

Dakota State University

**Beadle Scholar**

---

Masters Theses & Doctoral Dissertations

---

Spring 4-2021

## **The Role of Privacy Within the Realm of Healthcare Wearables' Acceptance and Use**

Thomas Jernejcic

Follow this and additional works at: <https://scholar.dsu.edu/theses>



Part of the [Databases and Information Systems Commons](#), [Data Science Commons](#), and the [Systems Architecture Commons](#)

---

**DAKOTA STATE UNIVERSITY**

**THE ROLE OF PRIVACY WITHIN THE REALM OF  
HEALTHCARE WEARABLES' ACCEPTANCE AND USE**

A doctoral dissertation submitted to Dakota State University in partial fulfillment of the  
requirements for the degree of

Doctor of Philosophy

in

Information Systems

April, 2021

By

Thomas M. Jernejcic

Dissertation Committee:

Dr. Omar El-Gayar

Dr. Cherie Noteboom

Dr. Yong Wang

Dr. Houssain Kettani

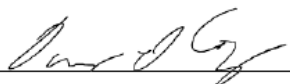


## **DISSERTATION APPROVAL FORM**

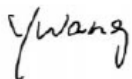
This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Thomas M. Jernejcic

Dissertation Title: The Role of Privacy within the Realm of Healthcare Wearables' Acceptance and Use

Dissertation Chair/Co-Chair:  Date: March 31, 2021

Committee member: Houssain Kettani  Date: April 1, 2021

Committee member:  Date: April 2, 2021

Committee member:  Date: April 2, 2021

## ACKNOWLEDGMENT

This endeavor would be incomplete without acknowledging those who contributed to its conclusion and my success. First, I would like to thank my dissertation chair, advisor and mentor, Dr. Omar El-Gayar, whose contribution to my development as a doctoral student and researcher cannot be overstated. His dedication towards his students is amazing. I would also like to thank my dissertation committee members Dr. Cherie Noteboom, Dr. Yong Wang, and Dr. Houssain Kettani, all who have gone above and beyond to ensure a credible outcome.

Second, I acknowledge my children, whose own achievements inspired me to aim high, and my grandchildren, who often provided escape from the books, journal articles, and research papers, bestowing opportunity to be a kid one more time. I thank my heavenly Father for the opportunity to be a part of their lives and I pray that my efforts will be an inspiration to them to seek their purpose and potential in Him.

Last and foremost, I acknowledge my wife, Grace, whose prompting several years ago initiated this incredible adventure. She has been my helpmate and late-night partner, encouraging me and staying up with me, regardless how late –or early. This achievement is hers as much as mine. I love you.

## ABSTRACT

The flexibility and vitality of the Internet along with technological innovation have fueled an industry focused on the design of portable devices capable of supporting personal activities and wellbeing. These compute devices, known as wearables, are unique from other computers in that they are portable, specific in function, and worn or carried by the user. While there are definite benefits attributable to wearables, there are also notable risks, especially in the realm of security where personal information and/or activities are often accessible to third parties. In addition, protecting one's private information is regularly an afterthought and thus lacking in maturity. These concerns are amplified in the realm of healthcare wearable devices. Users must weigh the benefits with the risks. This is known as the privacy calculus. Often, users will opt for the wearable device despite the heightened concern that their information may or will be disclosed. This is known as the privacy paradox. While past research focused on specific wearable technologies, such as activity trackers and smartphones, the paradox of disclosure despite concern for privacy has not been the primary focus, particularly in the realm of the manifestation of the paradox when it comes to the acceptance and use of healthcare wearable devices.

Accordingly, the objective of the present research was to propose and evaluate a research model specifically oriented towards the role of privacy in the realm of healthcare-related wearables' acceptance and use. The presented model is composed of sixteen constructs informed from multiple theories including multiple technology acceptance theories, the Protection Motivation Theory (PMT), the Health Belief Model (HBM), and multiple privacy calculus theories. Using a survey-oriented approach to collect data, relationships among privacy, health, and acceptance constructs were examined using SmartPLS with intentions to validate the posited hypotheses and determine the influence of the various independent variables on the intention to disclose and the intention to adopt healthcare-wearables. Of particular interest is the posited moderating effects of perceived health status on intention to disclose personal information.

The research endeavor confirmed significant evidence of the cost/benefit decision process, aka the privacy calculus, that takes place when deciding whether or not to disclose personal information in the healthcare wearables space. Perceived privacy risk was negatively correlated to intention to disclose while hedonic motivation and performance expectancy were positively correlated to intention to disclose. Furthermore, significant evidence was discovered

pertaining to the privacy paradox via the moderating role that perceived health status plays regarding the relationships between the constructs of perceived privacy risk and intention to disclose and hedonic motivation and intention to disclose. Intention to disclose was also found to have a significant positive influence on intention to adopt. Contributions include understanding and generalization in the healthcare wearables adoption knowledge space with a particular emphasis on the role of privacy, as well as practical implications for wearable manufacturers and users.

## DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

A handwritten signature in cursive script, reading "Thomas M. Jernejcic", is written over a horizontal line.

Thomas M. Jernejcic

## TABLE OF CONTENTS

<b>ACKNOWLEDGMENT .....</b>	<b>III</b>
<b>ABSTRACT.....</b>	<b>IV</b>
<b>DECLARATION.....</b>	<b>VI</b>
<b>TABLE OF CONTENTS .....</b>	<b>VII</b>
<b>LIST OF TABLES .....</b>	<b>IX</b>
<b>LIST OF FIGURES .....</b>	<b>X</b>
<b>INTRODUCTION.....</b>	<b>1</b>
BACKGROUND OF THE PROBLEM.....	1
STATEMENT OF THE PROBLEM .....	3
OBJECTIVES OF THE DISSERTATION .....	4
<b>LITERATURE REVIEW .....</b>	<b>6</b>
IOTs AND WEARABLES .....	6
PRIVACY .....	8
PRIVACY CALCULUS THEORIES.....	9
PRIVACY IN WEARABLE TECHNOLOGY .....	11
<b>THEORETICAL MODEL.....</b>	<b>14</b>
<b>RESEARCH METHODOLOGY .....</b>	<b>21</b>
SURVEY INSTRUMENT .....	21
DATA COLLECTION .....	21
ANALYSIS .....	22
<b>RESULTS .....</b>	<b>27</b>
DESCRIPTION OF THE SAMPLE .....	27
DESCRIPTIVE ANALYSIS.....	29
STATISTICAL ANALYSIS .....	33
<i>Measurement Model Testing</i> .....	34
<i>Structural Model Testing</i> .....	38



<i>Moderator Analysis</i> .....	42
<b>DISCUSSION</b> .....	<b>45</b>
<b>CONCLUSIONS</b> .....	<b>49</b>
<b>REFERENCES</b> .....	<b>52</b>
<b>APPENDIX A: RESEARH MODEL CONSTRUCTS MEASUREMENTS</b> .....	<b>63</b>
<b>APPENDIX B: SMARTPLS PARAMETERS</b> .....	<b>67</b>

## LIST OF TABLES

<b>Table 1:</b> Sample Description .....	28
<b>Table 2:</b> Statistical Measures of Central Tendency and Dispersion – Demographics .....	30
<b>Table 3:</b> Statistical Measures of Central Tendency and Dispersion – Measurement Instrument .....	32
<b>Table 4:</b> Measurement Model Test Summary .....	35
<b>Table 5:</b> Measurement Model Significance .....	36
<b>Table 6:</b> Endogenous Variable Summary .....	38
<b>Table 7:</b> Measurement Model Test Summary (loadings > 0.70) .....	39
<b>Table 8:</b> Measurement Model Significance (loadings > 0.70) .....	39
<b>Table 9:</b> Structural Model Test Summary .....	41

## LIST OF FIGURES

<b>Figure 1:</b> Research Model (adapted from Zhang et al. (2018) and Gao et al. (2015)).....	17
<b>Figure 2:</b> Example PLS-SEM Model (Wong, 2013) .....	24
<b>Figure 3:</b> Sample Distribution – USE, CHC, GDR, and AGE .....	30
<b>Figure 4:</b> Sample Distribution – EDU .....	31
<b>Figure 5:</b> Sample Distribution - PHS.....	33
<b>Figure 6:</b> Analyzed Research Model .....	34
<b>Figure 7:</b> Analyzed Research Model (loadings > 0.70) .....	37
<b>Figure 8:</b> Moderating Effect of PHS on PPR →ITD .....	42
<b>Figure 9:</b> Moderating Effect of PHS on HMO →ITD .....	43
<b>Figure 10:</b> Moderating Effect of PHS on PEX →ITD.....	44

# CHAPTER 1

## INTRODUCTION

### **Background of the Problem**

The flexibility and vitality of the Internet along with technological innovation have fueled an industry focused on the design of portable wearable devices capable of supporting personal activities and wellbeing (Ferraro & Ugur, 2011). These portable devices are known as wearables. Wearables are unique from other computers in that they are portable, specific in function(s), and worn or carried by the user (Jayden, 2018). They are a specialized category of Internet of Things (IoT) devices, a term coined by the Massachusetts Institute of Technology in 1999 (GAO, 2017). These devices are interconnected imbedded computing devices, forming an ecosystem of systems (Yuchen et al., 2017). Wearables are specialized in that they are IoT devices worn by the user. In addition to wearables, IoT devices include household thermostats, refrigerators, audio systems, and door locks to name a few.

Wearables can be classified under several categories including smart watches (Kritzler et al., 2015), body motion trackers (Yang et al., 2016), performance monitors, implantables, heart rate monitors (Muaremi et al., 2013), pedometers (Zenonos et al., 2016), and blood pressure monitors (Nadeem et al., 2015). These categories fall under two classifications including consumer wearables and special-purpose wearables (Perez & Zeadally, 2018). They are designed to accommodate a variety of body placements including the wrist, stomach, chest, arm, head, thigh, waist, knee, ankle, back, finger, neck, pocket, and over the body (Jayden, 2018). An example of the latter are IoT-enabled baby clothes designed to monitor temperature, respiration, and activity levels of the child wearing them (GAO, 2017). These versatile characteristics solicit a plethora of uses promising significant appeal for years to come.

The utility and attractiveness of wearables is made possible by the mobility afforded by the Internet, the increase in computational-power to consumption-power ratio, and the advancement of miniaturized sensors (Perez & Zeadally, 2018). The Internet has been of particular benefit due to the necessity to store and process data resulting from monitored

activities. This has been enhanced by advancements in wireless communications. For example, IoT-enabled fitness trackers can utilize a smartphone as a gateway device. The wearable fitness tracker connects to the smartphone via Bluetooth while the smartphone connects to the Cloud via Wi-Fi or cellular technologies (GAO, 2017). The increase in computational-power to consumption-power ratio as well as the miniaturization of sensors is attributable to the advancement in technology as manufacturers continue to increase the density of components and thus increase the effectiveness and utilization of the device's footprint. The ability to miniaturize sensors is particularly important towards expanding the capabilities of wearable technologies.

The benefits and attractiveness of wearables to the consumer have not gone unnoticed by the commercial sector. Consumers have accepted wearables into their everyday lives, considering them essential to their daily routines, wellness, and health. The global market value of wearables technology in 2015 was over \$24 billion (Perez & Zeadally, 2018). It was estimated that 130 million people used fitness trackers alone (GAO, 2017). By 2019, wearables were forecasted to reach \$42 billion (Costello, 2018), and by 2026, the market value is projected to increase by over 250% to \$150 billion (Perez & Zeadally, 2018). This projection reveals the untapped "blue ocean" opportunities resulting from the potential of wearables innovation over the coming years.

While there are definite benefits attributable to wearables, there are also significant risks, especially in the realm of privacy and security. Merriam-Webster defines privacy as "freedom from unauthorized intrusion" (2017). When applied to personal privacy, this definition can be rephrased as one's control over disclosure of their personal information. The question to consider in the current research is whether privacy (loss of control over disclosure) is at risk regarding the context of wearables. The answer to this question is complicated due to the issue of security, which speaks to the issue of device and/or data compromise by bad actors. This concern rises to the surface considering that design of IoT devices, including wearables, is often absent or severely lacking when it comes to security (Wei & Piramuthu, 2014). Even more concerning is the thought of compromise of health-oriented devices such as implantable medical devices (IMDs) which could threaten the life or wellbeing of the patient (Zhou et al., 2019). Privacy concerns are not necessarily confined to the individual. In 2018, locations of secret U.S. military installations were at risk as a result of

disclosure of exercise-related activity data collected from wearable fitness trackers worn by U.S. service personnel (Jernejcic & Kettani, 2019). Utilizing an online “heat map”, these secret bases, along with other military activities, were revealed based on data collected by Strava, a data service focused on collecting and analyzing fitness related data (Hsu, 2018). The discovery by an Australian National University student, who posted his findings on Twitter (Jernejcic & Kettani, 2019), prompted the U.S. military to reconsider its security policies in light of the potential impact to the safety of its personnel and the implication towards national security (Hsu, 2018). This highlights the criticality of understanding privacy concerns and the personal and national consequences pending should personal information be lost, stolen, and/or exposed.

