornell-Larcker criterion states that the square root of the Average Variance Extracted by constructs should be greater than the correlation coefficients between those constructs for adequate discriminant validity (Fornell & Larcker, 1981). In addition, cross-loadings can be checked, where the loading of the indicators on their own construct, should be higher than for other constructs. The HTMT criterion uses the correlations between items instead of cross-loadings and uses a threshold value of <0.9. PLS-SEM literature highly recommends using the HTMT criterion for establishing discriminant validity as checking Fornell-Larcker and cross-loadings can give a distorted view of discriminant validity (Henseler et al., 2015). If discriminant validity is not established, the recommended procedure is to check cross-loadings and look if indicators of a construct load on another construct with less than 0.1 difference from their own construct (Hair, Hult, et al., 2014). If this is the case, it is recommended to delete the problematic item. If no problems arise in the cross-loadings, and the HTMT is still >0.9, it is suggested to combine constructs as respondents did not see the two constructs as two distinct concepts. In SmartPLS 4.0, the HTMT is measured using absolute values, tackling counteracting negative and positive correlations (HTMT+). The HTMT tends to be upward biased for the case of constructs not being tau-equivalent (as in most empirical research) and the correlation between the constructs approaches 1.0. In this case, it may be better to rely on a modified coefficient, the HTMT2 (Roemer et al., 2021). This research will use the HTMT criterion to establish discriminant validity and check HTMT2 values and subsequently cross-loadings if problematic HTMT values arise.

4.2.3 Measurement Model: Formative Constructs

4.2.3.1 Multicollinearity

Multicollinearity is a problem in multiple regression modelling because it indicates independent variables are influencing each other and thus, the relationship between the indicators and the constructs can not be properly assessed. There

is no way to know how much the combination of the independent variables affects the dependent variable (construct). The multicollinearity of formative indicators is checked with the Variance Inflation Factor (VIF). Hair, Hult, et al. (2014) suggests the VIF should be <3.0 to ensure that there are no multicollinearity issues among the formative indicators.

4.2.3.2 Outer Weights

The equivalent of factor loading for reflective constructs is the checking of outer weights for formative constructs (Henseler et al., 2021). Outer weights of significance <0.05 are considered relevant for the construct. If significance is not established, outer loadings (factor loading) should be checked. If the outer loading of an indicator is less than 0.5, the item should be considered for removal. However, the item can possibly be maintained if it is deemed theoretically relevant or if it still performs well within the higher-order structural model. If the significance of the outer loading is also below the threshold value of 0.05, the item needs to be removed.

4.2.4 Measurement Model Fit

The significance of the evaluation of the goodness-of-fit for PLS-SEM models is under debate and needs more research. SmartPLS 4.0 provides the Standardized Root Mean Square Residual (SRMR) as a way to establish model fit for PLS-SEM models. The SRMR is based on a CB-SEM model fit criterion and is defined as the difference between the observed correlation and the model implied correlation matrix. Thus, it allows assessing the average magnitude of the discrepancies between observed and expected correlations as an absolute measure of (model) fit criterion. A SRMR of <0.9 is considered to be acceptable. The research will provide the SRMR for the model fit of the measurement model only.

4.2.5 Structural Model

4.2.5.1 Path Relevance

For the structural model, the most important evaluation metric is the size and statistical significance of the structural path coefficients. To this end, the Bootstrapping technique will be used. A path coefficient with a significance value of <0.05 is considered to indicate a relevant and reliable relationship. A two-tailed t-test approach is used.

4.2.5.2 Explained Variance

The explained variance will be examined with the coefficient of determination R^2. The explained variance is not to be seen as a way to assess model fit in PLS-SEM. According to Hair, Sarstedt, et al. (2014), R^2 values of 0.75 or above are substantial, 0.5 are moderate, and 0.25 are weak for endogenous constructs in the structural model.

4.2.5.3 Predictive Capability

The predictive relevance is analysed with the use of PLSpredict and cross-validated predictive ability testing (CVPAT) techniques. In PLSpredict, the Q^2 value is determined. If the Q^2 value is positive, the prediction error of the PLS-SEM results is smaller than the prediction error of simply using the mean values. In that case, the structural model offers better predictive performance. The CVPAT is an out-of-sample prediction approach to calculate the model's prediction error, which determines the average loss value. This average loss value is compared to the average loss value of a prediction using indicator averages or the average loss value of a linear model. The structural models' average loss should be lower than that of these benchmarks. The difference in the average loss values should be significantly below zero to indicate better predictive capabilities of the model compared to the prediction benchmarks. CVPAT can be used to compare models for predictive power. In the case of the relation between Privacy Concern and Trust, the CVPAT will be used to determine the direction of the relationship.

4.2.6 Comparison Structural Models

The PLS-SEM literature is not extensive on the comparison of two separate models for paired samples. A recommended method is to look for significant differences between confidence intervals, as provided by Cumming & Finch (2005). The authors suggest testing for less than 50% overlap in the 95% confidence intervals of the path coefficients. This means that, approximately, the upper limit of the lower mean CI must be lower than the midpoint of CI of the higher mean.

4.2.7 Multigroup Analysis

The research will examine if there are significant differences in the path coefficients based on age, gender and experience with consumer-grade wearables. This will give insight into the differences in the effect of clinical care functionality on the perception of potential end-users. To look at statistical differences between groups of respondents of the PLS-SEM model, multigroup analysis (MGA) is used. MGA is an approach that has been broadly used for group comparisons. It is a set of advanced techniques that are usually applied when researchers want to examine differences between categorical variables (e.g., gender and countries) or continuous variables that can be categorized through a dichotomization process or cluster analysis (Hair, Hult, et al., 2014). The research will use the PLS-MGA approach which is a non-parametric-based significance test for the difference of group-specific results that builds on PLS-SEM bootstrapping results. PLS-MGA relies on pairwise comparisons. Before the MGA results can be determined, a MICOM invariance test is conducted to establish that the significance of the difference do not stem from differences in the constructs across groups. This consists of three procedures; configural invariance, compositional invariance, and equal distribution of mean values and variances of composites. For MGA with more than two groups, the pairwise comparisons are carried out for all combinations in the groups and then corrected for family-wise error with Šidák's adjustment of the p-value in the MICOM test (Cheah et al., 2023). Before the start of the factor analysis, the groups will be generated in the data set.

4.2.8 Importance-Performance Mapping Analysis

From a business perspective, research constructs are associated with pursuing goals and managerial decisions that deserve careful attention regarding their importance and performance. The total effect of the constructs indicates their importance in shaping a specific target construct. This importance dimension can be complemented by considering the rescaled average latent variable scores as a performance dimension. By doing so, an Importance-Performance Map analysis (IPMA) can be conducted (Hair et al., 2018). The goal of IPMA is to identify predecessors with a relatively high total effect and a relatively low average latent variable score. To this end, the Importance-Performance map is divided into four quadrants by the mean values of the importance and performance values. The constructs with relatively high importance and low performance are principal areas in which improvements can be made and thus should be a focus of management activities. IPMA plots present the importance on the x-axis and performance on the corresponding y-axis. The IPMA analysis will also be conducted in Smart-PLS 4.0 and will be performed on both construct and indicator (questionnaire item or first-order construct) level. The indicator-level IPMA can be used to obtain in-depth information on defining indicators for constructs (in the case of reflective constructs) or the contribution of different indicators to a construct (in the case of formative constructs).

4.3 Sampling

4.3.1 Sampling Approach

The sample is a subset of the target population. The target population of the research consists of potential adult end-users of medical wearables in the Netherlands. The sampling approach is a non-probability sampling in the form of convenience sampling. The questionnaire is spread out to friends, family, and colleagues by mail and WhatsApp and asked to spread further with close acquaintances. Personal messages are included to increase the response rate and to reduce the perception of spam.

4.3.2 Sample Size

The sample size was determined by examining the literature on both CFA, PLS-SEM and IPMA sample size criteria. For CFA, a range of 5-10 respondents per indicator is recommended (Hair et al., 2013). As the questionnaire consists of 21 indicators per model, this would result in 105 people in the sample. For PLS-SEM several methods are considered. Originally, a popular method for determining the sample size for PLS-SEM was the 10-times rule (Kock & Hadaya, 2018). This rule states that the sample size should be greater than 10 times the maximum number of inner or outer model links pointing at any latent variable in the model (D. L. Goodhue et al., 2012). This means the sample size does not depend on the magnitude of the path coefficients in the model. This often leads to significantly inaccurate estimations of the minimum required sample size. In response to this, other methods were developed that do take into account path coefficients.

The minimum R-squared method, which builds on power tables for least squares regression (e.g., Cohen (1988)), relies on a table listing minimum required sample sizes based on three elements. The first element of the minimum R-squared method is the maximum number of arrows pointing at a latent variable in a model. The second is the

significance level used and the third is the minimum R-squared in the model. This method unfortunately also often leads to inaccurate estimations. In response to this, the inverse square root method was developed.

The inverse square root method is based on the relation between the path coefficient and the standard error. As the magnitude of the path coefficient and of the sample size analysed increase, the probability that the ratio will surpass a critical ratio of path coefficient to standard error will increase. As a result, the likelihood that an effect that does exist at the population level will be mistakenly rejected, will decrease. The minimum sample size with this method is estimated as the smallest positive integer that satisfies equation 1. The gamma exponential method helps the bias in the standard error by using an exponential smoothing function correction in the context of PLS-SEM for sample sizes greater than those covered by the gamma function correction (N>10) (Kock, 2014). Therefore, research uses the gamma exponential method as a sample size estimator.

$$\hat{N} = (\frac{2.486}{|\beta_{min}})^2 \tag{1}$$

$$\hat{S} = \frac{1}{\sqrt{N}} e^{-(\frac{e|\beta|}{\sqrt{N}}} \tag{2}$$

Kock & Hadaya (2018) state an approach for the minimum number of sample size before data collection and knowledge on minimum magnitude path coefficients, for both the Inverse Square method and the Gamma Exponential method. As a complex model would tend to lead to lower effect sizes because such models would likely include more competing links, a target effect size of 0.04 is acceptable. This rule of thumb was checked with Monte Carlo simulations and found to be valid for fairly complex models. The effect size leads to a path coefficient of $\beta \geq .197$. For the Gamma Exponential method, the minimum required sample size for this path coefficient was determined to be 146, which will be this research its aspired sample size.

4.4 Pre-test Modifications & Considerations

The pre-test of the questionnaire resulted in several modifications to the design and content of the questionnaire. Reminders were added above each statement list page, to keep respondents alert of the two studies being performed. Exemplary information was given for some statements to make them more easily recognizable and some statements were reworded in the Dutch variant to make them more understandable for general audiences. The pre-test also showed high conceptual relationships between the privacy and security statements. This means establishing the discriminant validity of the questionnaire might become a troubling area of the data analysis that should be approached with care.

4.5 Cluster Analysis

The expert review in the form of a brainstorming session brought about several data analysis considerations and a suggestion for additional cluster analysis. Using SPSS, the data of both studies is subjected to k-means cluster analysis. To check whether distinct cluster groups are considered to be present within the data, the number of iterations are checked. If the iterations converge to 0 in less than 10 iterations, this is a good first indicator of significant clusters. The significance of the ANOVA table is checked to be less than 0.05. Confirming the distinctive characteristics of clusters identified by the cluster analysis, a one-way ANOVA employing a Bonferroni post-hoc test for the entered indicators and the clusters is done and checked for significance <0.05 for each of the indicators.

If different clusters are established, linear regression is performed on the cluster classifications for the different user segments of gender, age and consumer-grade wearable experience. The results are checked by the significance of the ANOVA table. Moreover, if significant clusters are established, an additional MGA based on the cluster classifications is performed to check for significant differences in the path coefficients of the structural model.

5

Analysis & Results

This chapter outlines the data analysis and interpretations of the survey research regarding the potential end-user perception of medical wearables. The chapter follows the data analysis as described in chapter 4. In section 5.2, the assessment of the measurement model is performed, whereafter, in section 5.3 the hypotheses of the conceptual research model developed in chapter 3 are examined with the structural model assessment. From this section onward, interpretations will be given about the analyses of both studies and the differences between them. In section 5.4, the MGA analysis is performed for user groups based on gender, age and consumer-grade wearable experience. The IPMA analyses on both Behavioural Intention and Privacy Concern are performed in section 5.5. The results presented in this section are reviewed by two experts regarding the data analysis and research topic. The summary of this review can be found in Appendix D. In section 5.6, an addition to the data analysis in the form of cluster analysis is performed. The five-step approach used in this chapter is presented in figure 12. In this chapter subquestion 2; 'How do users' privacy and cybersecurity concerns influence their intention to adopt consumer-grade wearables for clinical care purposes?' is answered.

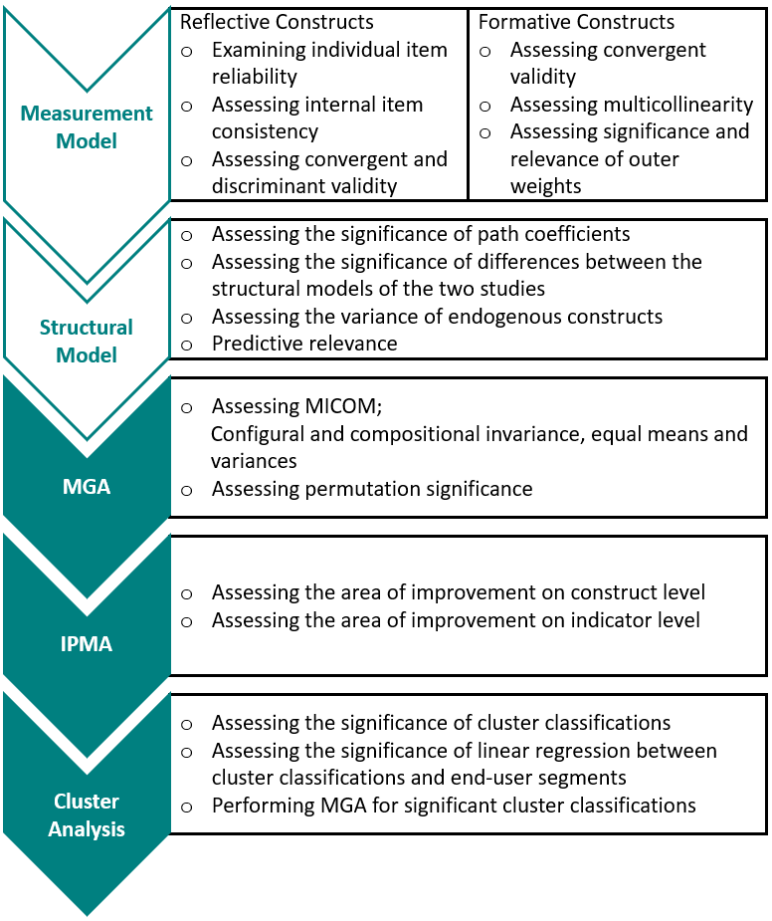


Figure 12: Data analysis path of the survey research

5.1 Descriptive Statistics

A total of 155 responses were recorded, which was above the aspired 146 as established in section 4.3.2. The demographic details can be found in table 7. From the 'User' group (respondents who currently own a consumer-grade wearable), the length of the experience and the type of wearable owned were recorded. The sample is well-distributed within all statistical groups. The age group of 70 years or older is considered high enough for the MGA (N>10).

Item	Details	Number	Percentage
Gender	Male	72	46.5%
	Female	82	52.9%
	Other/Rather not say	1	0.6%
Age	25 years and under	39	25.2%
	26-40 years	28	18.1%
	41-54 years	21	13.5%
	55-69 years	55	35.5%
	70 years or older	12	7.7%
Experience	Non-user	92	59.4%
	User	63	40.6%
Length of experience	Less than 1 year	15	23.8%
	1-2 years	10	15.9%
	Over 2 years	38	60.3%
Type of wearable use	Smartwatch	37	58.7%
	Activity tracker	22	34.9%
	Other	4	6.4%

Table 7: Descriptive sample details

5.2 Measurement Model

The data collected from the survey has been divided into Study 1; the consumer-grade wearable model (without clinical care functionality) and Study 2; the medical wearable model. The Kaiser-Meyer-Olkin (KMO) test and Bartlett's test of sphericity were applied to the data of Study 1 and Study 2. Study 1 had a KMO of 0.833, which is above the cut-off value of 0.6, and a Bartlett's test significance of $p<0.001$. Study 2 had a KMO of 0.844 and a Bartlett's test significance of $p<0.001$. Therefore, both studies were determined suitable for factor analysis.