Data is particularly at risk for two reasons. First, before transmission, data are stored on the wearable device, which, as noted, is often less than secure (Wei & Piramuthu, 2014). Second, once data has been transmitted, it now resides in a vendor and/or Cloud environment, accessible to the vendor or other third-party entities (Padyab & Ståhlbröst, 2018). Considering the context and purpose of the wearable device, the information stored will include personal information (Padyab & Ståhlbröst, 2018). At minimum, the information will represent monitored activities; however, it could also include Personally Identifiable Information (PII) and health-related data that the user may or may not want others to know. In addition to the concern that personal data might be accessible to known entities, the potential exists that information could be inadvertently lost, or worse, stolen by cybercriminals. Considering that security is often an afterthought when it comes to wearables, and IoT devices in general (Wei & Piramuthu, 2014), this latter concern of stolen information is a real threat that should not be marginalized.

## **Statement of the Problem**

The biome of the decision process is complex when it comes to venturing into the world of wearable technologies. Users must weigh the benefits with the risks. This is known as the privacy calculus (Smith et al., 2011). The benefits entice the individual to pursue the technology while the risks threaten to counter any potential gains through the disclosure and potential abuse of a person’s privacy. Today, many individuals are conscious and apprehensive of their private information with over 94% of Americans reporting to exhibit

such concern (Malhotra et al., 2004). Often, although concerned with their privacy, users will openly opt for the wearable and forego concerns with whether their information may or will be disclosed. This is known as the privacy paradox (Barth & de Jong, 2017; Norberg et al., 2007; Spiekermann et al., 2001). The privacy paradox combines reluctance to disclose with acceptance to disclose.

Past research focused on privacy in the realm of wearable technologies, such as (Bott, 2017; Doyle, 2019; Lehto & Lehto, 2017; Lidynia et al., 2017; Vitak et al., 2018), and other research efforts have investigated reasons and benefits for accepting the technology such as (Meyer et al., 2015; Preusse et al., 2017); however, little has been done to investigate the multi-dimensional role of privacy on the decision making process, particularly, the impact of the privacy calculus on the intention to disclose private information and the downstream effect regarding wearables' acceptance and use, specifically healthcare-related wearable devices. The present research sought to fill this gap by investigating constructs and relationships related to the privacy calculus and determining how the aggregate of those constructs influence (or fail to influence) a person's willingness to adopt a healthcare wearable device.

## **Objectives of the Dissertation**

The objective of the present research was to develop and test a research model specifically oriented towards the role of privacy in the realm of healthcare-related wearables' acceptance and use. Consequently, this endeavor sought to answer two research questions. The first question was:

*RQ1: To what extent does the implication of the privacy calculus impact intentions to disclose information in the process of adopting healthcare wearables?*

The privacy calculus represents the cost/benefit decision or privacy trade-off (Kehr et al., 2015) process assumed by the user to elect whether to disclose his or her personal information (Wilson & Valacich, 2012). Based on prior research, we conclude that this process imposes consequences towards intentions to use a wearable device (Smith et al., 2011). This question sought to measure the effect of the privacy calculus on a person's intention to disclose. The second question was:

*RQ2: To what extent is the privacy paradox observed in the context of healthcare wearable adoption decisions?*

The privacy paradox represents the situation where users contradict expressed concerns regarding privacy (Wilson & Valacich, 2012). In other words, in reference to the privacy calculus, users indicate a net concern regarding the disclosure of their personal information while still opting to disclose. This apparent paradox has been attributed to other moderating situational dynamics that override users' general privacy concerns, resulting in the decision to disclose (Wilson & Valacich, 2012). In search of the manifestation of the privacy paradox in healthcare-related wearables, RQ2 sought to measure the moderating effect of perceived health status on intention to disclose.

As noted, significant research has been directed towards understanding the dichotomy between an individual's privacy concerns and the willingness to disclose his or her personal information in a healthcare wearables environment. In addition, research has sought to understand factors influencing the acceptance and use of wearables. This research endeavor sought to study the potential of the privacy paradox as a contributor to disclosure and wearable device acceptance and use.



## CHAPTER 2

### LITERATURE REVIEW

Stimulated by the maturity of the Internet, Cloud computing, advancements in communications, and the miniaturization of sensor technologies, the phenomena of wearables continues to grow in both function and use (Perez & Zeadally, 2018). This is particularly relevant in the arena of personal health and wellbeing (Preusse et al., 2017), as well as in the workplace (Jayden, 2018; Kritzler et al., 2015; Yang et al., 2016). Although the benefits of wearables are real and their importance undisputed, their rapid development and utilization are sometimes at the expense of security and privacy concerns. It is urgent for innovators and researchers alike to take note and assume an offensive role to identify security and privacy concerns and address them in a manner apropos in protecting the consumer.

One of the necessities of any research project is to investigate past efforts in order to understand what is known about a particular topic and discover and contribute to the ongoing discussion and progression towards viable solutions to a related but new research problem (Machi & McEvoy, 2016). This section addresses this challenge by exploring the current state of knowledge regarding IoTs, wearables, and privacy with the objective of investigating the role of the privacy calculus and the manifestation of the privacy paradox regarding wearables acceptance and use. Related work in the context of wearables security and adoption will also be explored as a basis for the proposed theoretical model.

#### IoTs and Wearables

As previously noted, the ascription of the term *Internet of Things* (IoT) refers to Internet-enabled devices with a focus of providing a specific function or set of functions for an individual (Perez & Zeadally, 2018). Finding its roots as far back as 1964 with the teletypewriter and 1972 with the transmission of energy consumption by telephone (GAO, 2017), typical devices of today entail a host of “smart” devices including Blu Ray players, smart televisions, thermostats, refrigerators, garage doors, automobiles, and many other devices designed to enhance a consumer’s experience through the interconnectedness of a network and connectivity to the Internet (GAO, 2017). The Internet vastly expands the

capability and governance of devices by providing Cloud-enabled services and data storage as well as remote user administration and management.

Wearables are a specific category of IoTs referring to IoT devices that are worn and/or easily carried on the body by the user (Perez & Zeadally, 2018). Body locations include wrist, arm, finger, chest, thigh, head, upper body, and eye and wearable categories include fitness tracker, heart rate monitor, digital pedometer, and blood sugar monitor to name a few (GAO, 2017; Jayden, 2018). The construction of wearables consists of sensors, microprocessor, embedded storage, communication interface, and output devices (Perez & Zeadally, 2018). Sensors facilitate the purpose of the device, which is to monitor the biological functions of the body and, depending on their design, to treat and/or supplant those functions in order to enhance the quality of life of the individual (Ferraro & Ugur, 2011). The microprocessor and embedded storage units support the processing and storage needs of the wearable and the communication interface facilitates access to other wearables via a Personal Area Network (PAN) and/or to the Internet, forwarding data to a Cloud-based application (Perez & Zeadally, 2018). Finally, the wearable's output devices communicate status to the user via vibrations, sounds, and lights based on data collected from the sensors (Perez & Zeadally, 2018). Considering the complexities of the components supporting these relatively small devices and the personal nature of the data collected, security plays an important and critical role in keeping the user's information safe and sound from prying eyes.

Many, if not most, of today's wearables devices interface with Cloud-based applications (Perez & Zeadally, 2018). These wearable devices interface with applications and data repositories located in the Cloud. The Cloud is a general reference to Internet-based services existing in highly abstracted compute environments that are exceedingly scalable and can be provisioned almost instantly in response to need and usage (Catteddu et al., 2012). Considering the continuous and often unformatted nature of the data collected by wearable devices and transmitted to the Cloud application, Big Data repositories are the ideal solution for data storage. Big Data permits the collection, management, analysis, and extraction of large volumes of traditional (structured) and digital (unstructured) data (Arthur, 2013; Jernejcic & Kettani, 2019). This is particularly apropos considering the trend towards clinical Big Data, which is the collection and storage of clinical-based data into Big Data repositories for the purpose of data analysis, providing more substantial information for the purpose of

patient diagnosis and treatment (Amft, 2018). The integration of data from both clinical and wearable sources offers a significant advancement in medicine with the potential to advance biomedical knowledge (Amft, 2018).

While the advantages of the Cloud and Big Data are substantial in the realm of health-related wearables (Hahanov & Miz, 2015), the collection of personal data via the wearable device and the storage of such data on the Internet prompts numerous concerns (Jernejcic & Kettani, 2019). Who has access to the user's private data? Can the data be sold or made available to other third parties? How secure is the data? What measures are implemented to ensure the confidentiality, the integrity, and the availability of the data? Finally, will the user's private data be purged once no longer relevant (Ge et al., 2020)? These are vital questions that strike at the heart of concerns for privacy as well as general security. Understandably, apprehensions are justified considering hosting organizations have a vested interest in not only providing the wearables user with a service and a worthwhile experience, but ultimately in increasing profit (Uzialko, 2018). In order to garner consumer trust, wearables organizations must assure current and potential customers that their data is safe, and that privacy is of the utmost priority.

## **Privacy**

There are multiple definitions attributed to privacy. Merriam-Webster (2017) defines privacy as “freedom from unauthorized intrusion”. Based on a review of privacy-related research literature, Bélanger and Crossler (2011) summarized privacy as the autonomy one has over his or her own personal information. While one may attribute the term “personal information” to static information commonly employed to identify a person such as name, birthdate, and social security number, in regards to wearables, we argue the term expands to include biophysical characteristics as well as personal behavior. In the process of formulating an argument for legislative intervention regarding protection of privacy on the Internet, Clark (1999) identifies four dimensions of privacy that include person, personal behavior, personal communications, and personal data, all of which indeed encapsulate the various kinds of data that might be captured and synthesized by wearables. The motivation for Clark's (1999) research was the potential for lack of “trust in the information society” due to the

encroachment of cyberspace into the private lives of individuals with little or no protections regarding privacy (1999, p. 1).

Although somewhat “behind the eight ball” due to the aggressiveness of IoT and wearables innovation (Peppet, 2014), the uptick in concern for one’s privacy and wellbeing in the digital realm has manifested itself in the form of various laws, regulations, standards, and agreements. The Health Insurance Portability and Accountability Act (HIPAA), established in 1996 (Pulipaka, 2019), addresses the responsibilities of the health care provider, health plan, and businesses associates regarding the confidentiality of an individual’s health information (Glenn & Monteith, 2014; Peppet, 2014); however, not all data will fall under the protection of HIPAA since data generation is at the discretion of the consumer (Boysen et al., 2019; De Mooy & Yuen, 2017). Some leaders in the wearables and mobile app industries have established their own standards regarding the collection and use of wearables data (Polonetsky & Gray, 2017). Certain court rulings, such as the Third-Party Doctrine (resulting from two U.S. Supreme Court decisions) have weakened the case for legal protection of privacy for wearables regarding third-party access by affirming no Fourth Amendment protections (Scott, 2020). In addition, license agreements sometime erode privacy protection due to vague or open-ended declarations (Bergensstock, 2017). In that light, with the lens of legal protection somewhat gray, consumers need to be more diligent than ever to ensure they understand the privacy risks associated with wearables before volunteering their own personal and private information.

## **Privacy Calculus Theories**

Research has shown that wearable device consumers are indeed concerned with their privacy and the necessity for organizations to solicit informed consent before sharing with other third-party entities (Anaya et al., 2018). Privacy concerns are influenced by multiple factors including privacy experiences, privacy awareness, personality differences, demographic differences, culture, organizational trust, and state-based regulations (Smith et al., 2011). These factors inform the wearables user’s determination of risk regarding disclosing personal information. The perceived sensitivity and vulnerability of one’s information and the confidence level to effectively respond to corresponding threats also plays a significant role in determining risk (Kehr et al., 2015). This assessment of threats and

the perceived capacity to cope is known as the risk calculus (Zhang et al., 2018), which is informed by the Protection Motivation Theory (PMT) of threat and coping appraisals (Li, 2012). Perceived privacy risk (net risks) represents the conclusion of this appraisal process.

Risks associated with disclosing personal data are counterbalanced with the perceived benefits of healthcare wearables acceptance and use. Some of these benefits include but are not limited to fitness activity tracking (Meyer et al., 2015), blood pressure monitoring (Nadeem et al., 2015), heart rate monitoring (Muaremi et al., 2013), and other health-related activities focused on the health and wellbeing of the individual. Referred to as “personal metrics” (Page, 2015), the data collected via a multitude of embedded sensors offer the benefit of motivation, proactive detection, and, in some cases, early warning of life-threatening conditions. The process of weighing the costs/risks of disclosure against these benefits is recognized as the privacy calculus (Smith et al., 2011). As noted earlier, the privacy calculus represents the privacy trade-off (Kehr et al., 2015) process assumed by the user to elect whether to disclose his or her personal information (Wilson & Valacich, 2012). The joint representation of the risk calculus and privacy calculus theories is referred to as the dual-calculus model, which conceptualizes intentions of disclosure (Li, 2012).

Privacy theory research is not limited to the protection and disclosure of PII, but to personal health-related information as well. Shen (2019) created the Content-validated eHealth Trust Model in response to an investigation regarding the antecedents to trust, structural assurance, and a patient’s privacy perspective and the influence of trust and the privacy calculus (perceived benefit and perceived risk) on behavior. Zhang et al. (2018) integrated the dual-calculus model and PMT to investigate the antecedents and consequences of health information privacy concerns in the realm of online health communities. In addition to discovering the negative effects of response efficacy and self-efficacy and the positive effects of perceived vulnerability and severity on privacy concerns, the study found that Perceived Health Status (PHS) has a moderating effect on the relationships between perceived benefits and perceived risks and the intention to disclose Personal Health Information (PHI). It was found to weaken the influence of perceived benefits of informational and emotional support and strengthen the influence of perceived risk of health information privacy concerns on PHI disclosure intention.

Although the pledge of allegiance to the importance of privacy might be popular (Rainie et al., 2013), behavioral observance suggests that many are content to surrender privacy despite concerns for the welfare of their personal data (Williams et al., 2016). The motives for behavior towards the use of wearable devices despite risk-oriented intentions has been somewhat allusive (Gerber et al., 2018); however, Williams et al. (2016) identified five categories of antecedents contributing to the privacy paradox including education and experience, usability and design, privacy risk salience, social norms, and policies and configurations. Turow et al. (2015) observed that resignation to the loss of autonomy over personal privacy is a contributor to the privacy paradox. The Antecedents, Privacy Concerns, and Outcomes (APCO Macro) model as presented by Smith et al. (2011) presents the antecedents of privacy concerns as well as the influence of the privacy concern on the privacy calculus. The APCO model suggests that there is an opportunity for the privacy paradox to manifest itself between user intentions and user behavior since most research measures the former and not the latter. Borrowing from the old cliché that actions speak louder than words, consumers' intentions to error on the side of safety by intending to avoid disclosure is not necessarily representative of actual behavior, which is to choose the wearable device despite leanings towards privacy (Page, 2015).

## **Privacy in Wearable Technology**

The significance of privacy in the wearable technology domain has prompted multiple studies. Bott (2017) investigated the role of the privacy calculus as it pertains to personal mobile devices. The author developed a Personal Mobile Device Privacy Calculus model with the intention of predicting and explaining privacy disclosure behavior. Developed in the context of actual behavior, testing of the model revealed that a person's resignation to the perception that he or she has no control over disclosure contributes to actual disclosure. Vitak et al. (2018) researched the effect of concerns regarding general privacy and user-generated data in the realm of fitness trackers on users' perception of personal fitness information privacy. They observed a positive relationship between a user's concern for privacy and the value a user places on fitness data. Although the above noted studies were significant in the realm of privacy and wearable technology, they offered little in the way of the effect of privacy on technology acceptance.

Gao et al. (2015) performed an empirical study on the adoption of healthcare wearable technologies. In their empirical quest to discover and test antecedents of adoption of healthcare wearable devices, they found that fitness device users were most influenced by hedonic motivation, functional congruence, social influence, perceived privacy risk, and perceived vulnerability to a health risk. In contrast, they discovered that medical device users were more influenced by perceived expectancy, self-efficacy, effort expectancy, and perceived severity of health risk. Pulipaka (2019) investigated the impact of privacy concerns and user perceptions on healthcare wearable devices. The author discovered that performance expectancy, effort expectancy, facilitating conditions, and trust strongly predicted device usage intentions. Harper (2016) investigated the role of security awareness on the decision of consumers to adopt IoT devices finding that awareness had a significant influence; however, it was not the primary factor of adoption. Lehto and Lehto (2017) investigated the perception of users towards the sensitivity of their health information and their willingness to share such information with appropriate parties. Based on the results of ten interviews, the researchers found that users in general were not concerned with information collected by wearables as it was perceived to be unimportant (not sensitive) and not private. Consequently, decisions to accept and use wearables appeared to not be based on concerns of privacy; however, the small sample size of ten individuals and the lack of statistical analysis in the study prompts concern for the need for further research to support the conclusions. Finally, Scott (2020) reported on research concerning the acceptance and use of smartwatch wearables in correlation with concerns of privacy. It was discovered that privacy awareness significantly contributed to the adoption of smartwatches and that privacy concerns posed a negative influence on intention to use.

The above identified studies focus on privacy in the realm of wearable technologies with four out of seven specifically targeting healthcare devices. While they contribute towards the discussion of privacy and the acceptance and use of wearables, there remains a gap regarding the role played by the privacy calculus and the inter-play of other factors on the decision-making process. Of the four studies targeting healthcare devices, none of them specifically target the role of the privacy calculus and the impact of the privacy paradox on the decision-making process, particularly, the summarized influence of privacy and disclosure on healthcare-related wearables' acceptance and use. In addition, while the Gao et al. (2015)

study does consider the impact of perceived health threat on intention to adopt, none of the acceptance-related studies consider the influence of perceived health status on intention to disclose.

Considering the importance of healthcare-related wearable devices in the effort to contribute to improved health and wellbeing, it is critical to comprehensively consider privacy on adoption as opposed to a cursory approach. It is equally important to consider the role of the status of one's health in the decision to disclose the information warranted by the wearable device (Zhang et al., 2018). The present research sought to fill this gap by investigating constructs and relationships related to the risk calculus, the privacy calculus, health status, and the presence of the privacy paradox, in combination with other acceptance-related constructs, in determining how the aggregate of those constructs influence (or fail to influence) a person's readiness to participate in the use of healthcare wearable devices. This was accomplished via the adaptation and merging of the two aforementioned research efforts of Zhang et al. (2018) and Gao et al. (2015) with the former primarily informing health-related privacy and the latter primarily informing healthcare-related wearables acceptance and use. The first model was extended via adaptation of health privacy disclosure in a wearables context. The second model was extended via expansion of its privacy component to a more complete and expanded health information context as well as consideration of the moderation of perceived health status on the newly introduced privacy calculus.



## CHAPTER 3

### THEORETICAL MODEL

Figure 1 represents the current research model. The objective of the model was multifold. First, we sought to capture and measure the theoretical constructs regarding factors influencing the adoption and use of wearable devices. Second, we sought to capture and measure the factors that influence intention to disclose privacy information. The composite of the latter factors, which includes the assessment of risk (risk calculus) and the balance of risk and benefits of disclosure and their influence on a user's intention to disclose (privacy calculus), is representative of the dual calculus model. Finally, we sought to measure the moderated effect of perceived health status (perceived health vulnerability and perceived health severity) on the relationship of perceived privacy and intention to disclose (privacy paradox).

The theoretical foundation of the research model was informed by multiple technology acceptance models, the Protection Motivation Theory (PMT), the Health Belief Model (HBM), and multiple privacy calculus theories. The core objective of technology acceptance models is to predict the use of technology-based systems (Davis et al., 1989). Researchers have developed many models and theories over the past several decades to explain acceptance, three of which have garnered significant popularity in the annals of technology acceptance research. First, the Technology Acceptance Model (TAM), developed by Davis (1986) with a foundation based on Fishbein's and Ajzen's (1975) Theory of Reasoned Action (TRA), postulates that Actual System Usage (AU) is based on Behavioral Intention to Use (BI) and BI is influenced by the Perceived Usefulness (PU) of the technology plus the Attitude (AT) towards using it. In addition, AT is influenced by PU along with the additional determinant of Perceived Ease of Use (PEOU). The constructs of PU and PEOU, in turn, are influenced by other external variables. TRA's construct of Subjective Norm (SN) was thoughtfully excluded from the TAM model due to the lack of understanding (at the time) surrounding proper placement of its effects. It is important to note that additional evaluation and refinement of TAM resulted in just three constructs including PU, PEOU, and BI (Davis

et al., 1989; Venkatesh et al., 2003). Finally, TAM2, an extension of TAM, reconsidered SN as a significant contributor to technology acceptance (Venkatesh & Davis, 2000).

Second, the Unified Theory of Acceptance and Use of Technology (UTAUT), developed by Venkatesh et al. (2003), is informed by eight previous theories/models asserting that BI is predicted by Performance Expectancy (PE), Effort Expectancy (EE), and Social Influence (SI). The construct AU is predicted by Facilitating Conditions (FC) and BI. Informing models include TRA, TAM, the Motivational Model (MM), the Theory of Planned Behavior (TPB), a model combining TAM with TPB (C-TAM-TPB), the Model of PC Utilization (MPCU), the Innovation Diffusion Theory (IDT), and the Social Cognitive Theory (SCT). All relationships are moderated by Gender (G), Age (AGE), Experience (EX), and Voluntariness of Use (VU) with the exception of the relationship between BI and AU. The authors' findings were noteworthy, resulting in an adjusted  $R^2$  of 69% for the original inquiry and 70% for subsequent testing, significantly beating the performance of the individual contributing models.

The third significant technology acceptance model is the extended UTAUT model (UTAUT2), which was developed by the creators of the UTAUT theory (Venkatesh et al., 2012), attempts to improve UTAUT through the addition of three new constructs including Hedonic Motivation (HM), Price Value (PV), and Habit (HT). Moderators are reduced to G, AGE, and EX, removing VU from the model. The results proved to be significant with an increase in explained variance regarding behavioral intention (74% compared to 56% for UTAUT) and actual technology use (52% compared to 40% for UTAUT). We used this latter extended model to inform the research model of the current research effort.

Often, a person's decision to adopt technology is influenced by threats associated with its adoption (Gao et al., 2015). The Protection Motivation Theory (PMT) addresses this phenomenon by seeking to explain a person's ability to cope and respond to a threat (Woon et al., 2005). A person's response is grounded on the net effect of the person's threat appraisal and coping appraisal. The PMT theory was originally developed to model a person's response process to a physical event that would influence his or her health (Rogers, 1975); however, since its inception, it has been extensively utilized in the Information Systems (IS) research space. As opposed to addressing one's physical health, the theory is instead applied regarding the threat to one's wellbeing resulting from using technology and their willingness

to adopt technology or technology-related practices and processes (Boysen et al., 2019; Gao et al., 2015; Herath & Rao, 2009). We considered PMT in its application towards decisions to disclose private information.

The research model is comprised of sixteen constructs. These include Perceived Threat Vulnerability (PTV), Perceived Threat Severity (PTS), Response Efficacy (REF), Task Self-Efficacy (SEF), Perceived Privacy Risk (PPR), Hedonic Motivation (HMO), Performance Expectancy (PEX), Effort Expectancy (EEX), Social Influence (SIN), Technology Self-Efficacy (TSE), Functional Congruence (FCG), Perceived Health Status (PHS), Intention to Disclose (ITD), Perceived Health Vulnerability (PHVU), Perceived Health Severity (PHSE), and Intention to Adopt (ITA) healthcare wearable devices. The current model extended Gao et al.'s (2015) conceptual model, which was constructed to examine factors related to the adoption of healthcare wearable devices, and Zhang et al.'s (2018) conceptual model, which was constructed to examine factors influencing health information-related privacy concerns.