5.2.1 Reliability & Validity Reflective Constructs

The results of the reliability and validity analyses of the measurement model resulted in several necessary adjustments to the model. First, the reflective lower-order constructs were examined. The resulting, original factor loading (FL), composite reliability (CR) and average variance extracted (AVE) of the constructs can be seen in table 23 in Appendix C. The first criterion in the table is the Factor Loading (FL), which varies between -1.0 and +1.0. A higher absolute value of the factor loading indicates a higher correlation of the item with the underlying construct. Hair, Hult, et al. (2014) recommend a factor loading value of at least 0.5 for relevance. It is useful to check whether the dropping of items can improve the reliability and validity of the model. Indicators IN2 and AV2 were dropped because of low factor loadings in combination with low CR and AVE values.

The lower-order constructs of Collection and Control showed high discriminant validity issues. This means respondents could not significantly distinguish the two constructs as separate concepts. However, the cross-loadings showed no problems. Hair et al. (2018) recommends combining the two constructs into one and using this one construct for the formation of the higher-order construct. This new construct is called 'C'. After combining the constructs, Confidentiality still had discriminant validity issues with the combined construct C. This could be due to the highly related nature of the concepts of confidentiality and privacy. The cross-loadings are examined to see if indicators of Confidentiality load on C better than on their own construct or vice versa. CO2 loads higher on C than CO and

was therefore removed from the model. After this procedure, discriminant validity by means of the HTMT criterion was established. The subsequent paragraphs present the final model's reliability and validity analyses. Because of the adjustment of the model, Security Concern effectively has become a first-order formative construct. However, the original first-order constructs are still included in the HTMT criterion assessment to show the constructs now do have discriminant validity with the first-order constructs of Privacy Concern.

5.2.1.1 Individual Item Reliability, Internal Item Consistency & Convergent Validity

For the final model, the establishment of internal item reliability, in the form of FL>0.5, can be seen in table 8 below. This table also includes the establishment of internal item consistency and convergent validity, through the values of CR and AVE being higher than the threshold values of 0.7 and 0.5 respectively. In table 9, the same concepts of reliability and validity are established for the higher-order reflective construct of Privacy Concern.

Construct	Item	FL	CR	AVE
Behavioural Intention	BI1	.815	.818	.692
	BI2	.848		
Trust	TR1	.929	.904	.825
	TR2	.888		
Collection and Control	CL1	.828	.851	.590
	CL2	.710		
	CN1	.693		
	CN2	.832		
Awareness	AW1	.917	.876	.780
	AW2	.848		

(a) Study 1

Construct	Item	FL	CR	AVE
Behavioural Intention	BI1	.814	.853	.744
	BI2	.909		
Trust	TR1	.879	.821	.697
	TR2	.788		
Collection and Control	CL1	.771	.868	.624
	CL2	.757		
	CN1	.745		
	CN2	.879		
Awareness	AW1	.902	.841	.726
	AW2	.800		

(b) Study 2

Table 8: Reliability & validity lower-order reflective constructs

Construct	Item	FL	CR	AVE
Privacy Concern	C	.939	.904	.824
	AW	.876		

(a) Study 1

Construct	Item	FL	CR	AVE
Privacy Concern	C	.940	.891	.804
	AW	.851		

(b) Study 2

Table 9: Reliability and validity higher-order reflective construct Privacy Concern

5.2.1.2 Discriminant Validity

The discriminant validity is assessed with the recommended HTMT criterion which can be seen in table 10 and table 11. All the values are below the threshold value of 0.9 and discriminant validity is established for lower-order and higher-order constructs in both studies.

	BI	TR	C	AW	CO	IN	AV
BI							
TR	0.424						
C	0.394	0.483					
AW	0.169	0.230	0.869				
CO	0.211	0.341	0.817	0.654			
IN	0.169	0.439	0.851	0.665	0.804		
AV	0.116	0.103	0.358	0.300	0.339	0.323	

(a) Study 1

	BI	TR	C	AW	CO	IN	AV
BI							
TR	0.474						
C	0.294	0.693					
AW	0.124	0.259	0.851				
CO	0.223	0.415	0.717	0.536			
IN	0.273	0.570	0.877	0.686	0.627		
AV	0.103	0.132	0.459	0.354	0.354	0.408	

(b) Study 2

Table 10: Discriminant validity lower-order reflective constructs - HTMT criterion

	BI	TR	PC
BI			
TR	.424		
PC	.295	.398	

(a) Study 1

	BI	TR	PC
BI			
TR	.474		
PC	.185	.532	

(b) Study 2

Table 11: Discriminant validity higher-order reflective constructs- HTMT criterion

5.2.2 Reliability & Validity Formative Constructs

The formative constructs are assessed with the use of the significance of the outer weight, if not established, the outer loadings and their significance are checked. Additionally, multicollinearity is checked for the indicators. The results can be found in table 12. The only insignificant outer weight in both studies is that of the Availability indicator. For both studies, the outer loading of AV is significant. In Study 1, the *p* value is 0.010 and in Study 2 0.000. The significance of the outer loadings means that the Availability indicator is up for consideration to be removed. As the construct is an important part of the preconceived theory, the decision is made to keep Availability as a formative indicator of Security Concern and to use it in the structural model.

Construct	Item	OW	*p*-value	VIF
Security Concern	CO	0.344	0.023*	2.879
	IN	0.727	0.000***	2.847
	AV	-0.078	0.302	1.139
Adoption Factors	AF1	0.257	0.006**	1.010
	AF4	0.328	0.002**	1.128
	AF5	0.792	0.000***	1.118

(a) Study 1

Construct	Item	OW	*p*-value	VIF
Security Concern	CO	0.265	0.003**	1.681
	IN	0.807	0.000***	1.764
	AV	0.011	0.879	1.223
Adoption Factors	AF1	0.310	0.013*	1.258
	AF4	0.562	0.000***	1.315
	AF5	0.451	0.000***	1.134

(b) Study 2

Table 12: Reliability and validity formative constructs measurement model
Statistical significance outer weights: ***=$p<.001$; **=$p<.01$; *=$p<.05$

5.2.3 Model Fit

To determine the model fit of the measurement model, the saturated SRMR is assessed. For study 1, a value of 0.76 was found, while for study 2, a value of 0.75 was found. Both these values are below the threshold value of 0.8.

5.3 Structural Model

The structural model was assessed for path significance, variance explained and predictive capability. In addition, the significance of the differences between the path coefficients between the two studies was examined. As SmartPLS allows for only one way of path, cross-validated predictive ability testing was used as a way to determine the most appropriate direction for the relationship between Trust and Privacy Concern. The final model used in the structural model assessment can be seen in figure 13.

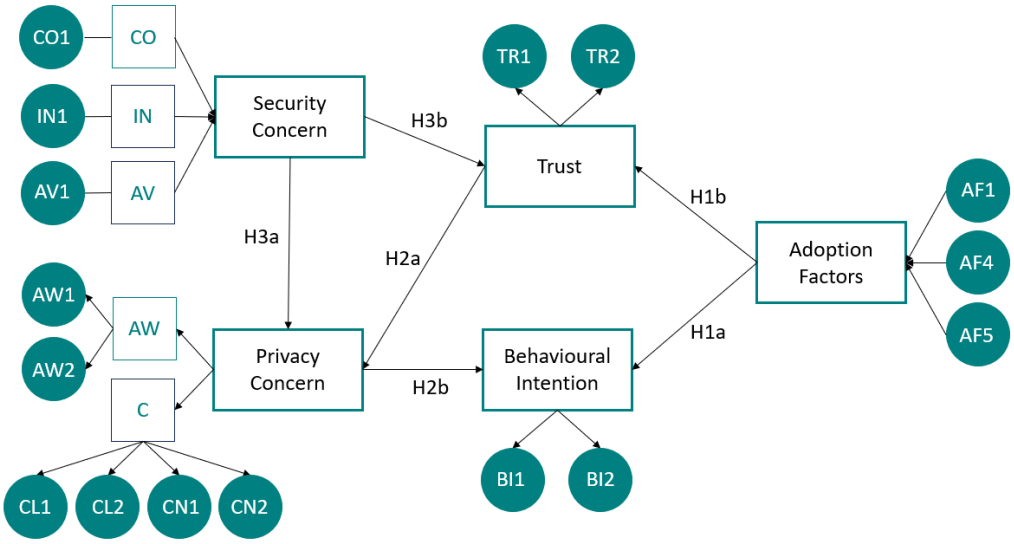


Figure 13: Structural model after measurement model assessment

5.3.1 Path Coefficients

The structural model's path coefficient for both studies can be seen in table 13. The table shows significant paths for all the hypothesised relationships of the conceptual research model but that of the direct effect of Trust on Privacy Concerns. Trust in wearable providers therefore has no significant lowering effect on potential end-users' privacy concern. A comparison between the two studies shows the influence of clinical care functionality on the two models. The results of Study 2 show that end-users trade off their privacy concern with other positive adoption factors and thus, a privacy calculus is present in the potential end-user considerations.

Hypothesis	Relationship	β	*p*-value
H1b	AF $\rightarrow TR$	0.264	0.000***
H1a	AF $\rightarrow BI$	0.648	0.000***
H2b	PC $\rightarrow BI$	-0.135	0.040*
H3a	SC $\rightarrow PC$	0.756	0.000***
H3b	SC $\rightarrow TR$	-0.361	0.000***
H2a	TR $\rightarrow PC$	-0.034	0.598

(a) Study 1

Hypothesis	Relationship	β	*p*-value
H1b	AF $\rightarrow TR$	0.201	0.036*
H1a	AF $\rightarrow BI$	0.718	0.000***
H2b	PC $\rightarrow BI$	-0.122	0.024*
H3a	SC $\rightarrow PC$	0.775	0.000***
H3b	SC $\rightarrow TR$	-0.415	0.000***
H2a	TR $\rightarrow PC$	-0.053	0.354

(b) Study 2

Table 13: Path coefficients structural model
Statistical significance: ***=$p<.001$; **=$p<.01$; *=$p<.05$

By looking into the path coefficients of both studies as explained in section 4.2.6, the significance of the differences between the models can be examined. The confidence intervals of the path coefficients are presented in table 14. The table shows no significant differences in the relations between the two studies. Potential end-users do not have different needs regarding the cybersecurity and privacy system of medical wearables based on clinical care functionality.

Relationship	Sample mean	2.5%	97.5%
AF $\rightarrow TR$	0.270	0.118	0.417
AF $\rightarrow BI$	0.648	0.511	0.754
PC $\rightarrow BI$	-0.134	-0.266	-0.008
SC $\rightarrow PC$	0.762	0.655	0.857
SC $\rightarrow TR$	-0.366	-0.513	-0.204
TR $\rightarrow PC$	-0.026	-0.150	0.099

(a) Study 1

Relationship	Sample mean	2.5%	97.5%
AF $\rightarrow TR$	0.200	-0.013	0.370
AF $\rightarrow BI$	0724	0.638	0.796
PC $\rightarrow BI$	-0.119	-0.223	-0.012
SC $\rightarrow PC$	0.773	0.690	0.848
SC $\rightarrow TR$	-0.423	-0.568	-0.268
TR $\rightarrow PC$	-0.053	-0.163	0.055

(b) Study 2

Table 14: Confidence Intervals path coefficients structural model

5.3.2 Mediation Analysis

By assessing the indirect effects of the model in both studies, significant mediation effects can be found. One significant indirect effect is found in both models, which can be seen in table 15. Security Concern does have a negative significant relationship with Behavioural Intention through Privacy Concern. However, the path via Trust is not significant. Trust is thus not established as a mediator between Security Concern and Privacy Concern. This mediation analysis helps to define Privacy Concern as largely influenced by Security Concern in its effect on Behavioural Intention. This indicates that the cybersecurity system is indeed an underlying system to the privacy system and is an important contribution in the user needs. There are no significant differences in the two studies for the mediation of Security Concern to Behavioural Intention.

Indirect effect	β	***p*-value**
SC $\rightarrow BI$	-0.103	0.039*
SC $\rightarrow PC \rightarrow BI$	-0.102	0.040*
SC $\rightarrow TR \rightarrow PC \rightarrow BI$	-0.002	0.649

(a) Study 1

Indirect effect	β	***p*-value**
SC $\rightarrow BI$	-0.097	0.026*
SC $\rightarrow PC \rightarrow BI$	-0.094	0.025*
SC $\rightarrow TR \rightarrow PC \rightarrow BI$	-0.003	0.445

(b) Study 2

Table 15: Mediation Analysis SC
Statistical significance: ***=p<.001; **=p<.01; *=p<.05.

5.3.3 Variance & Predictive Relevance

The variance explained by the model in both studies is assessed with R^2. The results are presented in the first column of table 16. The model has significant variance explained for both studies. However, Trust has an R^2 value of 0.228 which is considered weak in the most recent literature on the criterion. Study 2 has slightly better values for the explained variance. To determine the model's predictive capability in both studies, we consider the prediction relevance Q^2 and the cross-validated predictive ability test (CVPAT). The results can be seen in table 16 below. The CVPAT shows values of significantly below 0, and all the indicators show a Q^2 of over 0.

Construct	R^2		CVPAT		Q^2	
BI	0.459	0.000	-0.264	0.001	BI1	0.254
					BI2	0.293
TR	0.228	0.001	-0.140	0.015	TR1	0.197
					TR2	0.108
PC	0.593	0.000	-0.459	0.000	C	0.592
					AW	0.314
Overall			-0.288	0.000		

(a) Study 1

Construct	R2		CVPAT		Q2	
BI	0.534	0.000	-0.267	0.000	BI1	0.240
					BI2	0.484
TR	0.233	0.002	-0.136	0.016	TR1	0.166
					TR2	0.105
PC	0.640	0.000	-0.480	0.000	C	0.658
					AW	0.288
Overall			-0.294	0.000		

(b) Study 2

Table 16: Reliability and validity lower-order reflective constructs measurement model

5.4 Multigroup Analysis

For the MGA, first, the data is divided into predefined groups of gender, age and experience. For both models, a permutation group analysis is run to look at the MICOM and to establish the significance of the differences. For the age group pairwise comparisons, the significance value of 0.05 is adjusted to 0.011 according to Šidák p value calculation. The age group of 70 and older, included 12 respondents, which was too low to run MGA, as it led to a singular matrix error. The only significant differences were found in Study 1, for the age groups of 26-40 and 41-54-year-olds. In SmartPLS, the first step of MICOM, configural invariance, is already established. The analysis of the MICOM for step 2, compositional invariance, can be seen in table 17. The establishment of compositional invariance means there is at least partial measurement invariance. Step 3 of equal means and variances is not established for this pairwise comparison and therefore, the groups cannot fully be pooled in the data. The data is examined for significant differences in the structural path coefficients for the 26-40-year-olds and 41-54-year-olds. The analysis can be seen in table 18 below.

Construct	Original correlation	Permutation *p*-value
AF	0.680	0.121
BI	0.970	0.417
TR	0.999	0.867
PC	0.999	0.510
SC	0.922	0.746

Table 17: MICOM compositional invariance age groups (26-40) vs. (41-54)

Path	Original group 2	Original group 3	Original difference	Permutation *p*-value
AF $\rightarrow BI$	0.829	0.203	0.626	0.004*
AF $\rightarrow TR$	0.209	0.151	0.058	0.858
PC $\rightarrow BI$	-0.114	0.424	-0.538	0.014
SC $\rightarrow PC$	0.680	0.968	-0.287	0.208
SC $\rightarrow TR$	0.045	-0.493	0.538	0.247
TR $\rightarrow PC$	-0.302	0.386	-0.687	0.011

Table 18: MGA structural paths age groups (26-40) vs. (41-54)
Statistical significance: *=p<.01; **=p<.001

The permutation has a significant value for the path between Adoption Factors and Trust. Respondents belonging to the age category of 26-40 years and 41-54 years have a significantly different perception of the importance of Adoption Factors in the considerations they make if they want to use a wearable in Study 1. The 26 to 40-year-olds are considering positive adoption factors way less in their decision-making. The indirect effects that are present can be seen in table 19. Trust and Privacy Concern have significantly different mediating effects for the two age groups.

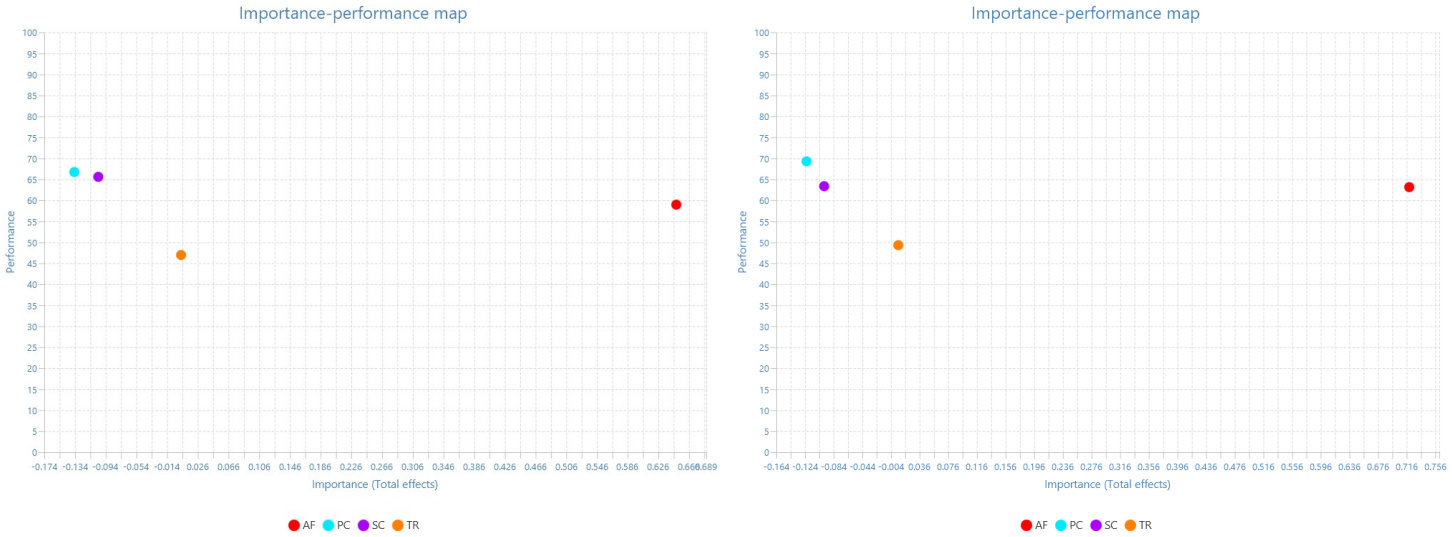
Indirect Effect	Original group 2	Original group 3	Original difference	Permutation *p*-value
AF $\rightarrow PC$	-0.063	0.058	-0.122	0.148
SC $\rightarrow BI$	-0.076	0.330	-0.406	0.009*
SC $\rightarrow PC \rightarrow BI$	-0.077	0.410	-0.488	0.001*
SC $\rightarrow TR \rightarrow PC \rightarrow BI$	0.002	-0.081	0.082	0.007*
TR $\rightarrow BI$	0.034	0.164	-0.129	0.002*
TR $\rightarrow PC \rightarrow BI$	0.034	0.164	-0.129	0.007*

Table 19: MGA indirect effects age groups (26-40) vs. (41-54)
Statistical significance: *=p<.01; **=p<.001

For the comparison of the MGA between Study 1 and 2, the MICOM of the MGA between the 20-40-year-olds and 41-54-year-olds of Study 2 is checked. The compositional invariance of the models can not be established for Study 2, which indicates that the data from the MGA for Study 2 is not reliably accommodated to the difference in the two age groups. Therefore, it is not reliable to check for significant differences between the studies for the MGA of the two groups. As no reliable analysis of the clinical care functionality model could be made, the MGA results have no further relevance for the user-centred cybersecurity and privacy environment of medical wearables.

5.5 Importance-Performance Mapping Analysis

To obtain more knowledge on how the concerns about cybersecurity and privacy by potential end-users can best be tackled on a managerial level, IPMA is used. First, an IPMA for the main endogenous construct of Behavioural Intention was performed. The analysis can be seen in figure 14. The importance values in this figure coincide with the path coefficients of table 13 and table 15. The structural model path and mediation analyses showed that there are no significant differences between the two studies in terms of importance. In addition, this research considers both the negatively and positively related factors as relevant in terms of importance. The IPMA of Study 2 shows that there are also no large differences between the performance of the significant constructs of Security Concern, Privacy Concern and Adoption Factors.



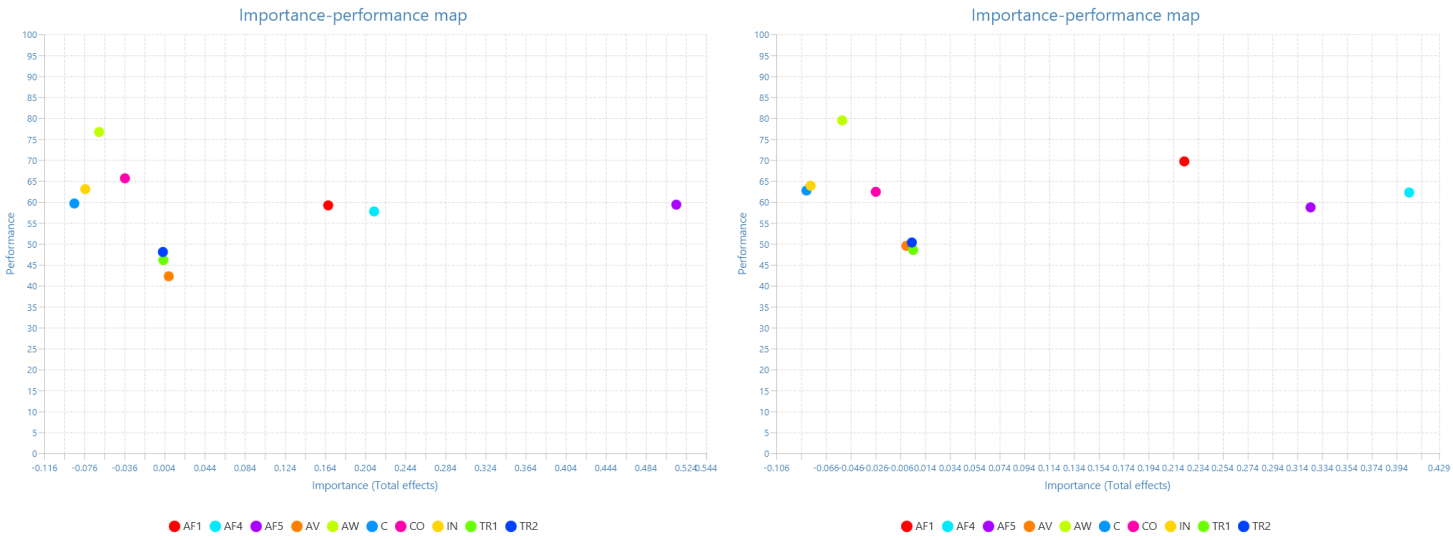
(a) Study 1

(b) Study 2

Figure 14: IPMA for BI: construct level

5.5.1 Behavioural Intention

An IPMA is done on the indicator level to gain an in-depth understanding of which aspects of the system medical wearable providers need to focus their attention on. First, the main endogenous construct of Behavioural Intention was chosen as the target construct. The resulting IPMA can be seen in figure 15. The values of the indicator-level IPMA for Behavioural Intention of both studies can be found in appendix C. The most important factor in consumer-grade wearables is that of AF5, which is an item concerning brand influence. When moving to medical wearables, this becomes less of an important factor, while AF4; influence from people who are important to the respondents, becomes the most important factor. The mean values of Study 1 show that a performance value of under 57.778 and an importance value of over 0.012, form the quadrant which is most useful for managerial decisions. For Study 2, these values are 60.706 and 0.012. When we split the quadrants in terms of positive and negative sides, the analysis is more relevant for the research. For Study 2, C has the most managerial potential on the negative side and AF5 on the positive side. This means that medical wearable providers in a user-centred approach to the system need to focus their attention on both data collection and control and social influence by people who are important to the end-user.



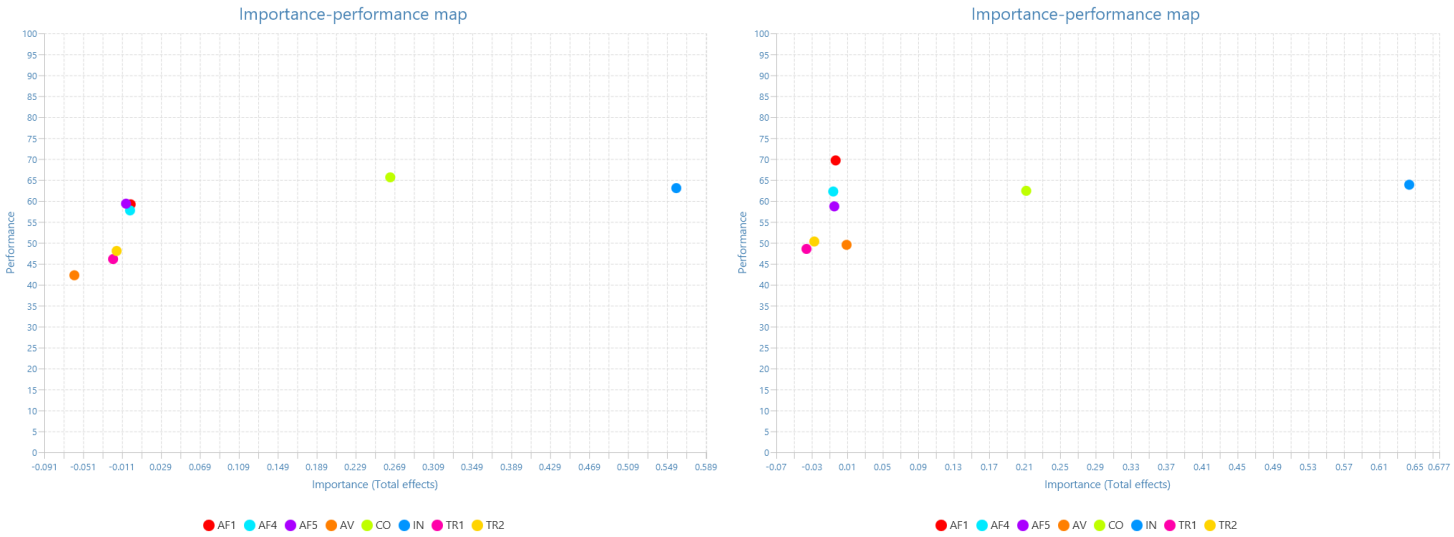
(a) Study 1

(b) Study 2

Figure 15: IPMA for BI: indicator level

5.5.2 Privacy Concern

The results of the mediation analysis and the IPMA for the Behavioural Intention construct indicated that security concern is an important causal factor for the relationship between privacy concern and behavioural intention. To further investigate how medical wearable providers can best tackle the privacy concern through the cybersecurity system, a second IPMA was performed on the target construct of Privacy Concern. The resulting indicator-level IPMA for Privacy Concern can be seen in figure 16. The corresponding most relevant quadrant for managerial purposes is indicated by a performance value of under 58.165 and an importance value of over 0.118 in Study 2. Looking purely at the indicators of Security Concern of Study 2, loss of data integrity is deemed the most important factor to consider for managerial purposes. This is important for medical wearable providers to take into account when steering the design of the cybersecurity system.



(a) Study 1

(b) Study 2

Figure 16: IPMA for PC: indicator level

5.6 Cluster Analysis

After consideration of an expert review of the results, it was decided to be informational to check whether there are different privacy trade-off groups in the data, as described by Westin (Margulis et al., 2010) (see section 2.1.3). A full overview of the expert review can be seen in appendix D. To perform this extra addition to the results, SPSS statistics k-means clustering was used on a combined version of the data sets of the two studies (excluding the indicators that were deleted during the measurement model assessment).

To check whether three distinct cluster groups are considered to be present within the data regarding the privacy perception, the number of iterations is checked. Confirming the distinctive characteristics of clusters identified by the cluster analysis, a one-way ANOVA employing a Bonferroni post-hoc test is done and checked for significance <0.05. For the Privacy Concern and Adoption Factors indicators, the following three significant clusters were found: 42 respondents scored Privacy Concern high and Adoption Factors relatively low (cluster 1), 45 respondents scored Privacy Concern relatively low and Adoption Factors also relatively low (cluster 2). A cluster of 68 respondents considered Privacy Concern and Adoption Factors both high (cluster 3). An overview of the cluster responses can be seen in figure 17.

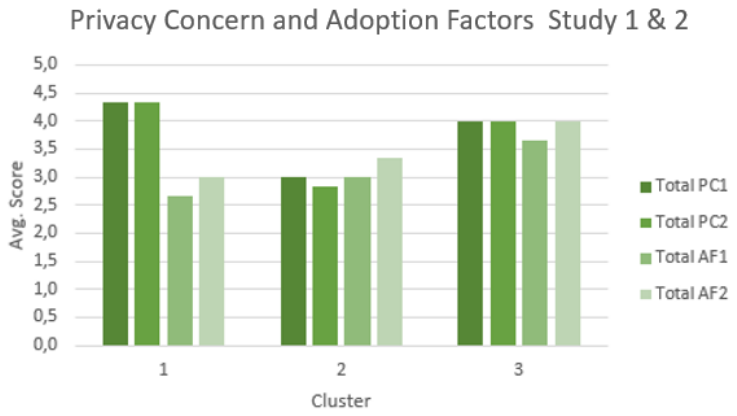


Figure 17: Privacy trade-off clusters

The privacy concern trade-off with positive adoption factors is significantly different for the three different clusters and the Westin privacy positions can be seen. Cluster 1 represents privacy fundamentalists; they are not swayed by positive adoption factors and have an uninfluenced high concern for privacy. Cluster 2 includes the privacy-unconcerned respondents, who have a medium level of consideration for both privacy concern and adoption factors, with slightly higher regard for positive adoption factors in Study 2. Cluster 3 represents the privacy pragmatists. They do have a high privacy concern, however also regard other adoption factors as equally important, thus indicating that these respondents are likely to trade off some of their privacy. The cluster analysis confirms the notion of the privacy literature that most people are privacy pragmatists. Subsequently to the k-means clustering analysis, linear regression analysis is performed on the groups of age, gender, and experience, to look for significant relationships between the privacy trade-off clusters and other user groups represented in the sample characteristics. The data shows no significant relationships between the different clusters and the predefined user groups of age, gender, and experience with consumer-grade wearables.

By defining the cluster groups in the data set of the PLS-SEM structural model of Study 2 and performing another MGA, the different relationships of the conceptual research model can be analysed for differences based on the privacy positions. The structural model evaluation does not pass the MICOM step 2 test and thus, no significant differences in the path coefficients were found. Thus there is no difference in the needs of users for the medical wearable based on the different privacy positions.