Adopted from PMT, Perceived Threat Vulnerability (PTV) concerns an individual's evaluation of how likely they are to succumbing to privacy threats (Zhang et al., 2018). We hypothesize that:

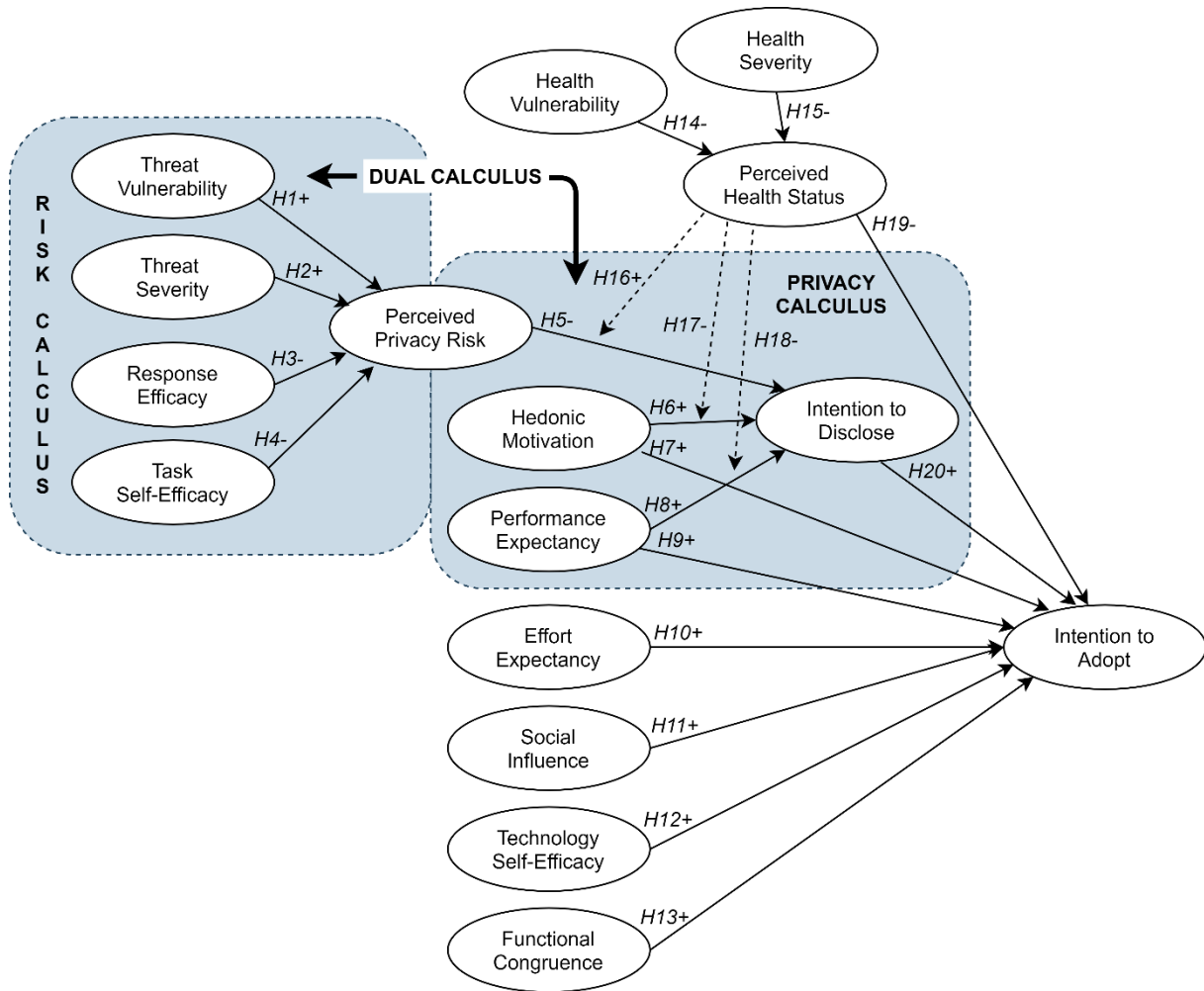
*H1. Perceived threat vulnerability is positively related to an individual's overall state of perceived privacy risk in the realm of healthcare wearable devices.*

Adopted from PMT, Perceived Threat Severity (PTS) concerns an individual's evaluation of the severity of consequences due to succumbing to privacy threats (Zhang et al., 2018). We hypothesize that:

*H2. Perceived threat severity is positively related to an individual's overall state of perceived privacy risk in the realm of healthcare wearable devices.*

Adopted from PMT, Response Efficacy (REF) concerns an individual's evaluation of the effectiveness of current protective measures to prevent succumbing to privacy threats (Zhang et al., 2018). We hypothesize that:

*H3. Response efficacy is negatively related to an individual's overall state of perceived privacy risk in the realm of healthcare wearable devices.*



**Figure 1:** Research Model (adapted from Zhang et al. (2018) and Gao et al. (2015))

Adopted from PMT, Task Self-Efficacy (SEF) concerns an individual's evaluation of his or her ability to effectively implement the appropriate tasks necessary to respond to privacy threats (Zhang et al., 2018). We hypothesize that:

*H4.* Task self-efficacy is negatively related to an individual's overall state of perceived privacy risk in the realm of healthcare wearable devices.

Perceived Privacy Risk (PPR) represents the measurable representation of the privacy risk perceived by an individual regarding use of the wearable device. It is based on four dimensions of privacy concerns including collection, errors, secondary use, and unauthorized access to one's information (Smith et al., 2011). We hypothesize that:

*H5.* Perceived privacy risk is negatively related to an individual's intention to disclose privacy information in the realm of healthcare wearable devices.

Adopted from UTAUT2, Hedonic Motivation (HMO) represents the intrinsic motivation experienced by the user (Venkatesh et al., 2012). Intrinsic motivation is concerned with the pleasure one experiences by using the wearable device (Brown, 2005). We hypothesize that:

*H6.* Hedonic motivation is positively related to an individual's intention to disclose privacy information in the realm of healthcare wearable devices.

*H7.* Hedonic motivation is positively related to an individual's intention to adopt healthcare wearable devices.

Adopted from UTAUT, Performance Expectancy (PEX) is concerned with the degree of benefit expected by the user regarding use of the wearable device (Venkatesh et al., 2003). We hypothesize that:

*H8.* Performance expectancy is positively related to an individual's intention to disclose privacy information in the realm of healthcare wearable devices.

*H9.* Performance expectancy is positively related to an individual's intention to adopt healthcare wearable devices.

Adopted from UTAUT, Effort Expectancy (EEX) represents the level of effort regarding ease of use and complexity expected when using the wearable device (Venkatesh et al., 2003). We hypothesize that:

*H10.* Effort expectancy is positively related to an individual's intention to adopt healthcare wearable devices.

Adopted from UTAUT, Social Influence (SIN) represents the perceived emphasis of others deemed important to the user regarding use of the wearable device (Venkatesh et al., 2003). We hypothesize that:

*H11.* Social influence is positively related to an individual's intention to adopt healthcare wearable devices.

Technology Self-Efficacy (TSE) is concerned with a user's perception or belief regarding their ability to use specific functions of the wearable device (Gao et al., 2015). Although TSE was dropped from the UTAUT model regarding general technology acceptance, it has been demonstrated to influence intentions to adopt in the realm of emerging health technologies (Sun et al., 2013). We therefore include it in the current research and hypothesize that:

*H12.* Technology self-efficacy is positively related to an individual's intention to adopt healthcare wearable devices.

Adapted from self-congruency theory (Huber et al., 2010), Functional Congruence (FCG) captures the perceived suitability of the wearable device to satisfy expectations regarding functional and basic product-related needs (Gao et al., 2015; Wenling et al., 2015). In contrast to PEX, which concerns the perceived basic effectiveness of the device to fulfil its stated purpose, FCG captures the aggregated quality of the wearable device, in terms of the level of comfort in wearing it, its durability, and price acceptance (Gao et al., 2015). In other words, although it may perform as expected (PEX), it also must be practical and applicable in light of the user's personal encounter and utilization of the device. We hypothesize that:

*H13.* Functional congruence is positively related to an individual's intention to adopt healthcare wearable devices.

Informed by PMT, Perceived Health Vulnerability (PHVU) represents the user's perception regarding the likelihood of succumbing to the health threat(s) directly or indirectly addressed by the wearable device (Gao et al., 2015). We hypothesize that:

*H14.* Perceived health vulnerability is negatively related to an individual's overall state of perceived health status in the realm of healthcare wearable devices.

Informed by PMT, Perceived Health Severity (PHSE) is concerned with the user's perception regarding the extent of the health threat(s) directly or indirectly addressed by the wearable device (Gao et al., 2015). We hypothesize that:

*H15.* Perceived health severity is negatively related to an individual's overall state of perceived health status in the realm of healthcare wearable devices.

Perceived Health Status (PHS) is one's perception of their level of illness and wellness (Jung A Kim et al., 2015), which has been found to moderate privacy/disclosure relationships (Zhang et al., 2018). Therefore, we posit a similar moderating effect in the current research model. Informed by HBM (Janz & Becker, 1984), which asserts that self-protective behavior is motivated by increases in perceived risk (Deng & Liu, 2017), we posit that PHS is an antecedent to intention to adopt, asserting that higher levels of PHS (better health) have a negative influence on adopting healthcare wearables. We hypothesize that:

*H16.* Perceived privacy risk has a stronger influence on intention to disclosure with high levels of perceived health status.

*H17.* Hedonic motivation has a weaker influence on intention to disclosure with high levels of perceived health status.

*H18.* Performance expectancy has a weaker influence on intention to disclosure with high levels of perceived health status.

*H19.* Perceived health status is negatively related to an individual's intention to adopt healthcare wearable devices.

Intention to Disclose (ITD) identifies the intentions of the user to disclose personal information as required when using the healthcare wearable device (Zhang et al., 2018). We hypothesize that:

*H20.* Intention to disclose is positively related to an individual's intention to adopt healthcare wearable devices.

Intention to Adopt healthcare wearable devices (ITA) identifies the intentions of the user to adopt a healthcare wearable device (Gao et al., 2015).

## **CHAPTER 4**

### **RESEARCH METHODOLOGY**

#### **Survey Instrument**

The survey instrument (Appendix A) consisted of a succession of questions where respondents were requested to submit responses in the form of a Likert seven-point scale with one representing “strongly disagree” and seven representing “strongly agree” (Dittrich et al., 2007). The construct PHS was the one exception, which was measured based on a single question, which queried the participant regarding whether they perceived their health to be “very poor”, “poor”, “fair”, “good”, or “excellent”. Past research has shown that the self-rating of one’s general health condition has been observed to demonstrate significant performance and is considered an acceptable alternative to multiple item measurements (Zhang et al., 2018). Each question measured a specific model construct and had been validated and tested based on prior research. It was vital each question stand on its own without influence of other questions in order to avoid common methods bias, a threat to construct validity (Straub et al., 2004). Key demographic information was also collected including use, gender, age range, and education.

#### **Data Collection**

Primary data was collected employing surveys circulated to a sample population of diverse individuals who have genuinely contemplated using healthcare-related wearable devices. It was vital to query a large enough sample to enable generalizing back to the general population (Roberts, 2012). A minimum of 200 responses were projected. Qualtrics was the tool of choice for building the survey and for assistance with survey distribution. The target audience for the survey were persons 18 years of age and older who have used, are using, or have considered using healthcare wearable devices. While demographic information was solicited such as use, gender, age range, and education level, no specific demographics were targets of the survey. In addition, no identifiable information was collected in order to ensure audience anonymity. The survey was distributed via email, social media and related



discussion board forums. Social media distribution included LinkedIn, Facebook, Twitter, Reddit, and Pinterest. There was a pledge to donate \$0.50/survey participant to a not-for-profit disaster-relief organization with a maximum donation of \$500.

## **Analysis**

After assessing data for missing values, Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied to discern cause and affect relationships through estimation of the measurement and structural models and testing of the hypotheses. While first generation multivariate techniques included cluster analysis, exploratory factor analysis, and multidimensional scaling, current (second generation) techniques are focused on the use of PLS-SEM (Hair et al., 2017). The PLS-SEM method, one of two types of Structural Equation Modeling (SEM), was chosen for this research effort due to its recognized aptitude towards exploratory research in the social science arena, and for its fortitude towards estimating causative relationships between constructs (Hair et al., 2017). Covariance-Based SEM (CB-SEM), the other SEM type, is specific to confirmation-based research to test existing theories. CB-SEM prefers a large sample sizes and data that is normally distributed whereas PLS-SEM is capable of handling smaller sample sizes and makes no assumptions regarding data distribution (Wong, 2013). The SmartPLS version 3.3.3 (Ringle et al., 2015) was chosen as the software tool for PLS-SEM estimation due to its acceptance among the academic community (Wong, 2019) and for its ease of use, graphical interface, and efficiency in estimation. See Appendix B for a list of parameters used for PLS-SEM estimation using SmartPLS.

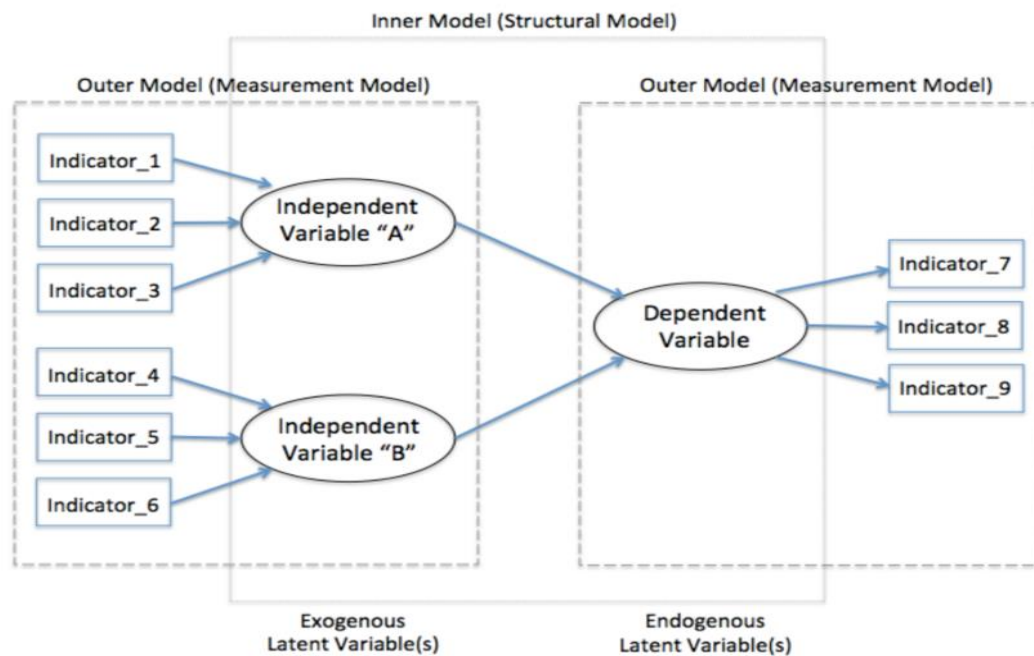
We selected PLS-SEM, also referred to as variance-based SEM (Hair et al., 2020), as the SEM of choice over CB-SEM due to multiple reasons. First, our project is exploratory in nature as we seek to investigate, measure, and predict relationships between latent constructs (Hair et al., 2017; Hair et al., 2011; Hair et al., 2020). One of the benefits of PLS-SEM, specifically Confirmatory Composite Analysis (CCA), is that it is both exploratory and confirmatory, eliminating the prerequisite for Exploratory Factor Analysis (EFA) (Hair et al., 2020; Kianto et al., 2019). Second, we can still acquire significant results in the presence of non-normality, heteroscedasticity, and/or error term autocorrelation issues (Wong, 2019). Third, our research model contains multiple moderating relationships, which is effectively

addressed using PLS-SEM (Wong, 2019). Fourth, PLS-SEM is considered appropriate for smaller sample sizes (Hair et al., 2020). And fifth, our model is somewhat complex with sixteen variables and up to eight relationships with a single dependent variable (Hair et al., 2017; Hair et al., 2020). Each of these characteristics are supported by PLS-SEM and thus make it an ideal candidate for our research effort. In addition, the PLS-SEM modeling approach has grown in popularity, particularly in the behavioral science and marketing domains, and has successfully endured the scrutiny of many relevant top-tiered journal peer reviews (Wong, 2019).

The PLS-SEM structural equation model is comprised of two primary architectural components including the measurement model and the structural model (Wong, 2013). Figure 2 presents an example of a PLS-SEM model. The measurement model, also referred to as the outer model, represents relationships between observed indicators and their corresponding latent variable constructs. A measurement model can be reflective or formative depending on its indicators (Hair et al., 2013). Reflective indicators reflect changes in the latent variable and are highly correlated and interchangeable (Hair et al., 2011; Hair et al., 2020; Wong, 2013). They are precipitated or influenced by the latent variable they are proposed to measure (Sarstedt et al., 2016). Graphically, they are identified with relationships that point from the latent variable to the indicator. Formative indicators cause changes in the latent variable and have varying levels of correlation and are not interchangeable (Hair et al., 2011; Wong, 2013). Graphically, they are identified with relationships that point from the indicator to the latent variable. Related coefficients for these relationships are referred to as outer loadings for reflective relationships and outer weights for formative relationships (Hair et al., 2011). Our research model is reflective in nature.

The structural model, also referred to as the inner model, represents relationships between independent (exogenous) latent variable constructs and corresponding dependent (endogenous) latent variable constructs. Independent latent variables are categorized as exogenous variables and dependent latent variables are categorized as endogenous variables. Graphically, they are identified with relationships that point from the independent variable to the dependent variable. Related coefficients for these relationships are referred to as path coefficients, which represent the effect of an independent variable on a dependent variable. Based on the sum effect of all independent variables pointing to a dependent variable,

Coefficient of Determination ( $R^2$ ) values are calculated, representing the total variance explained by the independent variables on the related dependent variable (Wong, 2019).



**Figure 2:** Example PLS-SEM Model (Wong, 2013)

The measurement and structural models were examined for validity and reliability. Construct validity, specifically convergent validity and discriminant validity, gauges how well one operationalizes the research model under evaluation (Drost, 2011). Indicator loadings of 0.40 or higher is the criteria for indicator acceptance in exploratory studies (Hair et al., 2013); however, 0.70 is optimal to ensure accounting for a minimum of 50% of the variance by the matching construct (Gao et al., 2015). Indicators with loadings between 0.40 and 0.70 are candidates for deletion only if doing so results in a higher Composite Reliability (CR) or Average Variance Extracted (AVE) (Hair et al., 2017). Indicator reliability, calculated based on the square of the loadings, is the measure of shared variance among indicators (Hair et al., 2019). A minimum value of 0.50 is considered acceptable (Hair et al., 2017).

In addition to satisfactory indicator loadings and reliability, an AVE of 0.50 or higher (Dinev & Hart, 2006) is the criteria to ascertain convergent validity, which is concerned with how well measures meant to converge, do converge. The reliability of the latent constructs was determined based on Cronbach's Alpha and CR measurements. Cronbach's Alpha has been the traditional method for validating reliability; however, research suggests that it tends

to be too conservative for PLS-SEM analysis and that CR is a more appropriate option (Wong, 2019). Consequently, both Cronbach's Alpha and CR were utilized in this study. Cronbach's Alpha score above 0.60 and a CR of 0.70 or higher is the criteria for adequate reliability (Hair et al., 2017). Two criteria are used to verify discriminant validity, including a Heterotrait-Monotrait Ratio of Correlations (HTMT) score below the conservative cutoff value of 0.85 (Hair et al., 2020; Wong, 2019) and an HTMT interval not containing the value of one, assuming a confidence level of 95% (Hair et al., 2017; Wong, 2019).

Performance analysis of the structural model included multiple areas of assessment. Coefficient of Determination ( $R^2$ ) values of 0.75, 0.50, and 0.25 are the criteria for determining whether each endogenous latent variable is considered substantial, moderate, or weak, respectively (Hair et al., 2011). The purpose of  $R^2$  is to identify the total variance of the endogenous latent variable explained by the contributing exogenous latent variables (Hair et al., 2017). A Variance Inflation Factor (VIF) of lower than 5.0 is the criteria for concluding that multicollinearity is not an issue (Hair et al., 2013). Multicollinearity measures the relationship between independent variables and to what extent they might vary in coordination with one another (Gefen et al., 2000). Path coefficient estimates are assessed for statistical significance utilizing the bootstrapping method (Hair et al., 2013). The absolute value of the coefficient determines the relative influence of the exogenous latent variable on the endogenous latent variable, with a positive value having a positive effect and a negative value having a negative effect on the endogenous latent variable.

Model  $f^2$  effect sizes of 0.02, 0.15, and 0.35 are the criteria for determining whether the impact or effect of an exogenous latent variable on a corresponding endogenous latent variable is small, medium, or large, respectively, with a value below 0.02 being of no effect (Hair et al., 2013). For moderation analysis,  $f^2$  effect sizes of 0.005, 0.01, and 0.25 are the criteria for determining small, medium, or large effect, respectively, regarding the moderating influence on corresponding exogenous/endogenous variable relationships (Hair et al., 2017; Kenny, 2018). Model  $f^2$  effect size is determined by evaluating the change in  $R^2$  when an exogenous latent variable is omitted (Hair et al., 2017). Finally, the predictive relevance of the model is exhibited using the Stone-Geisser's  $Q^2$  value. Blindfolding, with an Omission Distance (OD) of 7, is the technique utilized for calculating the Stone-Geisser's  $Q^2$  value (Wong, 2019).  $Q^2$  values of 0.02, 0.15, and 0.35 are the criteria for determining predictive

relevance of weak, moderate, or strong, respectively (Hair et al., 2013). Although potentially conservative, a Standardized Root Mean Square Residual (SRMR) value less than 0.08 is the criteria for model fit; however, for PLS-SEM research such as ours, model fit analysis is still in its infancy and is currently considered ambiguous as an assessment measure (Hair et al., 2017; Hair et al., 2020).

External validity refers to how well generalizations may be employed towards the larger population (Petursdottir & Carr, 2018). It is supported through random selection of the general population (Bhattacharjee, 2012). This study has addressed external validity through the random polling of wearable device consumers.

A significance factor of 0.05 has been employed as appropriate to assess the statistical significance of our findings. Determination of statistical significance of each component of assessment is ascertained based on the bootstrapping procedure utilizing a large number of subsamples (Wong, 2019). In this case, 5,000 subsamples were created, randomly selected from the original dataset. SmartPLS estimation was configured to stop after a maximum of 300 iterations or after convergence had been established. Convergence in less than the maximum is the criteria for an acceptable estimation with the assumption of a significant sample size, no or non-influential outliers, and an acceptable quantity of similar values (Wong, 2019).

## CHAPTER 5

### RESULTS

The objective of this nonexperimental quantitative research effort was to explore the role privacy plays in the acceptance and use of healthcare wearables, and to explore the relevance of the privacy calculus and the privacy paradox in the wearables acceptance process. A review of the literature highlighted notable efforts in the privacy, healthcare, and wearables research space. These efforts have resulted in important and relevant theoretical explanations in their prospective areas; however, there was a gap discovered regarding the application of those findings in a more comprehensive and extensive focus specific to privacy and wearable acceptance and use.

Capitalizing on the gains of previous efforts, this research effort sought to extend current theoretical understanding of privacy and technology acceptance to a broader and more comprehensive model, including drivers of privacy, drivers of acceptance, and the intersection of the two when it comes to healthcare-related wearables. This resulted in the afore mentioned research model (Figure 1) consisting of sixteen related constructs. Using the data collected via the survey instrument, this section discusses the results of the data collection process and reports on its findings. First, we present a description of the sample including sample size, missing data, and outliers. Second, we confer the results of a descriptive analysis of the data, including construct measurements and demographics. And third, we discuss the results of statistical analysis of the measurement and structural models.

#### **Description of the Sample**

As previously noted, data collection consisted of distribution of a survey instrument via email, social media outlets, and related discussion boards. The instrument consisted of 58 measurements, including 52 Likert-based questions, one interval-based measurement, and five demographics. Qualtrics was utilized to build, test, and deploy the survey to the target audiences (upon IRB approval). At conclusion, a total of 225 (N=225) responses were collected. Table 1 provides a summary of a description of the sample, highlighting missing values and outliers for each construct indicator.