As a second k-means clustering, an analysis is done to see if there are different groups in the data that have significantly different privacy and cybersecurity concerns. This k-means clustering approach was set to three groups as well. The analysis showed that there is a significant difference in the data for the security and privacy concerns of three groups of respondents. The analysis can be seen in figure 18 below. Cluster 1, represents relatively low privacy and cybersecurity concerns of 22 respondents, while cluster 2 represents moderate security and privacy concerns of 59 respondents. Cluster 3 includes 74 users and represents high security and privacy concerns. Moreover, the analysis shows no difference in the cluster values of security and privacy concerns due to clinical care functionality. After performing a linear regression analysis on the clusters, it was shown that there is a significant relationship with the sample characteristic of experience. Respondents who do own a wearable, are placed into clusters 1 and 2 significantly more often than cluster 3. Respondents who do not own a wearable were placed in the highly concerned cluster significantly more often. This analysis is then expanded to look for relationships between the cluster placement of the respondents who do own a wearable and the length of the experience and/or the type of wearable used. To this end, only the data of wearable-owning respondents was used. This resulted in no significant relationships with the clusters.

Figure 18: Security and privacy concern clusters

By defining the clusters in the data of the PLS-SEM structural model of Study 2 as a new user segment and performing another MGA, the different relationships of the conceptual research model can be analysed for differences based on the privacy positions. The structural model evaluation does not pass the MICOM step 2 test or does not give significant differences on the basis of the clusters. This means that there are no different needs of potential potential end-users based on these clusters.

5.7 Results Conclusions

The survey research presents pertinent results for the overall research regarding the user-centred cybersecurity and privacy environment. The results of Study 2, explain the user needs regarding the medical wearable cybersecurity and privacy system as they represent the factors which affect the adoption intention of potential end-users. This comprises the answering of research subquestion 2. The following results of the data analysis are considered important for the user-centred approach to the cybersecurity and privacy system:

- Security concern is an important causal concept for the privacy concern of potential end-users of medical wearables. The most contributing factor in this relation is the concern about the loss of data integrity.
- Privacy concern is an important factor in the adoption intention of potential end-users of medical wearables. The concepts of data collection and control are the most defining factors in the end-user perception of privacy concern.
- The potential end-users of medical wearables trade off their privacy concern with positive adoption factors. Social influence by people who are important to the end-user is the most important trade-off factor in the adoption intention considerations of potential end-users.

For conclusions on the user limitations, the results of the comparison between Study 1 and 2 and the second cluster analysis (Study 2) are considered. The following results of the data analysis, which represent results on user limitations, are used for the user-centred approach:

- There are no significant differences in the importance of cybersecurity and privacy concerns regarding the adoption intention of potential end-users based on clinical care functionality.
- There are significant differences in the cybersecurity and privacy concerns of potential end-users based on experience with consumer-grade wearables. These cybersecurity and privacy concerns are not significantly different due to clinical care functionality.

6

Discussion & Recommendations

In this chapter, recommendations for the cybersecurity and privacy system design by medical wearable providers are formed based on the literature review and the survey research. First, section 6.1 will form the guidelines for the design of a user-centred cybersecurity and privacy system by medical wearable providers. The results on the user needs and limitations, as explained in section 5.7, are used in combination with the human-centric cybersecurity components of user, usage, and usability. In section 6.2, the consequent recommendations are presented. This chapter answers subquestion 3: 'What are user-centred cybersecurity and privacy recommendations for medical wearable providers to be able to capitalise on clinical care functionality?'

6.1 Insights on the User-Centred Cybersecurity & Privacy Environment

The interpretation of the user-centred cybersecurity and privacy environment is done on the basis of the human-centric components of user, usage, and usability, which were established as the pillars of human-centric cybersecurity in the first part of the literature review of chapter 2. By combining these components with the results of the survey research (section 5.7), this section provides the formation of guidelines for the user-centred cybersecurity and privacy environment of medical wearables.

As stated before, the difference between Study 1 and 2 represents the clinical care functionality of the medical wearable and indicates the results on user limitations. The results of Study 2 indicate the user needs regarding the medical wearable. The usability component considers the influences of usability factors on the involvement of users with the cybersecurity and privacy system (needs and limitations). In the existing literature, positive adoption factors have been shown to influence the usability perception of users (Gumasing et al., 2023). The usage component considers the involvement of the end-user with the cybersecurity and privacy system more directly. The user component is an overarching component, which considers differences in user needs and limitations based on user segments. In theory, the three components could all have been coupled with both the needs and limitations. However, the results of section 5.7 allow for only one coupling for both the user and usability components. The resulting relevant combinations of the components and the survey research results can be seen in figure 19.

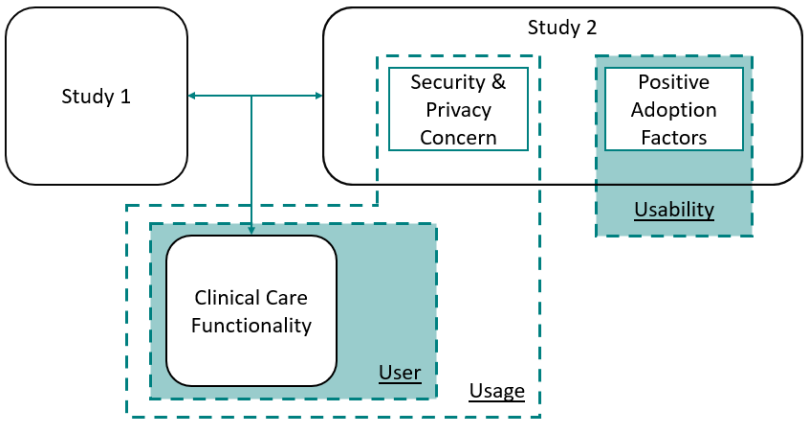


Figure 19: Survey research contributions to human-centric cybersecurity pillars

6.1.1 User

The user component in human-centric cybersecurity represents the notion that the cybersecurity and privacy system works more effectively when based on differences in user segments. User-oriented risks often result from human factors, which are different for different user groups. The interpretation of the cybersecurity and privacy environment of medical wearables on the user component helps to build a user-centred approach. If potential users feel that the cybersecurity and privacy environment is not suited to their needs, the likelihood of the cybersecurity and privacy system working properly is reduced.

From the cluster analysis of the privacy and security concerns, it was shown that there are significant differences in the cybersecurity and privacy concerns of end-users based on experience with consumer-grade wearables. These concerns were not affected by the presence of clinical care functionality. In existing literature, there is supporting research for the difference in the concerns of experienced and inexperienced users. Researchers find that inexperienced users may lack self-efficacy, competence, knowledge and/or awareness, all having heightening effects on their cybersecurity and privacy concerns (Chen et al., 2019) (Van Zoonen et al., 2019). These are human factors related to the psychological capability of users. The amount of cybersecurity and privacy concerns is linked to risky behaviour by end-users. As these are not affected by clinical care functionality, there is no adjusting of non-malicious non-secure behaviour. The following guideline for the user component of the user-centred cybersecurity and privacy environment is extracted:

There is a difference in non-malicious non-secure behaviour by end-users of medical wearables based on experience with consumer-grade wearables.

6.1.2 Usage

The usage component considers a baseline for the user involvement with the system. It combines traditional technology-centric cybersecurity and privacy with the involvement of users (e.g., expectations and intention to use). An important part of the usage component of human-centric cybersecurity, is the concept of differentiation. A cybersecurity and privacy environment can be more effective if it accounts for different needs of end-users and is based on differences in functionality. For this component, the results of the comparisons of Study 1 and 2 are considered (user limitations) as well as that of Study 2 alone (user needs).

The first aspect of the usage component is that of the user limitations. The comparison between the two studies showed that security and privacy concerns have no significantly different contribution to the adoption intention of consumer-grade wearables with and without clinical care functionality. This result was not expected from the literature, as established in section 3.1.4. Possible justifications for this result include environmental aspects of the clinical care functionality on users' cybersecurity and privacy perception. Iott et al. (2019) mention that patients have low privacy concerns about data sharing by healthcare professionals. Furthermore, users might not be aware of additional vulnerabilities and possible impact of clinical care functionality. In the context of section 2.2, this result is problematic. End-users will not actively change non-malicious non-secure behaviour when clinical care functionality is added even though the behaviour has a greater negative impact on the cybersecurity and privacy environment.

By looking at the difference in the cluster analysis for the privacy concern trade-off for the two studies, it can be seen that in all the clusters, the trade-off shifts towards positive adoption factors. This means that the different privacy positions are becoming less distinguishable due to the clinical care functionality. This result further indicates the importance of the usability of the medical wearable which will be explained in section 6.1.3. The following guideline for the user-centred cybersecurity and privacy environment is extracted:

There is no adjusting of non-malicious non-secure behaviour by end-users of medical wearables based on clinical care functionality.

6.1.2.1 Functional

The second aspect of the usage component of the user-centred approach is the defining concept of end-user needs, which are represented by the results on the relations with the adoption intention. For this aspect, the results of Study 2 are considered to inform measures for the cybersecurity system of the medical wearable. Functional measures are underlying measures which ensure specific functions are covered within the system. The mediation analysis showed that cybersecurity concern is an important causal factor for the relationship between the constructs of Privacy Concern and Behavioural Intention. This relation was expected from existing literature, as it was hypothesised and included in the conceptual research model (chapter 3). The most contributing factor in this relationship was found to be the

factor of concern about data integrity. The following guideline for the user needs regarding the cybersecurity system is extracted for the usage component:

Data integrity is the most important factor in the end-user perception of the cybersecurity system of medical wearables.

6.1.2.2 Technical & Legislation, Regulation & Policies

The results of Study 2 showed a significant negative relation between privacy concern and the adoption intention of end-users for medical wearables. Technical measures and legislation, regulation, and policies are useful in enhancing the privacy system, with which users directly interact. When looking at the results of the indicator-level IPMA for Behavioural Intention, privacy concern is mainly defined by concerns about data collection and control. Existing literature expressed measures for non-malicious non-secure behaviour regarding data collection and control approaches for consumer-grade wearables such as the ability to communicate sharing preferences with the device (Gabriele & Chiasson, 2020). In this way, end-users can differentiate types of data and sharing entities in the data-sharing capabilities of the device. The following guideline regarding the user needs of the privacy system is extracted:

Data collection and control are the most defining concepts in the end-user perception of the privacy system of medical wearables.

6.1.3 Usability

The usability component focuses on how well the user can use the cybersecurity and privacy system. This component is critical in providing added value and shows the importance of designing features with the premise that trade-offs come into play. The factors identified in this component that influence the usability perception of end-users are experience factors and interaction factors. From the cluster analysis on the privacy concern trade-off, the results confirmed most people in the sample are willing to trade off their privacy concern for positive adoption factors in the case of medical wearables and are therefore privacy pragmatists. This is consistent with the original literature on privacy positions (Westin, 2003). The positive adoption factors, in the context of the extended privacy calculus, give insight into the end-user's usability considerations. The results of the indicator-level IPMA for Behavioural Intention of Study 2, showed that for medical wearables, social influence by people who are important to the end-user is the most important positive adoption factor that was asked out. As a guideline, it is thus of vital importance to include the effects of the interaction factor of social influence in the cybersecurity and privacy system of the medical wearable.

The influence of important people to the end-user is the most defining factor for the usability perception of end-users of medical wearables

6.2 Recommendations

The insights of the user-centred cybersecurity and privacy environment as explained in the section above, allow for recommendations for medical wearable providers. From existing literature, useful notions of human-centric cybersecurity for the design of the cybersecurity and privacy system were identified as well as effective behavioural change techniques. By combining these 'best practices' with the challenges and risks of medical wearables, as established in section 2.2, the recommendations for the medical wearable providers are elaborated on. The first two recommendations consider user limitations and the consequences for the system in terms of user-oriented risks. The remaining recommendations 3 to 5 consider user needs and thus the importance of the cybersecurity and privacy system for the adoption intention of users. The recommendations on user limitations and user needs help to reduce both attacker-oriented and user-oriented risks.

1. To account for different levels of non-malicious non-secure behaviour of end-users, provide experience-based nudging and techno-regulation

This research stresses the importance of using different behavioural change techniques for inexperienced and experienced end-users of consumer-grade wearables. Existing end-users of consumer-grade wearables have significantly fewer cybersecurity and privacy concerns than non-users of consumer-grade wearables. By designing the system based on these differences, cybersecurity and privacy of medical wearables tackling non-malicious non-secure behaviour is more effective. Users of medical wearables could be asked for their experience with consumer-grade wearables and behavioural change techniques (i.e., nudging and techno-regulation) could be presented accordingly. For instance, existing literature on nudging based on user segments found promotion-based nudging to be especially effective for end-users who consider future consequences of their behaviour highly (Peer et al., 2020). This could be an effective

strategy for nudging inexperienced users. Moreover, existing literature states that effective nudging for cybersecurity includes nudges that only happen occasionally and which are transparent. This is also supported by (Wisniewskia et al., 2017) who consider experienced users making conscious privacy choices, finding techno-regulation or over-excessive nudging to be more of an annoyance. Medical wearable providers are advised to test different kinds of nudging and techno-regulation on user groups based on experience with consumer-grade wearables. Additionally, existing research points out a possible underlying cause in the form of lack of psychological capabilities by inexperienced users. Providers could pursue educational measures in the design to tackle this (Michie et al., 2011). Educational measures encompass the process of obtaining general knowledge, personal awareness, and skills training. Marketing strategies around the medical wearable could focus on providing information on cybersecurity and privacy measures.

2. To account for non-malicious non-secure behaviour of end-users of medical wearables, differentiate behavioural change techniques for SaMD and non-SaMD on the wearable

Medical wearable providers can help to reduce non-malicious non-secure behaviour in medical wearables and the high level of negative impact in the case of SaMD, by providing behavioural change techniques based on the SaMD functionality. Nudging and techno-regulation for influencing the behaviour of users could be more explicit when users access the SaMD, tackling increased user-oriented risks (section 2.2.3). For instance, warning messages could come up when trying to install SaMD, which makes sure users pay attention when they give permissions for secondary data sharing. This message could also include a security rating of the company involved. Such a nudge could be designed according to the notions of the MINDSPACE framework, e.g., being visual or gamified (Coventry, Briggs, Blythe, & Tran, 2014). The medical wearable could include privacy-preserving default privacy settings for SaMD, to counteract users leaving settings untouched. By adapting the behavioural change techniques of the system to the type of software, the non-SaMD functionality of the medical wearables maintains its usability.

3. To account for the cybersecurity concern of end-users, focus on functional measures tackling the loss of data integrity

The results of this research show that data integrity concerns in the medical wearable system are an important cause of privacy concern and consequently an adoption barrier for end-users. Data integrity loss has numerous causes, which are listed among the vulnerabilities in section 2.2. Medical wearable providers are advised to look into functional measures tackling the impact and probability of data integrity loss. For instance, a functional measure that could help data integrity in medical wearables mentioned in literature is to include edge computing in the system (Osama et al., 2023). This provides a computing layer between the medical wearable and the cloud which can be accessed by healthcare professionals and other third parties. Such a functional measure helps to reduce the data burden on healthcare professionals and tackles several vulnerabilities caused by device constraints. Both help to lower the probability and impact of data integrity loss.

4. To account for the privacy concern of end-users, focus on technical measures and legislation, regulation, and policies tackling improper data collection and loss of data control

The results of this research show that concerns about data collection and control are the most defining concepts in the effect of privacy concern of the end-user perception. The privacy concern can be tackled with technical measures as well as legislation, regulation, and policies. For instance, the privacy system of the medical wearable could provide the ability to communicate sharing preferences for different types of data. A policy incentive is to make sure data handling standardisation is applied across the industry. For medical wearable providers, it is important to unite in standards (e.g., sensor data formats, cybersecurity, and privacy measures) and steer the design of the system accordingly. This also indirectly helps to reduce risks due to several other vulnerabilities of the medical wearable system, e.g., data storage connections. This helps to prevent too much or unnecessary data from being collected and helps the loss of control over the data.