**Table 1:** Sample Description

Latent Variable	Indicators	N	Missing Values	% Missing Values	Outliers	
					3rd/1st Quartile +/- 1.5 * IQR	3rd/1st Quartile +/- 3.0 * IRQ (Extreme)
PTV	PTV1	225	0	0.0%		
	PTV2	225	0	0.0%		
	PTV3	225	0	0.0%		
	PTV4	225	0	0.0%		
PTS	PTS1	225	0	0.0%		
	PTS2	225	0	0.0%		
	PTS3	225	0	0.0%		
	PTS4	225	0	0.0%		
REF	REF1	225	2	0.9%		
	REF2	225	2	0.9%		
	REF3	225	2	0.9%		
SEF	SEF1	225	0	0.0%		
	SEF2	225	1	0.4%		
	SEF3	225	0	0.0%		
	SEF4	225	0	0.0%		
PPR	PPR1	225	0	0.0%		
	PPR2	225	0	0.0%		
	PPR3	225	0	0.0%		
HMO	HMO1	225	0	0.0%	47, 50, 124, 183, 193, 204	24, 175
	HMO2	225	0	0.0%	17, 47, 111, 124, 183, 184, 193	24, 175
	HMO3	225	0	0.0%		
	HMO4	225	0	0.0%	76, 111, 118, 135, 155, 173	24, 175
PEX	PEX1	225	1	0.4%	63, 88, 99, 140, 146, 147, 217	34, 61, 175, 204
	PEX2	225	0	0.0%	99, 153, 157, 184, 196, 197	24, 175
	PEX3	225	0	0.0%	2, 34, 99, 111, 126, 146, 153	24, 175
EEX	EEX1	225	0	0.0%	125, 128, 131, 178, 183	15, 24
	EEX2	225	0	0.0%		24
	EEX3	225	2	0.9%		24
	EEX4	225	0	0.0%	167, 186, 200, 208	24
SIN	SIN1	225	1	0.4%	95, 146, 171, 175, 181, 182, 184, 187, 204, 208	
	SIN2	225	1	0.4%	95, 146, 175, 204	
	SIN3	225	0	0.0%	146, 159, 164, 171, 175, 182, 204, 208, 210, 217	
TSE	TSE1	225	1	0.4%	44, 118, 146, 217	24, 204
	TSE2	225	2	0.9%	131	24, 204
	TSE3	225	0	0.0%	18, 70, 165, 171, 173, 208, 210	24, 204
FCG	FCG1	225	0	0.0%	144, 146, 158	24
	FCG2	225	0	0.0%		
	FCG3	225	0	0.0%		
	FCG4	225	1	0.4%	83, 133, 144, 155, 172, 195, 203	24, 76, 197
PHVU	PHVU1	225	1	0.4%		
	PHVU2	225	1	0.4%		
	PHVU3	225	1	0.4%		
PHSE	PHSE1	225	1	0.4%		
	PHSE2	225	1	0.4%		
	PHSE3	225	2	0.9%		
ITD	ITD1	225	0	0.0%		
	ITD2	225	1	0.4%		
	ITD3	225	0	0.0%	101, 115, 128, 147, 158, 169, 217	170, 175, 192
ITA	ITA1	225	0	0.0%	72, 80, 160, 175	
	ITA2	225	1	0.4%		
	ITA3	225	0	0.0%	72, 80, 175, 204	
	ITA4	225	0	0.0%		
PHS	PHS	225	0	0.0%		82, 133, 175, 202, 203, 204, 215, 217, 218

The examination of missing data and non-response bias is important for PLS-SEM analysis in order to instill confidence in the results and to avoid highly biased results when it comes to heterogeneity analysis (Hair et al., 2013). Three of the of the cases (57, 116, and 185) included missing values for all indicators for one or more constructs. These cases were removed due to the inability to measure specific constructs for those specific cases. For the 222 remaining cases, there was one case with two missing values (separate constructs), or 4%, and eleven cases with one missing value per case, or 2%, for a total of 13 missing values, or 0.11%, for the entire dataset. The maximum number of missing values for any specific indicator was 0.9%. Consequently, mean replacement was selected as the preferred method for missing value replacement during PLS-SEM analysis, since 0.9% falls well below the recommended 5% threshold (Hair et al., 2017).

Using IBM SPSS for outlier analysis, outliers were discovered for 22 of the 53 indicators. There were 109 outliers found to be greater than the 3<sup>rd</sup>/1<sup>st</sup> quartile  $\pm 1.5 * \text{interquartile range (IQR)}$  but less than the 3<sup>rd</sup>/1<sup>st</sup> quartile  $\pm 3.0 \text{ IRQ}$ . There were 41 outliers found to be greater than the 3<sup>rd</sup>/1<sup>st</sup> quartile  $\pm 3.0 * \text{IQR}$ . These are considered extreme outliers (NIST, 2013). After a review of the data, there was found to be no apparent explanation for these outliers (e.g., entry errors) apart from recording the actual opinion of the respondent (Hair et al., 2017). Consequently, no adjustments or deletions were applied in the case of these outliers. This decision was later supported when estimating the model, which completed in three iterations, substantially less than the 300 iterations configured as the stop criterion (Wong, 2019). This also confirmed the resulting sample size of 222, which is sufficient for PLS-SEM analysis when seeking a statistical power of 80%, a significance level of 0.01, and a minimum Coefficient of Determination ( $R^2$ ) of 0.100 when estimating models with a maximum of ten exogenous variables pointing to a single endogenous variable (Hair et al., 2017).

## **Descriptive Analysis**

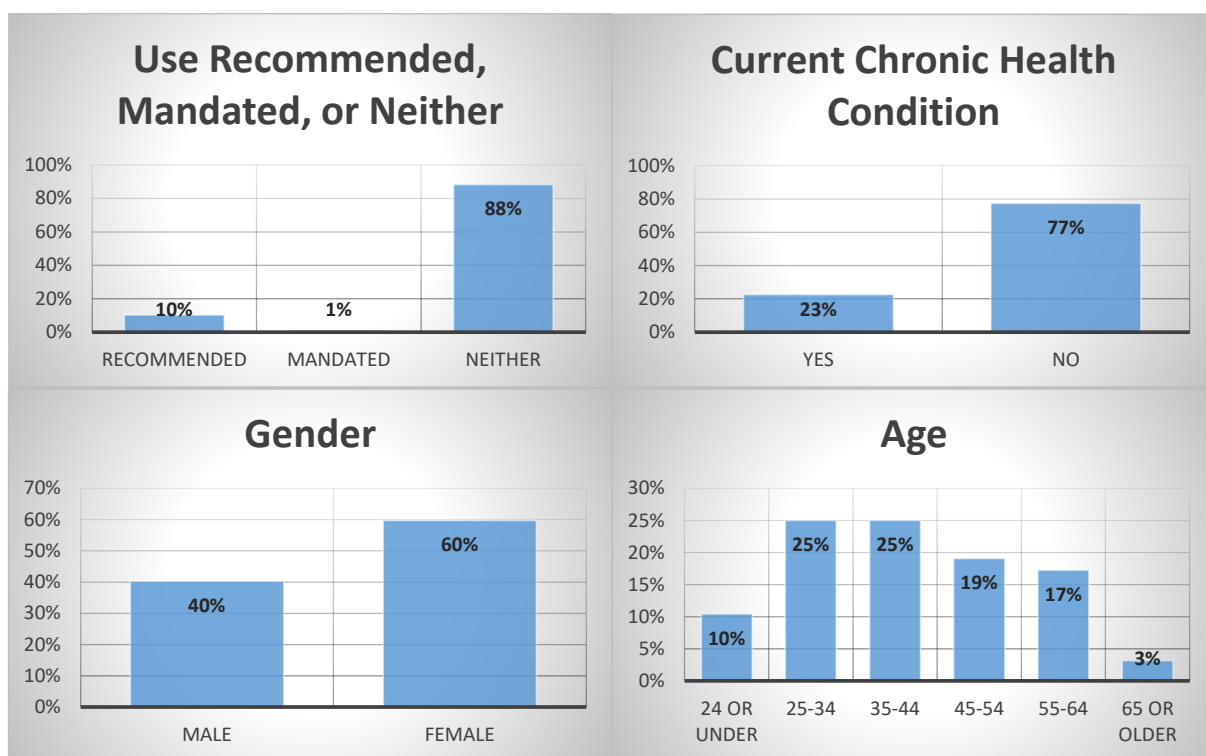
Table 2 represents the statistical measures of central tendency and dispersion for demographic related data. Figures 3 and 4 provide graphical representations of the distribution of the data. First, we observe a mean of 2.78 and a standard deviation of 0.617 for USE, which identified whether the use of a wearable was recommended (1) or mandated (2) by a



physician, or neither recommended or mandated (3). We note that 10% of use was recommended, 1% was mandated, and 88% was neither recommended or mandated. Second, we observe a mean of 1.77 and a standard deviation of 0.419 for CHC, which identified respondents as having or not having a current chronic health condition. We note that 23% of respondents did have a current chronic health condition and 77% did not at the time of taking the survey. Third, we observe a mean of 1.6 and a standard deviation of 0.492 for GDR, which identified the gender of the participant. We note that 40% of the participants were male and 60% were female.

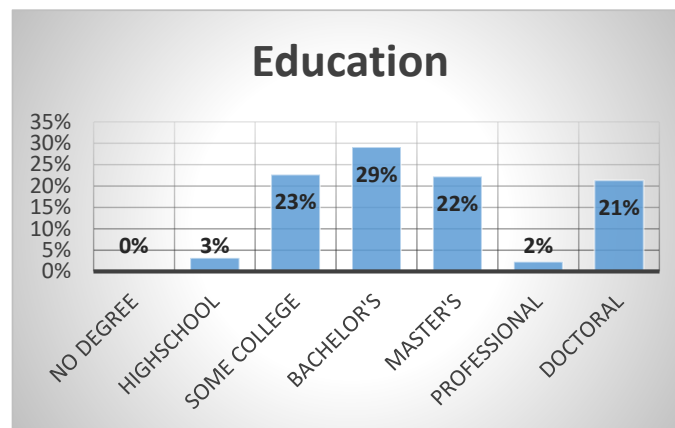
**Table 2:** Statistical Measures of Central Tendency and Dispersion – Demographics

Demographic	Description	N	Min	Max	Mean	StdDev
USE	Use recommended, mandated, or neither	222	1	3	2.78	0.617
CHC	Current chronic health condition	221	1	2	1.77	0.419
GDR	Gender	221	1	2	1.60	0.492
AGE	Age	220	1	6	3.17	1.347
EDU	Education	222	2	7	4.61	1.484



**Figure 3:** Sample Distribution – USE, CHC, GDR, and AGE

Fourth, we observe a mean of 3.17 and a standard deviation of 1.347 for AGE, which chronicled the age range of the participant. We note that 10% of participants were under the age of 24, 25% were between the ages of 25 and 34, another 25% were between the ages of 35 and 44, 19% were between the ages of 45 and 54, 17% were between the ages of 55 and 64, and 3% were ages 65 or older. In light of the fact that wearables are an emergent technology, the observation that 60% of respondents were below the age of 44 is in alignment with current trends. Finally, we observe a mean of 4.61 and a standard deviation of 1.484 for EDU, which noted the education level of the participant. We observe no participants with less than a high school diploma, 3% with a high school diploma, 23% with some college but no degree, 29% with a bachelor's degree, 22% with a master's degree, 2% with a professional degree, and 21% with a doctoral degree.



**Figure 4:** Sample Distribution – EDU

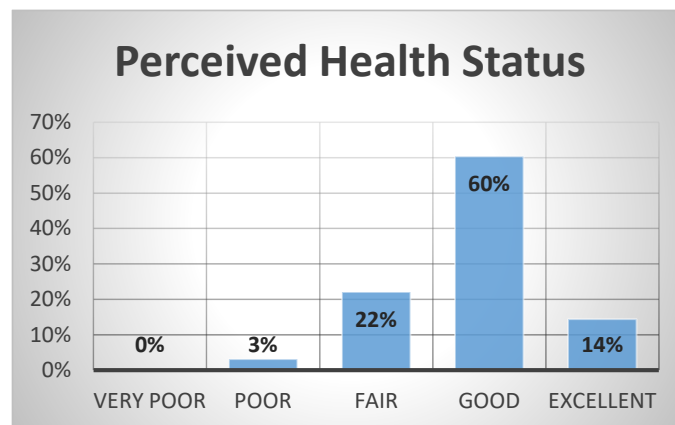
Table 3 represents the statistical measures of central tendency and dispersion for the measurement instrument. With the exception of PHS, all construct measurements consist of multiple indicators based on a Likert seven-point scale with one representing “strongly disagree” and seven representing “strongly agree” (Dittrich et al., 2007). The construct PHS was measured based on a single question, which queried the user regarding whether they perceived their health to be “very poor”, “poor”, “fair”, “good”, or “excellent. The statistical measures observed in Table 3 include the latent variable and corresponding indicators, sample size (which varies due to missing values), minimum and maximum values, mean, standard deviation, and skewness and kurtosis.

**Table 3:** Statistical Measures of Central Tendency and Dispersion – Measurement Instrument

Latent Variable	Indicator	N	Min	Max	Mean	StdDev	Skewness		Kurtosis	
							Statistic	StdErr	Statistic	StdErr
PTV	PTV1	222	1	7	4.14	1.854	-0.169	0.163	-1.143	0.325
	PTV2	222	1	7	3.97	1.780	0.007	0.163	-1.087	0.325
	PTV3	222	1	7	4.85	1.732	-0.737	0.163	-0.398	0.325
	PTV4	222	1	7	4.36	1.821	-0.292	0.163	-1.064	0.325
PTS	PTS1	222	1	7	3.75	1.782	0.183	0.163	-1.037	0.325
	PTS2	222	1	7	4.04	1.843	-0.012	0.163	-1.217	0.325
	PTS3	222	1	7	4.20	1.840	-0.135	0.163	-1.180	0.325
	PTS4	222	1	7	4.40	1.902	-0.335	0.163	-1.185	0.325
REF	REF1	222	1	7	4.13	1.545	-0.407	0.163	-0.580	0.325
	REF2	222	1	7	4.00	1.518	-0.282	0.163	-0.632	0.325
	REF3	222	1	7	4.39	1.508	-0.537	0.163	-0.166	0.325
SEF	SEF1	222	1	7	4.05	1.511	-0.299	0.163	-0.383	0.325
	SEF2	221	1	7	4.12	1.629	-0.377	0.164	-0.820	0.326
	SEF3	222	1	7	4.02	1.625	-0.202	0.163	-0.990	0.325
	SEF4	222	1	7	4.01	1.648	-0.253	0.163	-0.893	0.325
PPR	PPR1	222	1	7	3.55	1.682	0.552	0.163	-0.763	0.325
	PPR2	222	1	7	3.35	1.618	0.425	0.163	-0.564	0.325
	PPR3	222	1	7	4.65	1.811	-0.577	0.163	-0.588	0.325
HMO	HMO1	222	1	7	5.46	1.175	-1.069	0.163	1.770	0.325
	HMO2	222	1	7	5.45	1.209	-1.093	0.163	1.599	0.325
	HMO3	222	1	7	5.16	1.328	-0.820	0.163	0.608	0.325
	HMO4	222	1	7	5.32	1.273	-0.885	0.163	0.692	0.325
PEX	PEX1	221	1	7	5.26	1.312	-0.959	0.164	1.138	0.326
	PEX2	222	1	7	5.60	1.163	-1.115	0.163	1.895	0.325
	PEX3	222	1	7	5.49	1.199	-1.116	0.163	1.621	0.325
EEX	EEX1	222	1	7	5.90	1.059	-1.531	0.163	3.324	0.325
	EEX2	222	1	7	5.82	1.078	-1.276	0.163	2.240	0.325
	EEX3	220	1	7	5.83	1.144	-1.345	0.164	2.109	0.327
	EEX4	222	1	7	5.82	1.106	-1.329	0.163	2.144	0.325
SIN	SIN1	221	1	7	4.24	1.534	-0.379	0.164	-0.327	0.326
	SIN2	221	1	7	4.12	1.491	-0.262	0.164	-0.386	0.326
	SIN3	222	1	7	4.05	1.497	-0.264	0.163	-0.341	0.325
TSE	TSE1	221	1	7	5.71	1.048	-1.408	0.164	3.722	0.326
	TSE2	220	1	7	5.84	0.965	-1.418	0.164	4.651	0.327
	TSE3	222	1	7	5.64	1.156	-1.273	0.163	2.288	0.325
FCG	FCG1	222	1	7	5.67	1.019	-1.082	0.163	1.797	0.325
	FCG2	222	1	7	5.07	1.375	-0.776	0.163	0.389	0.325
	FCG3	222	1	7	4.83	1.438	-0.645	0.163	-0.209	0.325
	FCG4	221	1	7	5.41	1.246	-1.248	0.164	1.758	0.326
PHVU	PHVU1	222	1	7	3.13	1.662	0.579	0.163	-0.651	0.325
	PHVU2	222	1	7	3.11	1.617	0.619	0.163	-0.569	0.325
	PHVU3	222	1	7	3.45	1.711	0.323	0.163	-1.010	0.325
PHSE	PHSE1	222	1	7	3.87	1.655	-0.050	0.163	-0.866	0.325
	PHSE2	222	1	7	3.97	1.683	-0.181	0.163	-0.904	0.325
	PHSE3	221	1	7	4.04	1.738	-0.199	0.164	-1.015	0.326
ITD	ITD1	222	1	7	4.92	1.743	-0.947	0.163	-0.262	0.325
	ITD2	221	1	7	4.71	1.851	-0.732	0.164	-0.705	0.326
	ITD3	222	1	7	5.05	1.789	-1.087	0.163	0.033	0.325
ITA	ITA1	222	1	7	5.64	1.466	-1.442	0.163	1.922	0.325
	ITA2	221	1	7	5.11	1.761	-0.839	0.164	-0.311	0.326
	ITA3	222	1	7	5.55	1.515	-1.389	0.163	1.583	0.325
	ITA4	222	1	7	5.02	1.892	-0.907	0.163	-0.393	0.325
PHS	PHS	222	2	5	3.86	0.688	-0.400	0.163	0.373	0.325

Skewness measures asymmetry and Kurtosis measures the “peakedness” of the distribution of the data (Hae-Young, 2013, p. 2). Although PLS-SEM makes no assumptions regarding distribution (Wong, 2013), and is less sensitive to concerns of normality (Hair et al., 2017), it is important to consider its presence as a part of the analysis process (Hair et al., 2017). A skewness value greater than two and/or a kurtosis value greater than four (when using SPSS) is considered an extreme departure from normality (Hae-Young, 2013). Using this criterion, we observe no concerns regarding skewness and one concern ( $TSE2 = 4.651$ ) regarding kurtosis.

Figure 5 represents the sample distribution for PHS. We observe that none of the sampled participants perceived themselves as being in very poor health, 3% perceived their health as poor, 22% perceived their health as fair, 60% perceived their health as good, and 14% perceived themselves to be in excellent health.

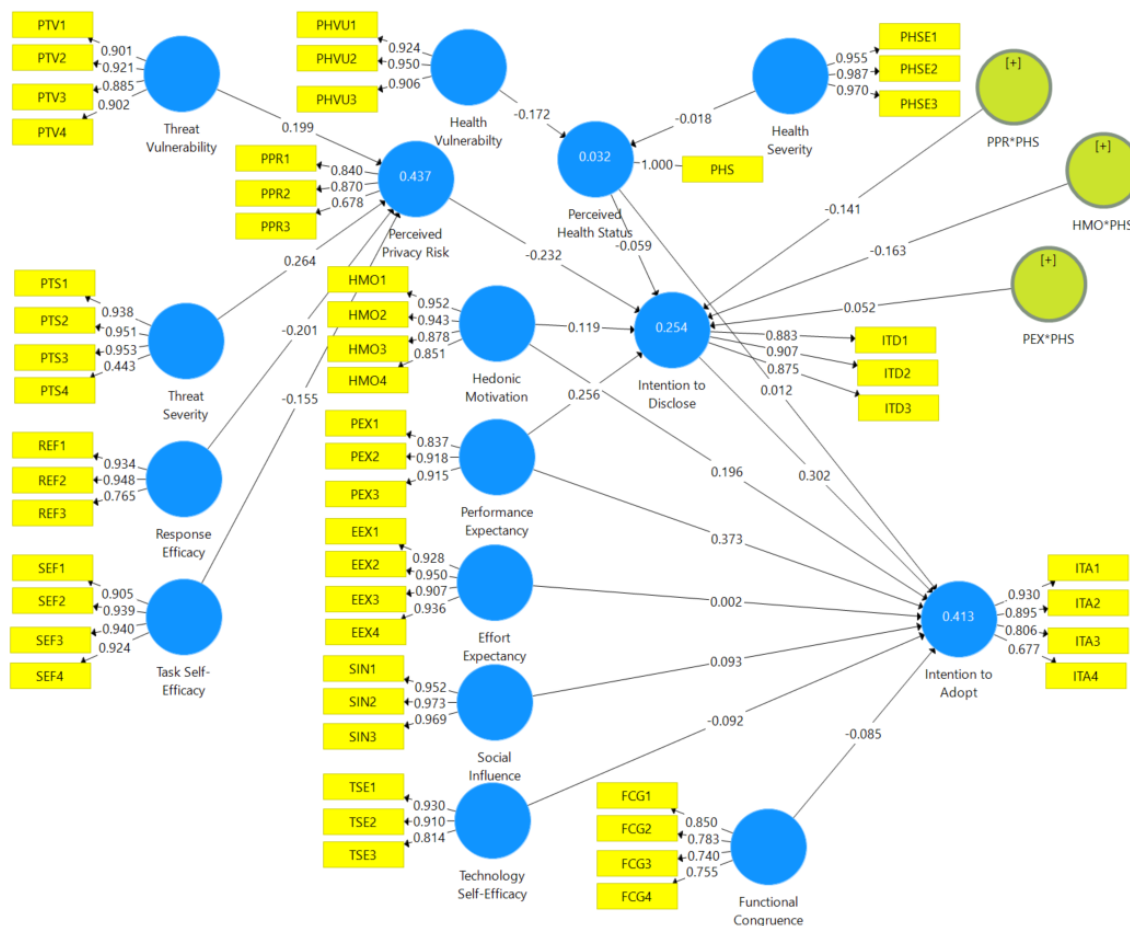


**Figure 5:** Sample Distribution - PHS

## Statistical Analysis

Figure 6 represents the research model post analysis using SmartPLS (Ringle et al., 2015). Displayed are all indicators (yellow) and loadings for each latent variable construct (blue). Arrows pointing to the indicators are indicative of a reflective model (Wong, 2019). Endogenous variables are identified with their corresponding  $R^2$  values, which is a measurement of how much of the variable is explained by the exogenous variables (empty blue circles) that point to them (Hair et al., 2011). The green circles represent the moderating effects of PHS on the relationships  $PPR \rightarrow ITD$ ,  $HMO \rightarrow ITD$ , and  $PEX \rightarrow ITD$ . The indicators and their associated constructs are representative of the measurement model

whereas the exogenous and endogenous variables and their relationships represent the structural model. The next few sections will discuss testing results of both models.



**Figure 6: Analyzed Research Model**

## Measurement Model Testing

Table 4 represents a summary of the quality assessment of the measurement model, which included tests for convergent validity, internal consistency reliability, and discriminant validity using a significance level (alpha) of 0.05 and Bias Correction (BC) for interval analysis. All loadings, with the exception of three indicators, exceeded the recommended value of 0.70, which accounts for a minimum of 50% of the variance regarding the related constructs (Gao et al., 2015). Of the three that fell below, PPR3 and ITA4 measured just under the 0.70 minimum (Hair et al., 2017) at 0.678 and 0.677, respectively, and PTS4 measured significantly under the recommended minimum with a value of 0.443. Table 5 exhibits the significance of the measurement model after bootstrapping.