5. To ensure the usability of the cybersecurity and privacy system, design the system and structure the system environment with social influences in mind

The usability of the medical wearable is an important factor in the adoption intention of end-users. The cybersecurity and privacy system can benefit in terms of usability by taking into account the social influence of people who are important to end-users. For instance, the system design can enable possibilities for security cues by other trusted users (Das et al., 2014). Furthermore, it is helpful for medical wearable providers to strike up partnerships with healthcare professionals who are close to the end-user. This can help increase the usability perception of end-users regarding the cybersecurity and privacy system by reassuring and motivating end-users. To gain the confidence of healthcare professionals, it is important to reduce barriers to their involvement with medical wearables. Accuracy and data burden were shown to be two important barriers to take into account (section 2.2) when trying to involve healthcare professionals and institutions.

7

Conclusion

Recently, remote healthcare of patients has become a significant trend in the healthcare sector. Consumer-grade wearables present an opportunity for providing clinical care functionality as they can collect a variety and large amounts of data, have a large user base, and are complementary to people's lifestyles. They allow for early detection and advancements in diagnostics and they present a more complete symptom overview. The success of consumer-grade wearable use for clinical care purposes can help relieve the Dutch healthcare sector of workload, allow for more accurate and personal healthcare and provide people with more health autonomy. Maintaining the cybersecurity and privacy of these consumer-grade wearables remains a challenge. Medical wearable system and environment characteristics leave them open to attacker-oriented and user-oriented risks. A user-centred approach to the cybersecurity and privacy of medical wearables could help to take into account user limitations and needs. Therefore, the main research question this thesis aimed to answer is:

How can user-centred cybersecurity and privacy help the success of consumer-grade wearable use for clinical care purposes?

The question is answered with the help of the answering of the research subquestions.

7.1 Reflection Research Questions

Research Subquestion 1: What are the cybersecurity and privacy challenges and risks of medical wearables? Research subquestion 1 was asked to determine the role of users in the cybersecurity and privacy environment of medical wearables. To this end, first a theoretical background on human-centric cybersecurity was established. Important concepts of human-centric cybersecurity were set out to guide the user-centred approach of the research. The literature pointed out the importance of including human limitations and needs, taking into account human factors as contributing to the risk of non-malicious non-secure behaviour. Moreover, it was found important to consider actor incentive trade-offs in the cybersecurity and privacy environment. The components mentioned in the literature, on which human-centric cybersecurity is built, are user, usage, and usability. Behavioural change techniques (e.g., Michie et al. (2011)) and system design are more effective if they are adaptive to these components.

Subsequently, a human-centric risk assessment regarding the cybersecurity and privacy of medical wearables was performed. To this end, the challenges and vulnerabilities of the technology were examined. Many studies pointed out vulnerabilities in the system that arise due to device constraints of medical wearables. Computational power, memory, and battery life, all affect the level of security in the system. Unsecured network connections, insufficient encryption, and weak authentication methods are the results. Another leading concept in literature that was found to bring about vulnerabilities is the large amount of data that needs to be processed in the environment. Especially in the healthcare sector, the organisational, and technical infrastructure is not suitable/prepared for the amount of data collected by consumer-grade wearables. Database linkages with other medical databases allow for more sensitive data in the system. The fact that medical wearables are remote and highly mobile brings about an increased importance of human factors in the system. The sheer amount of heterogeneous devices and SaMD entering the market is another important challenge of medical wearables. A lack of appropriate standards means that devices and SaMD have different security and privacy measures, adding to the human factors of users. There are many connections in the system with differing levels of security and privacy, leading to a large attack surface.

Attacker-oriented risks are often linked to the vulnerabilities brought about by the device constraints of medical wearables. Prominent attacks in consumer-grade wearables such as MITM, eavesdropping, replay, and buffer overflow, all make use of vulnerabilities such as unsecured WPANs. However, they also target the human factors vulnerability by using social engineering attacks. They use phishing, spoofing, and tailgating to install malware or to gain access to confidential information, identify individuals, and ask for ransoms. The impact of when these attacks are successful is detrimental to the system due to the clinical care functionality of medical wearables. Wrong diagnoses and treatment from faulty data can have an enormous impact on consumers and the healthcare sector (e.g., regulatory fines and reputational damage). Identity theft and loss of privacy can cause anxiety and loss of trust in end-users.

The user-oriented risks found in the literature on consumer-grade wearables include both intentional and unintentional non-malicious non-secure behaviour. Previous research pointed out the presence of privacy calculus in the end-user's adoption intention of consumer-grade wearables. Also, lack of knowledge and awareness were found to be prominent causes of non-malicious non-secure behaviour. Various examples of non-malicious non-secure behaviours were found such as leaving default privacy settings, using weak passwords or exhibiting bad password management, and sharing sensitive information on social media.

With the answering of research subquestion 1, the important role of users in the cybersecurity and privacy environment of medical wearables was confirmed and explored. The user-oriented risks affect the impact and probability of attacker-oriented risks or have a direct impact themselves. A cybersecurity and privacy system that is designed to lower user-oriented risks is of vital importance.

Research Subquestion 2: How do users' privacy and cybersecurity concerns influence their intention to adopt consumer-grade wearables for clinical care purposes?
The research now shifted its focus to examining the needs and limitations of users in their involvement with the cybersecurity and privacy system. Needs were determined to be best represented by the concerns about the impact side of the attacker-oriented risks. Users have certain expectations of the cybersecurity and privacy system based on their concerns about risks, which affects their adoption intention. Limitations are human factors and corresponding non-malicious non-secure behaviour by end-users.

To address SQ2, the research aimed to capture the user perception. In this research, the cybersecurity system was deemed a supporting system to the privacy system, with which users directly interact. Furthermore, the literature review of chapter 2 showed significant relationships between cybersecurity and privacy concerns about risks and non-malicious non-secure behaviour by users of consumer-grade wearables. Because of the presence of a privacy paradox in the user involvement with consumer-grade wearables, it was determined user limitations could not reliably be determined directly with research into the user perception. The user limitations were determined to be best represented by a lack of differences in the user needs of the system due to the clinical care functionality (the main cause of the impact of the risks in the system).

In chapter 3, hypotheses about the cybersecurity and privacy perception of potential end-users regarding medical wearables were formulated based on past research into consumer-grade wearables. Previous research found that cybersecurity and privacy concerns were significant negative factors for the adoption intention of consumer-grade wearable end-users. Trust in providers was found to be negatively related to privacy concerns in consumer-grade wearables while being negatively affected by security concerns. Positive adoption factors, as established by UTAUT, were found to trade off with privacy concerns in the adoption intention of end-users, while positively affecting trust in providers. The clinical care functionality was found to have a strengthening effect on the negative relationship between privacy concern and adoption intention and weaken the positive relationship between the adoption factors and adoption intention. The hypotheses were used to construct a conceptual research model which was analysed with the help of survey research. A questionnaire was set out with potential adult end-users of medical wearables in the Netherlands. In this way, the end-user perception of the cybersecurity and privacy risks was captured.

To analyse the survey research, a two-step PLS-SEM model was used in combination with IPMA, MGA and cluster analysis. The response of users to the clinical care functionality in medical wearables was established by asking out the questionnaire once for consumer-grade wearables with clinical care functionality and once for those without this functionality. An overview of the accepted and rejected hypotheses in this research can be seen in table 20 below.

Number	Hypothesis	Result
1a	Adoption Factors (AF) will have a direct positive effect on Behavioural Intention (BI)	Confirmed
1b	Adoption Factors (AF) will have a direct positive effect on Trust (TR)	Confirmed
2a	Privacy Concern (PC) will have a direct negative relationship with Trust (TR)	Rejected
2b	Privacy Concern (PC) will have a direct negative effect on Behavioural Intention (BI)	Confirmed
3a	Security Concern (SC) will have a direct positive effect on Privacy Concern (PC)	Confirmed
3b	Security Concern (SC) will have a direct negative effect on Trust (TR)	Confirmed
4a	Clinical care functionality will have a significant positive effect on the negative relationship between Privacy Concern (PC) and Behavioural Intention (BI)	Rejected
4b	Clinical care functionality will have a significant negative effect on the positive relationship between Adoption Factors (AF) and Behavioural Intention (BI)	Rejected

Table 20: Survey research findings medical wearables

The findings confirmed the existence of an extended privacy calculus in the perception of potential end-users of medical wearables. Cluster analysis showed that most people in the sample are privacy pragmatists, which further emphasises the importance of the significance of the trade-off with positive adoption factors. The importance of positive adoption factors for the adoption intention was shown to be mostly due to social influence by people who are important to the respondents. The most defining concept of privacy concern for end-users was found to be data collection and control, which are thus important user needs in the privacy system. The most important contribution of cybersecurity concern to privacy concern was found to be the data integrity concern of end-users, which thus called for its consideration as a user need in the cybersecurity system. No significant differences in the factors affecting adoption intention based on clinical care functionality were found. This was a problematic result in the face of the user limitations and thus non-malicious non-secure behaviour of end-users. The MGA showed no significant differences between the predefined user segments for the relationships of the medical wearable adoption intention nor for the clinical care functionality. This meant that there were no differences in user needs for medical wearables based on the predefined user segments. A second cluster analysis showed that there were differences in terms of security and privacy concern for three clusters in the data, which were linked to potential end-users who are experienced in the use of consumer-grade wearables. These were not affected by clinical care functionality.

Research Subquestion 3: What are user-centred cybersecurity and privacy recommendations for medical wearable providers to be able to capitalise on clinical care functionality
This research question was answered to establish how the consideration of user needs and limitations would influence the cybersecurity and privacy system. Thus, the research now shifted its focus to providing recommendations for medical wearable providers to steer the design of the cybersecurity and privacy system and its environment. Subquestion 3 was answered by combining the information attained from the literature review with the results of the survey research. Guidelines for medical wearable providers were formed with the help of the human-centric cybersecurity components of user, usage, and usability and the end-user needs and limitations. The recommendations were elaborated on by considering the established challenges and risks in the medical wearable environment.

The establishment of the user component was guided by the fact that there were different security and privacy concerns of end-user groups which were not affected by clinical care functionality. These end-user groups were found to represent experienced and inexperienced users of consumer-grade wearables. This indicated that these user groups exhibit different non-malicious non-secure behaviours. This resulted in the following recommendation for the steering of the system design:

1. To account for different levels of non-malicious non-secure behaviour of end-users, provide experience-based nudging and techno-regulation

The usage component was partly guided by the non-significant differences in the relationships of the conceptual research model based on clinical care functionality. This indicated user limitations and a lack of necessary adjusting of non-malicious non-secure behaviour when accessing SaMD. The following recommendation regarding this part of the usage component was formed:

2. To account for non-malicious non-secure behaviour of end-users of medical wearables, differentiate behavioural change techniques for SaMD and non-SaMD on the wearable

The usage component was further established by the concept of the user needs regarding the cybersecurity system and privacy system. The importance of the cybersecurity system for end-users' adoption intention, calls for functional measures tackling the most important factor of data integrity loss. Edge computing was explored as a possible functional improvement of the cybersecurity system. The following recommendation was formed for medical wearable providers:

3. To account for the cybersecurity concern of end-users, focus on functional measures tackling the loss of data integrity

The fact that privacy concern significantly affects the adoption intention of end-users, leads to the necessity of technical measures as well as regulation, legislation, and policies regarding the privacy system. Data collection and control could be enhanced with data-sharing preference options and standardisation of data flow protocols. The recommendation regarding this final part of the usage component is as follows:

4. To account for the privacy concern of end-users, focus on technical measures and legislation, regulation, and policies tackling improper data collection and loss of data control

Finally, the importance of social influence by people who are important to the end-user, represents an opportunity to influence the usability perception of potential end-users. This was deemed useful for the usability component of the user-centred approach for the cybersecurity and privacy system as well. The system environment could be enhanced by involving healthcare professionals and enabling social cues by trusted people could enhance the system design. The following recommendation for the steering by medical wearable providers was formed:

5. To ensure the usability of the cybersecurity and privacy system, design the system and structure the system environment with social influences in mind

Main Research Question: How can a user-centred cybersecurity and privacy approach help the successful use of consumer-grade wearables for clinical care purposes?
With the answering of the three research subquestions and the formulation of the recommendations, the user-centred approach to the cybersecurity and privacy of medical wearables is concluded. The research shifted the focus of cybersecurity and privacy from a compulsory practice, focused on preventing breaches, where humans are seen as the 'weakest link', to an environment which can be a business opportunity. In this new focus, the system provides usable security and privacy, and human behaviour and perceptions are complementary to the device. By guiding the design of the cybersecurity and privacy system and its environment based on a combination of end-user needs and limitations and human-centric cybersecurity components, the system becomes more effective in tackling user-oriented risks. This in turn helps to substantially reduce attacker-oriented risks of medical wearables.

By reducing the cybersecurity and privacy risks in the environment, the chance and potential impact of breaches are lowered. Medical wearables face fewer adverse effects on the adoption intention, fewer regulatory fines, a better reputation, and increased positive word-of-mouth. The overall satisfaction of the end-user with the cybersecurity and privacy system will increase and the likelihood of the wearable being used to its full capacity is increased, stimulating sustainable usage. All these aspects help to make the use of consumer-grade wearables for clinical care purposes a success.

7.2 Theoretical Contributions

This research was able to expand on the knowledge about the cybersecurity and privacy of consumer-grade wearables that can provide treatment, diagnosis, alleviation, and monitoring functionality. The existing academic literature presented a knowledge gap in practical research into human-centric cybersecurity regarding system design. The research in this thesis presents theoretical contributions in the form of a novel way of applying human-centric cybersecurity to managerial-level system design. A conceptual framework to look into user needs and limitations based on clinical care functionality and medical wearables was proven to be of theoretical significance. Furthermore, an integration of theories was presented to establish the user-centred approach. The approach provides a coupling between the human-centric components of user, usage, and usability with the user needs and limitations. This is then followed by a coupling between the user-centred approach and the established risks in the cybersecurity and privacy environment. Finally, the research presents a paradigm shift in the medical wearable environment, moving away from a 'human-as-a-problem' perspective.

7.3 Practical Contributions

The user-centred approach taken in the research helps to tackle cybersecurity and privacy risks due to valid users (subsequently tackling the risks due to attackers). To do this, the research identifies best practices from the human-centric cybersecurity field. The research presents guidelines of the user-centred approach to design a cybersecurity and privacy environment which includes the components of user, usage, and usability. Moreover, the research provides practical contributions in the form of managerial-level recommendations for medical wearable providers. These recommendations provide practical strategies for medical wearable providers to steer the cybersecurity and privacy system design and system environment to account for user-oriented risks. This makes the cybersecurity and privacy of medical wearables more effective.

7.4 Management of Technology Relevance

The Master of Science Management of Technology teaches its students how firms can use technology to design and develop products and services that contribute to improving outcomes, such as consumer satisfaction, corporate productivity, profitability, and competitiveness. This thesis shows the understanding of technology as a corporate resource. The thesis helps the success of medical wearables by providing a user-centred approach to the cybersecurity and privacy environment, which makes it more equipped for the substantial impact of user-oriented risks on the environment. Herewith, the research helps consumer adoption intention, as well as the competitiveness of medical wearable providers. This thesis contains multiple research approaches (literature review and survey research) in a technological context. The research looks into the product development management of medical wearable technology by considering cybersecurity and privacy system design. The research uses several techniques to analyse the problem of cybersecurity and privacy risks regarding medical wearables. The research is multidisciplinary as it combines the field of cybersecurity and that of human behaviour. It considers multiple perspectives and trade-offs in the environment analysis and adds to responsible research, taking into account user needs.

The curriculum of the master's included several courses which were crucial to the development of this thesis. For instance, the course MOT1452 Inter- and Intra-Organisational Decision-Making tackled the concept of 'wicked problems'. Wicked problems are characterised by having no straightforward answer or a 'best' solution. These problems are multi-stakeholder problems with conflicting agendas and fading boundaries of disciplines and organisations. This course taught students to look at different perspectives of a problem and consider trade-offs in decision-making processes. The notions of this course were important for the research regarding the consideration of the system and the environment characteristics of medical wearables.

In the specialisation track of Cybersecurity, the importance of considering user limitations and needs in cybersecurity was covered in the course TPM025A User-Centred Security. The importance of taking into account user tasks and responsibilities of all stakeholders involved (e.g., managers, cybersecurity officers, and developers) to keep a secure environment was discussed. It is important to consider human factors and incentives for secure behaviour for the designing of cybersecurity measures. Moreover, stakeholder inter-dependencies and trade-offs need to be taken into account for a good overview of the different cybersecurity challenges that users experience. The notions of user-centred approach to cybersecurity and privacy discussed in this course, are central to the thesis.

7.5 Limitations & Ethical Considerations

The results of the research should be interpreted and applied with caution due to limitations in the research. The literature review poses some limitations. In the scope of the thesis, there was only a focus on the negative implications of non-malicious non-secure behaviour. For a more complete overview of the user-centred cybersecurity and privacy environment, it is important to examine the positive side of human behaviour as well. In addition, the research relies on existing research in consumer-grade wearable behaviours and usability perception. This was done on account of the scope and time frame of the research. Additionally, as stated in the literature review, only the contribution of the end-user (consumer) perception is considered in the user-oriented risk. In reality, as the data of the medical wearable is stored within clouds and databases in a large, connected environment, the perceptions of all stakeholders are relevant.

Furthermore, the quantitative survey research approach poses various limitations. The sampling method of convenience sampling presents limitations for generalisation, as the sample is not a true depiction of Dutch society. The cross-sectional approach of the research provides a picture of the potential end-user perception and lacks the changing perception of users over time. The survey research focuses its concept on the extended privacy calculus, however, the

concern of respondents is only examined with the use of impact statements regarding risks. However, the perception of potential end-users on the probability of these risks is also a contributing factor to concerns. Moreover, the choice for an adaptive version of the general privacy and security concern scales, IUIPC and CIA, was mainly used to establish good reliability and validity. However, more specific concern statements could have helped the insights of the study. This was also discussed in the expert review brainstorm session (appendix D). Several choices were made regarding the construction of the conceptual research model. The direct relations between Trust and Behavioural Intention as well as Security Concern and Behavioural Intention, were looked into. These relations were often mentioned in related literature sources, and although not part of the original conceptual research model, sparked interest for an exploratory look. These relations were found to decrease the predictive capability of the model and added no further explained variance to the relevant endogenous constructs.

Several respondents of the quantitative survey research provided feedback on the questionnaire. Respondents expressed that it was hard to grasp the concept of two different studies (with and without clinical care functionality) being performed simultaneously. This could have had a significant effect on the results of the research. In addition, the questionnaire was found to be long and repetitive, which means the alertness and consideration of the responses at the end of the questionnaire could have gone down. Even after pre-testing the survey, some statements were up for interpretation, although this was expected from the theories in the formation of the items. The data analysis of the questionnaire, in addition, showed some problematic areas. Even though the Fornell-Larcker criterion was met, the decision to combine the constructs of Control and Collection, as well as the dropping of a confidentiality concern item, was made to satisfy the suggested HTMT criterion. This causes further analyses to lose depth in the perception of cybersecurity and privacy concerns. However, this does give insight into the perception of potential end-users and the trouble they have to distinguish cybersecurity and privacy concepts. This was also expected from the pre-testing. The inclusion of more indicators per construct would have helped the reliability and validity of the results and allowed for a stronger structural model after measurement model assessment. For instance, Security Concern hereby effectively became a three-indicator first-order construct, instead of the desired second-order construct.

In the data analysis, the 70-years or older group in the sample was not large enough to perform MGA on. This analysis would have been very informative in examining the privacy calculus differences between younger and older respondents. Moreover, this group is crucial in reaping the societal benefits of consumer-grade wearables for clinical care. This group is the most dependent on the Dutch healthcare sector and thus could benefit the most from remote monitoring. Simultaneously, the group contributes the most to the sustainability issues of the sector. Cybersecurity and privacy incentives for medical wearables based on this user group could have been a substantial contribution to the success of the use of consumer-grade wearables for clinical care.

When applying behaviour change techniques in technologies based on user segments and other types of segmentation for personalising purposes, medical wearable providers need to consider the ethical dimension. Several studies question the privacy of users when collecting these types of personal data for behavioural change techniques. Moreover, basing behavioural change techniques on psychometric user segments (e.g., experience and gender) might be inferior to actual behaviour segments (Qua et al., 2022). The final recommendation of using social influence to increase the usability perception of end-users also brings about some ethical considerations. Healthcare institutions may not be entirely unbiased in the field of privacy, as they have partnerships with insurance companies, which benefit from the lack of privacy of patients.

7.6 Future Research

The research presents opportunities for future research. Mainly, research could inform the user-centred cybersecurity and privacy environment by specifically examining the types of non-malicious non-secure security and privacy behaviour displayed by potential end-users and associated human factors. This could give more insight into which type of risky behaviour needs to be tackled and how. The research could be expanded by performing qualitative research (e.g., interviews) on the results, to examine the underlying reasons for privacy concerns and to gain more knowledge on actual trade-offs and decision-making justifications of individuals. A suggestion from the expert review of this research included using focus groups, giving groups different scenarios and cybersecurity and privacy choices while capturing responses. A longitudinal study can add to the changing perspective after recommendations have been implemented. This way, the research could look into more precise types of behavioural change techniques which can work for the different dimensions of user, usage, and usability. Further research is necessary to understand the feasibility and effectiveness of the recommendations and the stance of healthcare institutions (their user adoption). Longitudinal studies could also help to research the actual adoption intention of end-users.

Additionally, several results were found which did not match the corresponding hypotheses or were beyond the scope of the research. Although possible explanations were provided from existing literature, these findings could benefit from further research. Qualitative research could be used to gain insight into why respondents did not significantly change their privacy concern' effect on adoption intention. More information could be gathered on the lack of effect of trust in medical wearable providers on privacy concerns (and adoption intention). Future research could also be done in different countries to examine the effect of the demographic culture of the sample on the results, adding another dimension to user segments.

The research can further be expanded by building on the identified limitations, as set out in the previous section. Performing research on the privacy calculus of 70-year-old and older respondents can help gain an overview of the user perception of this very important group for the Dutch healthcare system. Research could be done on the barriers, cybersecurity concerns and non-malicious non-secure behaviour of healthcare professionals. The research could benefit from quantitative research with more items dedicated to cybersecurity and privacy concerns of potential end-users. Future research could also focus on the lack of distinction in the perception of users on privacy and cybersecurity definitions.

References

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behaviour: Losses, gains and hyperbolic discounting. *The Economics of Information Security*, *12*, 165–178. https://doi.org/10.1007/1-4020-8090-5_13

Adams, A., & Sasse, A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46. https://doi.org/10.1145/322796.322806

Ajzen, I. (1985). From intentions to actions: A theory of planned behaviour. In *J. Kuhl and J Beckmann (Eds.), Action control (pp. 11-39).* Springer. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. In (1st ed.). Pearson.

Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the challenges and issues in adopting cybersecurity in Saudi smart cities: Conceptualization of the cybersecurity-based UTAUT model. *Smart Cities*, *6*(3), 1523-1544. https://doi.org/10.3390/smartcities6030072

Aliaga, M., & Gunderson, B. (2002). Interactive statistics. Sage Publications.

Alqhatani, A., & Lipford, H. R. (2019). 'There is nothing that i need to keep secret': Sharing practices and concerns of wearable fitness data. *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, 421–434. https://www.usenix.org/conference/soups2019/presentation/alqhatani

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: An approach for cyber security education training and awareness. *Proceedings of the 27th European Conference on Information Systems (ECIS)*. https://aisel.aisnet.org/ecis2019_rp/100

Anderson, N., Blythe, J., Lefevre, C., & Michie, S. (2023). Maintaining cyberhygiene in the internet of things (IoT): An expert consensus study of requisite user behaviours. *Qeios*. https://doi.org/10.32388/KIR04H

Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In *P. Siarry, M. Jabbar, R. Aluvalu, A. Abraham, and A. Madureira (Eds.), The fusion of internet of things, artificial intelligence, and cloud computing in health care. Internet of things (pp. 105–134).* Springer. https://doi.org/10.1007/978-3-030-75220-0_6

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. In (1st ed.). Prentice-Hall.

Bansal, G., Zahedi, F., & 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

Baudier, P., Kondrateva, G., Ammi, C., Chang, V., & Schiavonee, F. (2022). Digital transformation of healthcare during the COVID-19 pandemic: Patients' teleconsultation acceptance and trusting beliefs. *Technovation*, *120*, 102547. https://doi.org/10.1016/j.technovation.2022.102547

Bauer, J. M., & Van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*, 706-719. https://doi.org/10.1016/j.telpol.2009.09.001

Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2022). Consumers' privacy calculus: The prical index development and validation. *International Journal of Research in Marketing*, *39*(1), 20-41. https://doi.org/10.1016/j.ijresmar.2021.05.005

Ben Arfi, W., Ben Nasr, I., Kondrateva, G., & Hikkerova, L. (2021). The role of trust in intention to use the IoT in ehealth: Application of the modified UTAUT in a consumer context. *Technological Forecasting & Social Change*, *167*, 120688. https://doi.org/10.1016/j.techfore.2021.120688

Bhatt, V., & Chakraborty, S. (2020). Importance of trust in IoT based wearable device adoption by patient: An empirical investigation. *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 1226-1231. https://doi.org/10.1109/I-SMAC49090.2020.9243533

Blagodarny, D. (2017). Do privacy concerns matter in adoption of location-based smartphone applications for entertainment purposes. *[Master's Thesis, Linnaeus University]*. http://www.diva-portal.org/smash/get/diva2:1128461/FULLTEXT01.pdf

Blow, F., Hu, Y., & Hoppa, M. A. (2020). A study on vulnerabilities and threats to wearable devices. *Journal of The Colloquium for Information Systems Security Education*, *7*(1). https://cisse.info/journal/index.php/cisse/article/view/113

Burns, N., & Grove, S. (2005). The practice of nursing research: Conduct, critique and utilization. In (5th ed.). Elsevier Saunders.

Caldwell, Z. B. (2022). The case for a security metric framework to rate cyber security effectiveness for internet of medical things (IoMT). In *Hudson, F.D. (Ed.) Women securing the future with tippss for connected healthcare. Women in engineering and science.* Springer. https://doi.org/10.1007/978-3-030-93592-4_4

Cangardel, K. and Volgina, D. (2023, September 7). *The convergence of consumer wearables medical devices, part 1: Understanding the convergence. Blue Matter Consulting.* https://bluematterconsulting.com/convergence-consumer-wearables-medical-devices-part-1/

Cartwright, J. A. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, *14*, 1123–1132. https://doi.org/10.1007/s10877-023-01013-5

Cheah, J., Amaro, S., & Roldan, J. L. (2023). Multigroup analysis of more than two groups in PLS-SEM: A review, illustration, and recommendations. *Journal of Business Research*, *156*, 113539. https://doi.org/10.1016/j.jbusres.2022.113539

Chen, X., Sun, M., Wu, D., & Song, X. Y. (2019). Information-sharing behavior on WeChat moments: The role of anonymity, familiarity, and intrinsic motivation. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.02540

Ching, K. W., & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security Its Applications*, *8*(3), 19-30. https://doi.org/10.5121/ijnsa.2016.8302

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: a systematic literature review. *Behaviour and Information Technology*, *38*(3), 1-19. https://doi.org/10.1080/0144929X.2019.1583769

Clement, S. (2019). SME decision making in using bank loans: Applying an adapted model with attitudinal variables of the theory of planned behaviour in Nigeria. *[Doctoral dissertation, University of Bedfordshire]*. https://doi.org/10.13140/RG.2.2.11476.83844

Cohen, J. (1988). Statistical power analysis for the behavioral science. In (2nd ed.). Routledge.

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *A. Moallem (Ed.), HCI for cybersecurity, privacy and trust. HCII 2020. Lecture notes in computer science: vol. 12210 (pp. 105-122).* Springer. https://doi.org/10.1007/978-3-030-50309-3_8

Coventry, L., Briggs, P., Blythe, J. M., & Tran, M. (2014). Using behavioural insights to improve the public' s use of cyber security best practices. *Government Office of Science*, 1-20. https://doi.org/10.13140/RG.2.1.2387.3761

Coventry, L., Briggs, P., Jeske, D., & Van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In *A. Marcus (Ed.), Design, user experience, and usability. Theories, methods, and tools for designing the user experience. DUXU 2014. Lecture notes in computer science: vol. 8517 (pp. 229–239).* Springer. https://doi.org/10.1007/978-3-319-07668-3_23

Cronbach, L. (1946). Response sets and test validating. *Educational and Psychological Measurement*, *6*(4), 475-494. https://doi.org/10.1177/0013164446006004

Cumming, G., & Finch, S. (2005). Inference by eye: Confidence intervals and how to read pictures of data. *American Psychologist*, *60*(2), 170-180. https://doi.org/10.1037/0003-066X.60.2.170

Das, S., Kim, T.-J., Dabbish, L. A., & Hong, J. I. (2014). The effect of social influence on security sensitivity. *SOUPS '14: Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, 143-157.

Davis, F. (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

De Korver, F. (2019). The digital health market in the netherlands and switzerland. *Rijksdienst voor Ondernemend Nederland (RVO)*. https://www.rvo.nl/sites/default/files/2019/03/the-digital-health-market-in-the-netherlands-and-switzerland.pdf

Deci, E. L., & Ryan, R. M. (1985). Intrinsic motivation and self-determination in human behavior. In (1st ed.). Plenum Press.

Dirven, H., & Gielen, W. (2022, November 17). *Werkdruk en arbeidstevredenheid in de zorg. CBS.* https://www.cbs.nl/nl-nl/longread/statistische-trends/2022/werkdruk-en-arbeidstevredenheid-in-de-zorg

Dolan, P., Hallsworth, M., Halpern, D., King, D., & Metcalfe, R. (2012). Influencing behavior: The MINDSPACE way. *Journal of Economic Psychology*, *33*(1), 264–277. https://doi.org/10.1016/j.joep.2011.10.009

Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R. K., Gardezi, A. A., Weerasinghe, H., & Welhenge, A. (2021). Security and privacy issues in medical internet of things: Overview, countermeasures, challenges and future directions. *Sustainability*, *13*(21), 11645. https://doi.org/10.3390/su132111645

Enaizan, O., Eneizan, B., Almaaitah, M., Al-Radaideh, A. T., & Saleh, A. M. (2020). Effects of privacy and security on the acceptance and usage of emr: The mediating role of trust on the basis of multiple perspectives. *Informatics in Medicine Unlocked*, *21*, 100450. https://doi.org/10.1016/j.imu.2020.100450

Eysenbach, G., & Buis, L. (2021). Privacy concerns about health information disclosure in mobile health: Questionnaire study investigating the moderation effect of social support. *JMIR mHealth uHealth*, *9*(2). https://doi.org/10.2196/19594

Ferro, L. S., Marrella, A., & Catarci, T. (2021). A human factor approach to threat modeling. In *A. Moallem (Ed.), HCI for cybersecurity, privacy and trust. HCII 2021. Lecture notes in computer science: vol. 12788 (pp. 139–157).* Springer. https://doi.org/10.1007/978-3-030-77392-2_10

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50. https://doi.org/10.2307/3151312

Fuster, J., Solera-Cotanilla, S., Perez, J., Vega-Barbas, M., Palacios, R., Alvarez-Campana, M., & Lopez, G. (2023). Analysis of security and privacy issues in wearables for minors. *Wireless Networks*. https://doi.org/10.1007/s11276-022-03211-6

Gabriele, S., & Chiasson, S. (2020). Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. http://dx.doi.org/10.1145/3313831.3376651

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

Goodhue, D., & Loiacono, E. T. (2002). Randomizing survey question order vs. grouping questions by construct: An empirical test of the impact on apparent reliabilities and links to related constructs. In *Proceedings of the 35th hawaii international conference on system sciences.* https://doi.org/10.1109/HICSS.2002.994385

Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly*, *36*(3), 981-1001. https://doi.org/10.2307/41703490

Grobler, M., Gaire, J., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Dat*, *4*. https://doi.org/10.3389/fdata.2021.583723

Gumasing, J. J., Prasetyo, Y. T., Ong, A. K. S., Persada, S. F., & Nadlifatin, R. (2023). Factors influencing the perceived usability of wearable chair exoskeleton with market segmentation: A structural equation modeling and k-means clustering approach. *International Journal of Industrial Ergonomics*, *93*, 103401. https://doi.org/10.1016/j.ergon.2022.103401

Gutfleisch, M., Klemmer, J. H., Busch, N., Acar, Y., & Sasse, F. S., A. M. and. (2022). How does usable security (not) end up in software products? results from a qualitative interview study. *2022 IEEE Symposium on Security and Privacy (SP)*, 893-910. https://doi.org/10.1109/SP46214.2022.9833756

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2013). Multivariate data analysis. In (7th ed.). Pearson.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). A primer on partial least squares structural equation modeling. Sage Publications.

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool for business research. *European Business Review*, *26*(2), 106-121. https://doi.org/10.1108/EBR-10-2013-0128

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2018). Advanced issues in partial least squares structural equation modeling (PLS-SEM). In (3rd ed.). Sage Publications.

Haney, J. (2022). Users are not stupid: Six cyber security pitfalls overturned. *Cyber Security: A Peer-Reviewed Journal*, *6*(3), 230–241. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935795

Hassan, I. B., Murad, M. A. A., El-Shekeil, I., & Liu, J. (2022). Extending the UTAUT2 model with a privacy calculus model to enhance the adoption of a health information application in malaysia. *Informatics*, *9*(2), 31. https://doi.org/10.3390/informatics9020031

Henseler, J., Ringe, C. M., & Sinkovic, R. R. (2009). The use of partial least squares path modeling in international marketing. In *R.R. Sinkovics and P.N. Ghauri (Eds.), New challenges to international marketing (Advances in international marketing) (pp. 277-319).* Emerald JAI Press. https://doi.org/10.1108/S1474-7979(2009)0000020014

Henseler, J., Ringle, C. M., Hult, T. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Evaluation of formative measurement models. In *Partial least squares structural equation modeling (PLS-SEM) using R. Classroom companion: Business.* Springer. https://doi.org/10.1007/978-3-030-80519-7_5

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115-135. https://doi.org/10.1007/s11747-014-0403-8

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, *3*, 117–1124. https://doi.org/10.1016/j.promfg.2015.07.186

Herley, C. (2014). More is not the answer. *Security and Privacy*, *12*(1), 14-19. https://doi.org/10.1109/MSP.2013.134

Hern, A. (2018, January 8). *Fitness tracking app Strava gives away location of secret US army bases. The Guardian.* https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Hilbel, T., & Frey, N. (2023). Review of current ecg consumer electronics (pros and cons). *Journal of Electrocardiology*, *77*, 23-28. https://doi.org/10.1016/j.jelectrocard.2022.11.010

Hilowle, M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2023). Improving national digital identity systems usage: Human-centric cybersecurity survey. *Journal of Computer Information Systems*, 1-15. https://doi.org/10.1080/08874417.2023.2251452

Iott, B. E., Campos-Castillo, C., & Anthony, D. L. (2019). Trust and privacy: How patient trust in providers is related to privacy behaviors and attitudes. *AMIA Annual Symposium Proceedings*, 487-493. https://pubmed.ncbi.nlm.nih.gov/32308842/

Jernejcic, T. (2021). The role of privacy within the realm of healthcare wearables' acceptance and use. *[Doctoral dissertation, Dakota State University]*. https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1384&context=theses

Johnson, R. B., & Christensen, l. B. (2008). Educational research: Quantitative, qualitative, and mixed approaches. In (3rd ed.). Sage Publications.

Khan, N. (2023). A human-centric approach to unintentional insider threat: Development of a sociotechnical framework. *[Doctoral Dissertation, Nottingham University]*. https://eprints.nottingham.ac.uk/73952/1/Thesis_FINAL%20v2.5.pdf

Kim, D., Park, K., Park, Y., & Ahn, J. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281. https://doi.org/10.1016/j.chb.2018.11.022

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sciences*, *13*(6), 3410. https://doi.org/10.3390/app13063410

Kock, N. (2014). Stable p value calculation methods in PLS-SEM. ScriptWarp Systems. https://doi.org/10.13140/2.1.2215.3284

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227–261. https://doi.org/10.1111/isj.12131

Kohnfelder, L. and Grag, P. (1999, April 1). *The threats to our products. Microsoft.* https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx

Kounoudes, A. D., Kapitsaki, G. M., & Katakis, I. (2023). Enhancing user awareness on inferences obtained from fitness trackers data. *User Modeling and User-Adapted Interaction*, *33*, 967–1014. https://doi.org/10.1007/s11257-022-09353-8

Kraudel, R. (2019, July 16). *The convergence of consumer wearables and medical devices. Voler Systems.* https://www.volersystems.com/blog/news/the-convergence-of-consumer-wearables-and-medical-devices

Kromhout, M., Van Echelt, P., & Feijten, P. (2020). Sociaal domein op koers? *Sociaal en Cultureel Planbureau*. https://www.scp.nl/publicaties/publicaties/2020/11/16/sociaal-domein-op-koers

Kumar, Y., Koul, A., Singla, R., & Ijaz, M. F. (2023). Artificial intelligence in disease diagnosis: a systematic literature review, synthesizing framework and future research agenda. *Journal of Ambient Intelligence and Humanized Computing*, *14*(7), 8459–8486. https://doi:10.1007/s12652-021-03612-z

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(10). https://doi.org/10.1186/s42400-020-00050-w

Lee, S. M., & Lee, D. (2020). Healthcare wearable devices: an analysis of key factors for continuous use intention. *Service Business*, *14*, 503–531. https://doi.org/10.1007/s11628-020-00428-3

Linssen, L. (2022, June 27). *No quick fix for the GP shortage. Maastricht University.* https://www.maastrichtuniversity.nl/news/no-quick-fix-gp-shortage

Louis-Harris & Associates & Westin, A. F. (1995). Equifax-Harris mid-decade consumer privacy survey. Equifax.

Lupton, D. (2021). "Sharing is caring:" Australian self-trackers' concepts and practices of personal data sharing and privacy. *Frontiers in Digital Health*, *3*. https://doi.org/10.3389/fdgth.2021.649275

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.1040.0032

Mancuso, V. F., Strang, A., Funke, G. J., & Finomore, V. (2014). Human factors of cyber attacks: A framework for human-centered research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), 437-441. https://doi.org/10.1177/1541931214581091

Margulis, S. T., Pope, J. A., & Lowen, A. (2010). The Harris-Westin index of general concern about privacy: An exploratory conceptual replication. In *E. Zureik, L. Lynda Harling Stalker, E. Smith, D. Lyon, and Y. Chan (Eds.), Surveillance, privacy, and the globalization of personal information: International comparisons (pp. 91-109).* McGill-Queen's University Press. https://doi.org/10.1515/9780773591042-010

McKeon, J. (2021, September 16). *61m Fitbit, Apple users had data exposed in wearable device data breach. Health IT Security.* https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, *6*(42). https://doi.org/10.1186/1748-5908-6-42

Momani, M. A. (2020). The unified theory of acceptance and use of technology: A new approach in technology acceptance. *International Journal of Sociotechnology and Knowledge Development*, *12*(3), 79-98. https://doi.org/10.4018/IJSKD.2020070105

Montalbano, E. (2023, April 19). *Popular fitness apps leak location data even when users set privacy zones. Dark Reading*. https://www.darkreading.com/application-security/popular-fitness-apps-leak-location-data-even-when-users-set-privacy-zones

Moore, G., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222. https://doi.org/10.1287/isre.2.3.192

Motti, K., V. G. Caine. (2015). Users' privacy concerns about wearables. In *FC 2015: Financial cryptography and data security*. Springer. https://doi.org/10.1007/978-3-662-48051-9_17

Namahoot, K. S., & Jantasri, V. (2022). Integration of UTAUT model in thailand cashless payment system adoption: the mediating role of perceived risk and trust. *Journal of Science and Technology Policy Management*, *14*(2). https://doi.org/10.1108/JSTPM-07-2020-0102

Neumann, D., Tiberius, V., & Biendarra, F. (2022). Adopting wearables to customize health insurance contributions: a ranking-type Delphi. *BMC Medical Informatics and Decision Making*, *22*(112). https://doi.org/10.1186/s12911-022-01851-4

NIST. (1992). Foundations of a security policy for use of the national research and educational network. *NISTIR 4734*. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf

NIST. (2008). An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule. *NIST Special Publication 800-66 Revision 1*. https://doi.org/10.6028/NIST.SP.800-66r1

NIST. (2015). Supplemental information for the interagency report on strategic u.s. government engagement in international standardization to achieve u.s. objectives for cybersecurity. *NISTIR 8074*, *2*. http://dx.doi.org/10.6028/NIST.IR.8074v2

Osama, M., Ateya, A. A., Sayed, M. S., Hammad, M., Plawiak, 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

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., & et al. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *International journal of surgery*, *88*, 105906. https://doi.org/10.1136/bmj.n71

Peer, E., Egelman, S., Harbach, M., Malkin, M., Mathur, & Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavio*, *109*, 106347. https://doi.org/10.1016/j.chb.2020.106347

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: Promises and barriers. *PLOS Medicine*, *13*(2). https://pubmed.ncbi.nlm.nih.gov/26836780/

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*, 371–390. https://doi.org/10.1007/s10111-021-00683-y

Ponemon Institute. (2023). Cyber insecurity in healthcare: The cost and impact on patient safety and care. *Proofpoint*. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Princi, E., & Kramer, 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*. https://doi.org/10.3389/fpsyg.2020.582054

Priyananadan, R., & Brahm, S. (2016). Digitalisation: The future of health care. *Journal of Business Management*, *11*, 126-135. https://journals.riseba.eu/index.php/jbm/article/view/99

Qu, L., Xiao, R., Wang, C., & Shi, W. (2021). Design and evaluation of CFC-targeted security nudges. *CHI EA '21: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-6. https://doi.org/10.1145/3411763.3451624

Qua, L., Xiaoa, R., Shi, W., Huang, K., Qina, B., & Liang, B. (2022). Your behaviors reveal what you need: A practical scheme based on user behaviors for personalized security nudges. *Computers & Security*, *122*, 102891. https://doi.org/10.1016/j.cose.2022.102891

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. *The 12th International Conference on Advances in Information Technology (IAIT2021)*, 1-11. https://doi.org/10.1145/3468784.3468789

Rising, C. J., Gaysynsky, A., Blake, K. D., Jensen, R. E., & Oh, A. (2021). Willingness to share data from wearable health and activity trackers: Analysis of the 2019 health information national trends survey data. *Journal of Medical Internet Research mHealth and uHealth*, *9*(12). https://doi.org/10.2196/29190

Rizk, D., Rizk, R., & Hsu, S. (2019). Applied layered-security model to IoMT. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 227-227. https://doi.org/10.1109/ISI.2019.8823430

Roemer, E., Schuberth, F., & Henseler, J. (2021). HTMT2–an improved criterion for assessing discriminant validity in structural equation modeling. *Industrial Management Data Systems*, *121*(12), 2637-2650. https://doi.org/10.1108/IMDS-02-2021-0082

Rosman, L., Gehi, A., & Lampert, R. (2021). When smartwatches contribute to health anxiety in patients with atrial fibrillation. *Cardiovascular Digital Health Journal*, *1*(1), 9-10. https://doi.org/10.1016/j.cvdhj.2020.06.004

Rousseau, D. M., Sitkin, S. B., Burt, R. S., , & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Sarstedt, M., Hair, J., J. F. Cheah, Becker, J., & Ringle, C. M. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australasian Marketing Journal*, *27*(3), 197-211. https://doi.org/10.1016/j.ausmj.2019.05.003

Schomakers, E., Lidynia, C., & Ziefle, M. (2022). The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. *International Journal of Human–Computer Interaction*, *38*(13), 1276-1289. https://doi.org/10.1080/10447318.2021.1994211

Schuster, F., & Habibipour, A. (2022). Users' privacy and security concerns that affect IoT adoption in the home domain. *International Journal of Human–Computer Interaction*, 1-12. https://doi.org/10.1080/10447318.2022.2147302

Sekeran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. In (7th ed.). Wiley.

Shah, K. T. (2019). Privacy and security issues of wearables in healthcare. *[Master's thesis, Flinders University]*. https://flex.flinders.edu.au/file/c81182bb-2896-48da-95b8-bb943d3f7722/1/Privacy%20and%20Security%20Issues%20of%20Wearables%20in%20Healthcare.pdf

Silva-Trujillo, A. G., Gonzalez Gonzalez, M. J., Rocha Perez, L. P., & Garcia Villalba, L. J. (2023). Cybersecurity analysis of wearable devices: Smartwatches passive attack. *Sensors*, *23*(12). https://doi.org/10.3390/s23125438

Simonjan, J., Taurer, S., & Dieber, B. (2020). A generalized threat model for visual sensor networks. *Sensors*, *20*(13), 3629. https://doi.org/10.3390/s20133629

Smart Medical Devices. (n.d.). *ScienceSoft.* https://www.scnsoft.com/healthcare/medical-devices/smart (Accessed on Augustus 4, 2023)

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

Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital transformation in healthcare: Technology acceptance and its applications. *International Journal of Environmental Research and Public Health*, *20*(4), 3407. https://doi.org/10.3390/ijerph20043407

Sun, Q., Willemsen, M. C., & Knijnenburg, B. P. (2020). Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing. *Computers Security*, *97*, 101924. https://doi.org/10.1016/j.cose.2020.101924

Tabachnick, B., & Fidell, L. (2014). Using multivariate statistics. In (6th ed.). Pearson.

Tanga, K. L., Aikb, N. C., & Choong, W. L. (2021). A modified UTAUT in the context of m-payment usage intention in Malaysia. *Journal of Applied Structural Equation Modeling*, *5*(1), 40-59. https://doi.org/10.47263/JASEM.5(1)05

Taylor, S., & Todd, P. (1995). Understanding information technology usage: a test of competing models. *Information Systems Research*, *6*(2), 144–176. https://doi.org/10.1287/isre.6.2.144

Thapa, S., Bello, A., Maurushat, A., & Farid, F. (2023). Security risks and user perception towards adopting wearable internet of medical things. *International Journal of Environmental Research and Public Health*, *20*(8), 5519. https://doi.org/10.3390/ijerph20085519

The Chartered Institute of Ergonomics & Human Factors (CIEHF). (2022). *Human affected cyber security (hacs) framework.* https://ergonomics.org.uk/resource/human-affected-cyber-security-framework.html

Toulas, B. (2023, June 11). *Strava heatmap feature can be abused to find home addresses. Bleeping Computer.* https://www.bleepingcomputer.com/news/security/strava-heatmap-feature-can-be-abused-to-find-home-addresses/

Triandis, H. C. (1979). Values, attitudes, and interpersonal behavior. In *Nebraska symposium on motivation* (p. 195-260). University of Nebraska Press, Licoln. https://pubmed.ncbi.nlm.nih.gov/7242748/

Tu, J., & Gao, W. (2021). Ethical considerations of wearable technologies in human research. *Advanced Healthcare Materials*, *10*(17), 2100127. https://doi.org/10.1002/adhm.202100127

Tziouras, J. (2022). Health data from wearable technologies: Privacy and security regulatory aspects. *[Master's thesis, University of Tilburg]*. http://arno.uvt.nl/show.cgi?fid=159350

Udoh, E. S., & Alkharashi, A. (2016). Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. *Proceedings of the 2016 Future Technologies Conference*, 926-931. https://doi.org/10.1109/FTC.2016.7821714

Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2022). Threat modeling and risk analysis for miniaturized wireless biomedical devices. *Internet of Things Journal*, *9*(15). https://doi.org/10.1109/JIOT.2022.3144130

Van der Kleij, R. (2022). From security-as-a-hindrance towards user-centred cybersecurity design. *Human Factors in Cybersecurity*, *35*, 120-127. https://doi.org/10.54941/ahfe1002209

Van Steen, T. (2022). When choice is (not) an option: Nudging and techno-regulation approaches to behavioural cybersecurity. In *D.D. Schmorrow and C.M. Fidopiastis (Eds.), Augmented cognition. HCII 2022. Lecture notes in computer science: vol. 13310 (pp. 120-130).* Springer. https://doi.org/10.1007/978-3-031-05457-0_10

Van Zoonen, L., Rijshouwer, E., Leclerq, E., & Hirzalla, F. (2019). Privacy behavior in smart cities. *International Journal of Urban Planning and Smart Cities*, *3*(1). https://doi.org/10.4018/IJUPSC.302127

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. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157-178. https://doi.org/10.2307/41410412

Vermeulen, W. (2015). Decentralization of social policy in the netherlands. *CPB Netherlands Bureau for Economic Policy Analysis*. https://www.cpb.nl/sites/default/files/publicaties/download/cpb-background-document-decentralization-social-policy-netherlands.pdf

Vishwanatha, A., Neo, L. S., Goh, P., Leec, S., Khaderb, M., Ong, K., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Von Kalckreuth, N., & Feufel, N. A. (2021). Disclosure of health data – conceptualizing the intention to use wearables as an extended privacy calculus. *Human-Computer Interaction (SIG HCI)*, *Conference: AMCIS 2021*. https://aisel.aisnet.org/amcis2021/sig_hci/sig_hci/6

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, J., Zhang, W., & Wang, H. (2022). Privacy concerns toward short-form video platforms: Scale development and validation. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.954964

Westin, A. F. (1968). Privacy and freedom. Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431-453. https://doi.org/10.1111/1540-4560.00072

Wetsman, N. (2020, October 7). *Why Apple needed the FDA to sign off on its ekg but not its blood oxygen monitor. The Verge.* https://www.theverge.com/2020/10/7/21504023/apple-watch-ekg-blood-oxygen-fda-clearance

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, *8*, 305–316. https://doi.org/10.2147/MDER.S50048

Wisniewskia, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human–Computer Studies*, *98*, 95-108. http://dx.doi.org/10.1016/j.ijhcs.2016.09.006

Young, H., Van Vliet, T., Van de Ven, J., Jol, S., & Broekman, C. (2018). Understanding human factors in cyber security as a dynamic system. *Conference Paper in Advances in Intelligent Systems and Computing*. https://doi.org/10.1007/978-3-319-60585-2_23

Yuchao, W., Ying, Z., & Liau, Z. (2020). Health privacy information self-disclosure in online health community. *Frontiers in Public Health*, *8*. https://doi.org/10.3389/fpubh.2020.602792

Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019). Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Research Review*. https://doi.org/10.1108/PRR-08-2019-0027

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information Management*, *55*, 482-493. https://doi.org/10.1016/j.im.2017.11.003

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Chamberlain Kritikos, K. (2020). 'There's nothing really they can do with this information': unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society*, *23*(7), 1020–1037. https://doi.org/10.1080/1369118X.2018.1543442

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Zufferey, N., Niksirat, K. S., Humbert, M., & Huguenin, K. (2023). "Revoked just now!" users' behaviors toward fitness-data sharing with third-party applications. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, *1*, 47-67. https://doi.org/10.56553/popets-2023-0004

A

Technology Adoption Models

Author(s)	Model	Elements/Contributions	Pertinence
(Ajzen & Fishbein, 1980)	TRA	An individual's behaviour can be predicted by evaluating the individual's 'behavioural intention' to perform the specified behaviour. This behavioural intention is in turn determined by the constructs of Attitude and Subjective Norm.	It is designed to explain virtually any human behaviour, however, stays quite general because of this.
(Ajzen, 1985)	TPB	An individual's behaviour can be predicted by evaluating the individual's 'behavioural intention' to perform the specified behaviour. This is influenced by subjective norms, attitude and perceived behavioural control.	It helps understanding of individual acceptance and usage of many different technologies, but suggests that the behaviours are already planned.
(Davis, 1989)	TAM	Perceived usefulness and perceived ease of use are added in favour of the concepts of subjective norms and attitude of previous models (TPM, TPB).	It doesn't include subjective norms, nor does it look at integration, flexibility, completeness of information, and information currency. Most importantly, it does not include expectations.
(Taylor & Todd, 1995)	C-TAM-TPB	Combines the fields of IT and social psychological technology acceptance. It includes factors of both TAM and TPB.	The factor of behaviour planning is not stated. It still doesn't pay attention to fear or threat concerning use.
(Deci & Ryan, 1985)	MM	Has applications on motivational studies, learning, and healthcare. Includes perceived enjoyment.	It lacks a thorough representation of adoption factors relevant to technology usage.
(Triandis, 1979)	MPCU	It is suitable to predict individual acceptance of many technologies. It is successful in understanding and explaining the usage behaviour with a voluntary causative.	It is quite complex and does not have a history of being linked with extended privacy calculus.
(Bandura, 1986)	SCT	It considers the interactive nature between behaviour, personal and environmental factors.	Hard to navigate in a cross-sectional study. No connection in literature with the extended privacy calculus.
(Moore & Benbasat, 1991)	IDT	It has the ability to study any kind of innovations. It explains and predicts the rates of the adoption factors of innovation.	It is general. It does not indicate how the attitude impacts the accepting or rejecting the decisions, or how innovation factors affect decisions.
(Venkatesh et al., 2003)	UTAUT	This theory is considered as the combination of earlier theories such as TRA, TAM, MM, TPB, and IDT. It considers the factors of performance expectancy, effort expectancy facilitating conditions and social influence.	It is used in research of healthcare technologies. It has been linked to the extended privacy calculus.

Table 21: Research models technology acceptance
Adapted from (Momani, 2020)

B

Questionnaire

B.1 Introduction

This study is done by PS as part of the master program of MSc Management of Technology of the Technical University of Delft. The study focuses on the cybersecurity and privacy perception on the use of consumer-grade wearables for clinical care purposes.

A wearable is a device that can be worn on the body which, by online connection, collects physiological data. There are all kinds of wearables such as smartwatches (e.g. Apple Watch), activity trackers (e.g. Fitbit) and even smart hearing aids. A new development in the healthcare sector is the use of data collected by wearables (e.g., heart rate, sleep pattern, and calorie usage) for remote monitoring, diagnosis and treatment of disease. In this case, the wearable has clinical care functionality.

The questionnaire consists of 42 statements and lasts approximately 7 minutes. It is important to note your opinion on the statements spontaneously. The questionnaire differentiates between the use of a wearable with and without clinical care functionality. You can partake in the questionnaire regardless of whether you own a wearable or not and is anonymous. The results will contribute to cybersecurity and privacy incentives for medical wearable providers. The anonymous answers will be made available in the public data repository of the TU Delft as supporting material. Your participation is entirely voluntarily. You can quit the questionnaire at any moment and will not be participating in the study. As the questionnaire is anonymous, it is not possible to change/retract answers after completion.

B.2 Questionnaire Items

Construct	Label	Item	Adapted from
Behavioural Intention	BI1	I would use a wearable in the future / already use one	(Jernejcic, 2021)
	BI2	In the case of a positive experience, I would recommend the use of a wearable to people who are important to me	
Trust	TR1	I think providers of wearables are trustworthy	(Enaizan et al., 2020)
	TR2	I think providers of wearables have consumers' best interest at heart	
Adoption Factors	AF1	The use of a wearable can help me improve my health	(Jernejcic, 2021)
	AF2	It would be easy for me to become skillful in using a wearable	
	AF3	When I have troubles with a wearable, help is available to me	
	AF4	I would use a wearable if this is recommended by people who are important to me	
	AF5	I would use a wearable if it sold by a company I am familiar with	
Confidentiality	CO1	I am worried that data collected by a wearable can be accessed by unauthorized parties	(Alhalafi & Veeraraghavan, 2023)
	CO2	I am worried that data collected by a wearable will be sold	
Integrity	IN1	I am worried that data collected by a wearable will be improperly used/handled	(Alhalafi & Veeraraghavan, 2023)
	IN2	If data collected by a wearable is not accurate, this is a serious problem	
Availability	AV1	If data of a wearable is temporarily unavailable, this is a serious problem	(Enaizan et al., 2020)
	AV2	The existence of a back-up of the data that a wearable collects, is important	
Collection	CL1	I am worried that wearables would collect too much information from me	(Enaizan et al., 2020)
	CL2	I would not hesitate to provide personal information to a wearable	
Control	CN1	If it is possible, I would change the default privacy settings of a wearable	(Enaizan et al., 2020)
	CN2	I am worried that I do not have control over the way wearables collect, handle and storedata	
Awareness	AW1	I find it important to know what happens to the data that a wearable collects	(Enaizan et al., 2020)
	AW2	I find it important that providers of wearables have a transparent and clear privacy statement	

Table 22: Questionnaire items structural model

C

Data Analysis

C.1 Measurement Model

Construct	Item	FL	CR	AVE
Behavioural Intention	BI1	.811	.817	.691
	BI2	.852		
Trust	TR1	.925	.905	.826
	TR2	.0892		
Confidentiality	CO1	.923	.922	.855
	CO2	.927		
Integrity	IN1	.996	.577	.509
	IN2	.161		
Availability	AV1	.975	.693	.565
	AV2	.425		
Collection	CL1	.899	.811	.684
	CL2	.748		
Control	CN1	.794	.829	.709
	CN2	.888		
Awareness	AW1	.918	.876	.780
	AW2	.847		

(a) Model 1

Construct	Item	FL	CR	AVE
Behavioural Intention	BI1	.814	.853	.744
	BI2	.908		
Trust	TR1	.925	.820	.696
	TR2	.785		
Confidentiality	CO1	.877	.884	.792
	CO2	.903		
Integrity	IN1	.993	.600	.515
	IN2	.214		
Availability	AV1	.925	.760	.622
	AV2	.622		
Collection	CL1	.857	.827	.706
	CL2	.823		
Control	CN1	.836	.875	.778
	CN2	.926		
Awareness	AW1	.901	.841	.726
	AW2	.800		

(b) Model 2 (CF)

Table 23: Original reliability and validity measurement model

C.2 Cluster Analyses

C.2.1 Westin Privacy Positions

	Cluster 1	Cluster 2	Cluster 3
Number of respondents	42	45	68
AW1-s1	5	3	4
AW2-s1	5	4	5
AW1-s2	5	3	5
AW2-s2	5	4	5
CL1-s1	4	3	4
CL2-s1	4	3	4
CL1-s2	4	2	3
CL2-s3	4	3	4
CN1-s1	4	3	4
CN2-s1	4	2	3
CN1-s2	4	3	4
CN2-s2	4	2	4
AF1-s1	3	3	3
AF4-s1	2	3	4
AF5-s1	3	3	4
AF1-s2	3	4	4
AF4-s2	3	3	4
AF5-s2	3	3	4

Table 24: Final clusters of Privacy Concern and Adoption Factors

C.2.2 Combined Security & Privacy Concerns

	Cluster 1	Cluster 2	Cluster 3
Number of respondents	22	59	74
AW1-s1	3	4	5
AW2-s1	4	4	5
AW1-s2	3	4	5
AW2-s2	4	5	5
CL1-s1	2	3	4
CL2-s1	3	4	4
CL1-s2	2	3	4
CL2-s3	3	3	4
CN1-s1	3	4	4
CN2-s1	2	3	4
CN1-s2	3	4	4
CN2-s2	2	3	4
CO1-s1	2	3	4
CO1-s2	2	3	4
IN1-s2	2	3	4
IN1-s2	2	3	4
AV1-s1	2	3	3
AV1-s2	2	3	3

Table 25: Final clusters of Privacy Concern and Security Concern

C.3 IPMA

C.3.1 Contruct Level

	BI		PC	
	Total effect	Performance	Total effect	Performance
AF	0.649	58.974	-0.008	58.974
SC	-0.104	65.537	0.767	65.537
TR	0.004	46.974	-0.031	46.974
PC	-0.136	66.769		

Table 26: Construct-level IPMA Study 1

	BI		PC	
	Total effect	Performance	Total effect	Performance
AF	0.720	63.148	-0.011	63.148
SC	-0.097	63.351	0.795	63.351
TR	0.007	49.316	-0.055	49.316
PC	-0.123	69.213		

Table 27: Construct-level IPMA of Study 2

C.3.2 Indicator Level

	BI		PC	
	Total effect	Performance	Total effect	Performance
AV1	0.008	42.258	-0.060	42.258
CO1	-0.036	76.664	0.267	65.645
IN1	-0.075	63.065	0.554	63.065
AF1	0.167	59.194	-0.002	59.194
AF4	0.213	57.742	-0.003	57.742
AF5	0.514	59.355	-0.006	59.355
TR1	0.003	46.129	-0.019	46.129
TR2	0.002	48.065	-0.015	48.065
C	-0.086	59.662		
AW	-0.062	76.664		

Table 28: Indicator-level IPMA Study 2

	BI		PC	
	Total effect	Performance	Total effect	Performance
AV1	-0.001	49.516	0.010	49.516
CO1	-0.026	62.419	0.212	62.419
IN1	-0.078	63.871	0.640	63.871
AF1	0.223	69.677	-0.003	69.677
AF4	0.404	62.258	-0.006	62.258
AF5	0.325	58.710	-0.005	58.710
TR1	0.005	48.548	-0.037	48.548
TR2	0.003	50.323	-0.028	50.323
C	-0.082	62.930		
AW	-0.053	78.810		

Table 29: Indicator-level IPMA Study 2

D

Summary Expert Review

The expert review was performed to review the data analysis and subsequent interpretations of the results of the survey research. It was conducted in the form of a brainstorming session, with two Technology, Policy and Management faculty employees; PhD candidate Kathleen Guan and postdoc Wirawan Agahari. They have experience with the topic and research methodology of the survey research. Kathleen Guan has experience in the field of holistic integration of biopsychosocial factors in adaptive and personalised digital intervention designs. She researches how to promote health behaviour change in youth and across the lifespan. She also has experience in consulting on patient experience research for early-stage start-ups across a range of technologies, including telemedicine and mobile applications. Wirawan Agahari has experience in the field of privacy-enhancing technologies. His PhD research looked into multi-party computing (MPC) as a privacy-enhancing technology and its effect on data-sharing practices. Moreover, he has experience with research in cryptography, data science, and telecommunication technologies.

The review resulted in important insights on the data analysis. The choices made in the measurement model assessment of the two studies were discussed. Also, the considerations of the different relations between the constructs of the conceptual research model were discussed. During the brainstorming session, it was noted that the decisions regarding the relationships between the constructs should be clear from the thesis and that different considerations should be included in the text. A suggestion to use the predictive capability and the explained variance to differentiate between models was supported during the brainstorming session. Certain insignificant relationships, such as the one between Trust and Behavioural Intention, were ultimately presented in this way.

Subsequently, the interpretations of the survey research findings and possible justifications were discussed. The participants were also asked for their take on the findings and if there were similarities with their (past) research. One of the most pertinent contributions of the brainstorming session was that of suggestions for possible analysis extensions. The most relevant extension was to perform cluster analysis. It was considered an addition to the already performed Multigroup Analysis, by looking for direct links between established clusters and pre-defined user groups with linear regression. This could then be used for the different privacy positions of Westin, which could give more insight into the needs of users for the privacy system. Moreover, the different levels of security and privacy concerns within the sample could be looked into. The significance of these clusters could be increased by considering both the items of Study 1 and 2. It was also suggested to further look into the relationship between cybersecurity and privacy concerns in potential end-users' perception. The privacy-personalisation paradox was noted to possibly be relevant to behavioural change technique interventions.

For future studies, it was suggested that focus groups could help to extend the research. Each group could be presented with cybersecurity and privacy scenarios and different behaviours and choices could be captured. This would allow for both quantitative and qualitative research on the matter including a more reliable look at user limitations.