**Table 4:** Measurement Model Test Summary

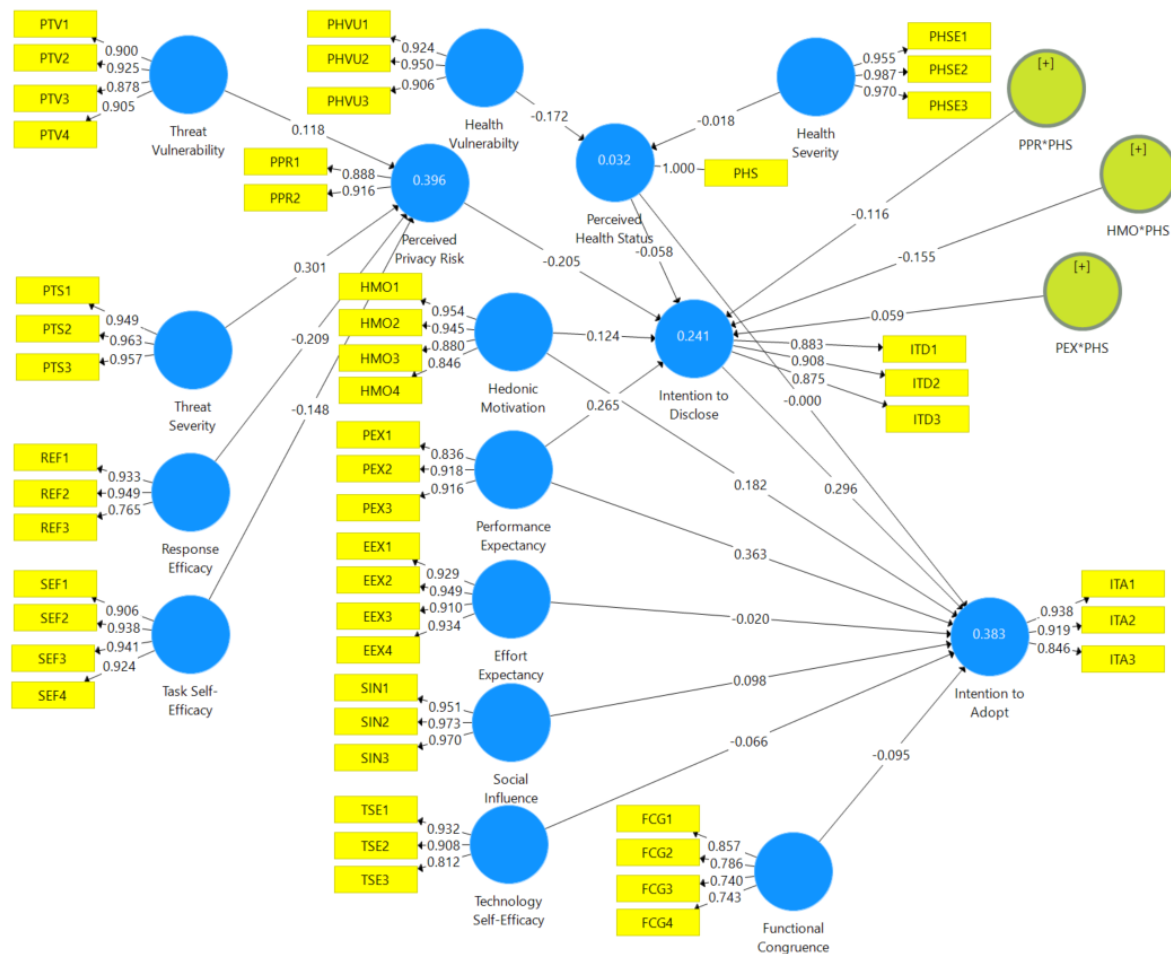
Latent Variable	Indicator	Convergent Validty		AVE	Internal Consistency Reliability		Discriminant Validity	
		Loadings	Indicator Reliability		Cronbach's Alpha	Composite Reliability	HTMT	
		>0.70	>0.50		>0.60	>0.70	<0.85?	HTMT confidence level (BC) does not include 1
PTV	PTV1	0.901	0.812	0.815	0.924	0.946	Yes	Yes
	PTV2	0.921	0.848					
	PTV3	0.885	0.783					
	PTV4	0.902	0.814					
PTS	PTS1	0.938	0.880	0.723	0.851	0.907	Yes	Yes
	PTS2	0.951	0.904					
	PTS3	0.953	0.908					
	PTS4	0.443	0.196					
REF	REF1	0.934	0.872	0.786	0.864	0.916	Yes	Yes
	REF2	0.948	0.899					
	REF3	0.765	0.585					
SEF	SEF1	0.905	0.819	0.860	0.946	0.961	Yes	Yes
	SEF2	0.939	0.882					
	SEF3	0.940	0.884					
	SEF4	0.924	0.854					
PPR	PPR1	0.840	0.706	0.641	0.715	0.841	Yes	Yes
	PPR2	0.870	0.757					
	PPR3	0.678	0.460					
HMO	HMO1	0.952	0.906	0.823	0.927	0.949	Yes	Yes
	HMO2	0.943	0.889					
	HMO3	0.878	0.771					
	HMO4	0.851	0.724					
PEX	PEX1	0.837	0.701	0.793	0.869	0.920	Yes	Yes
	PEX2	0.918	0.843					
	PEX3	0.915	0.837					
EEX	EEX1	0.928	0.861	0.866	0.948	0.963	Yes	Yes
	EEX2	0.950	0.903					
	EEX3	0.907	0.823					
	EEX4	0.936	0.876					
SIN	SIN1	0.952	0.906	0.931	0.963	0.976	Yes	Yes
	SIN2	0.973	0.947					
	SIN3	0.969	0.939					
TSE	TSE1	0.930	0.865	0.785	0.864	0.916	Yes	Yes
	TSE2	0.910	0.828					
	TSE3	0.814	0.663					
FCG	FCG1	0.850	0.723	0.613	0.790	0.863	Yes	Yes
	FCG2	0.783	0.613					
	FCG3	0.740	0.548					
	FCG4	0.755	0.570					
PHVU	PHVU1	0.924	0.854	0.859	0.918	0.948	Yes	Yes
	PHVU2	0.950	0.903					
	PHVU3	0.906	0.821					
PHSE	PHSE1	0.955	0.912	0.942	0.970	0.980	Yes	Yes
	PHSE2	0.987	0.974					
	PHSE3	0.970	0.941					
PHS	PHS1	1.000	1.000	1.000	1.000	1.000	Yes	Yes
ITD	ITD1	0.883	0.780	0.790	0.867	0.919	Yes	Yes
	ITD2	0.907	0.823					
	ITD3	0.875	0.766					
ITA	ITA1	0.930	0.865	0.693	0.847	0.899	Yes	Yes
	ITA2	0.895	0.801					
	ITA3	0.806	0.650					
	ITA4	0.677	0.458					

**Table 5: Measurement Model Significance**

Latent Variable	Indicator	Convergent Validty				Internal Consistency Reliability			
		Loadings		AVE		Cronbach's Alpha		Composite Reliability	
		Confidence Interval (BC)	p-value	Confidence Interval (BC)	p-value	Confidence Interval (BC)	p-value	Confidence Interval (BC)	p-value
PTV	PTV1	[0.851, 0.937]	0.000	[0.772, 0.855]	0.000	[0.902, 0.944]	0.000	[0.931, 0.959]	0.000
	PTV2	[0.895, 0.942]	0.000						
	PTV3	[0.844, 0.917]	0.000						
	PTV4	[0.868, 0.928]	0.000						
PTS	PTS1	[0.913, 0.956]	0.000	[0.687, 0.764]	0.000	[0.809, 0.887]	0.000	[0.886, 0.926]	0.000
	PTS2	[0.930, 0.969]	0.000						
	PTS3	[0.937, 0.965]	0.000						
	PTS4	[0.255, 0.596]	0.000						
REF	REF1	[0.907, 0.953]	0.000	[0.727, 0.834]	0.000	[0.814, 0.900]	0.000	[0.887, 0.938]	0.000
	REF2	[0.926, 0.964]	0.000						
	REF3	[0.652, 0.839]	0.000						
SEF	SEF1	[0.868, 0.930]	0.000	[0.819, 0.893]	0.000	[0.926, 0.960]	0.000	[0.948, 0.971]	0.000
	SEF2	[0.915, 0.956]	0.000						
	SEF3	[0.917, 0.957]	0.000						
	SEF4	[0.869, 0.955]	0.000						
PPR	PPR1	[0.770, 0.886]	0.000	[0.582, 0.693]	0.000	[0.631, 0.775]	0.000	0.803, 0.871]	0.000
	PPR2	[0.820, 0.901]	0.000						
	PPR3	[0.564, 0.764]	0.000						
HMO	HMO1	[0.930, 0.966]	0.000	[0.771, 0.867]	0.000	[0.899, 0.948]	0.000	[0.931, 0.963]	0.000
	HMO2	[0.917, 0.960]	0.000						
	HMO3	[0.822, 0.915]	0.000						
	HMO4	[0.777, 0.904]	0.000						
PEX	PEX1	[0.742, 0.893]	0.000	[0.725, 0.848]	0.000	[0.808, 0.910]	0.000	[0.887, 0.944]	0.000
	PEX2	[0.867, 0.947]	0.000						
	PEX3	[0.878, 0.940]	0.000						
EEX	EEX1	[0.882, 0.956]	0.000	[0.817, 0.905]	0.000	[0.926, 0.965]	0.000	[0.947, 0.975]	0.000
	EEX2	[0.916, 0.969]	0.000						
	EEX3	[0.839, 0.945]	0.000						
	EEX4	[0.894, 0.961]	0.000						
SIN	SIN1	[0.922, 0.971]	0.000	[0.898, 0.953]	0.000	[0.947, 0.976]	0.000	[0.963, 0.984]	0.000
	SIN2	[0.952, 0.984]	0.000						
	SIN3	[0.952, 0.980]	0.000						
TSE	TSE1	[0.885, 0.956]	0.000	[0.699, 0.856]	0.000	[0.788, 0.916]	0.000	[0.873, 0.947]	0.000
	TSE2	[0.850, 0.947]	0.000						
	TSE3	[0.644, 0.908]	0.000						
FCG	FCG1	[0.765, 0.917]	0.000	[0.542, 0.690]	0.000	[0.719, 0.847]	0.000	[0.825, 0.901]	0.000
	FCG2	[0.665, 0.864]	0.000						
	FCG3	[0.572, 0.832]	0.000						
	FCG4	[0.605, 0.850]	0.000						
PHVU	PHVU1	[0.805, 0.964]	0.000	[0.796, 0.908]	0.000	[0.881, 0.945]	0.000	[0.923, 0.968]	0.000
	PHVU2	[0.874, 0.972]	0.000						
	PHVU3	[0.789, 0.964]	0.000						
PHSE	PHSE1	[0.355, 0.986]	0.000	[0.812, 0.966]	0.000	[0.955, 0.980]	0.000	[0.930, 0.989]	0.000
	PHSE2	[0.854, 0.994]	0.000						
	PHSE3	[0.839, 0.998]	0.000						
PHS	PHS	[1.000, 1.000]	0.000	[1.000, 1.000]	0.000	[1.000, 1.000]	NA	[1.000, 1.000]	NA
ITD	ITD1	[0.818, 0.924]	0.000	[0.724, 0.847]	0.000	[0.811, 0.910]	0.000	[0.887, 0.943]	0.000
	ITD2	[0.867, 0.938]	0.000						
	ITD3	[0.809, 0.916]	0.000						
ITA	ITA1	[0.906, 0.948]	0.000	[0.628, 0.751]	0.000	[0.791, 0.887]	0.000	[0.868, 0.923]	0.000
	ITA2	[0.859, 0.921]	0.000						
	ITA3	[0.689, 0.875]	0.000						
	ITA4	[0.549, 0.778]	0.000						

The AVE values for all latent variables were higher than the minimum recommended value of 0.50 (Hair et al., 2017), confirming convergent validity. Internal consistency was measured against accepted values of 0.60 and 0.70 for Cronbach's Alpha and Composite Reliability (CR), respectively. All constructs passed, indicating no problems with internal consistency (Hair et al., 2017). Finally, two criteria of Heterotriat-Monotrait (HTMT) were measured to assess discriminant validity, including an HTMT ratio of correlations score below the cutoff of 0.85 (Hair et al., 2020) and an HTMT interval not containing the value of one, considering a confidence level of 95% (Hair et al., 2017; Wong, 2019). All constructs were found to pass both criteria, confirming discriminant validity. Referring to Table 5, all tests were significant at the 0.05 significance level.

To ensure adherence to the recommended minimum for loadings, the three indicators with loadings less than 0.70 were removed and the research model reanalyzed (Figure 7).



**Figure 7:** Analyzed Research Model (loadings > 0.70)



Table 7 and Table 8 represent the test and significance of the measurement model, respectively. We observe an increase in AVE and internal consistency reliability values, confirming the decision to remove the low performing indicators (Hair et al., 2017). For all constructs, we recognize continued compliance regarding convergent validity, internal consistency reliability, and discriminant validity at the required significance level.

### Structural Model Testing

As noted, PLS-SEM modeling, using SmartPLS (Ringle et al., 2015), was applied to discern cause and affect relationships of the structural model. The model was estimated utilizing the PLS algorithm with complete bootstrapping using the bias-corrected confidence interval method, two-tailed test, 5,000 subsamples, and mean replacement for missing values. Table 6 represents a summary of the model estimation results pertaining specifically to the endogenous latent variables. We observe explained variances of 39.6% (moderate) for PPR, 3.2% (very weak) for PHS, 24.1% (weak) for ITD, and 38.3% (moderate) for ITA (Hair et al., 2011); however, the significance level (p-value) for PHS was notably larger than 0.05, casting doubt on the ability to estimate its explained variance.

**Table 6:** Endogenous Variable Summary

Endogenous Latent Variable	Coefficient of Determination (R2)			R2 Adjusted			Predictive Relevance Q2
	Value	Confidence Interval (BC)	p-value	Value	Confidence Interval (BC)	p-value	
PPR	0.396	[0.285, 0.485]	0.000	0.385	[0.272, 0.476]	0.000	0.306
PHS	0.032	[0.004, 0.084]	0.227	0.023	[-0.005, 0.076]	0.385	0.014
ITD	0.241	[0.116, 0.336]	0.000	0.216	[0.088, 0.315]	0.000	0.170
ITA	0.383	[0.203, 0.511]	0.000	0.36	[0.173, 0.492]	0.000	0.287

Blindfolding, utilizing an Omission Distance (OD) of 7, was the technique used to calculate Stone-Geisser's  $Q^2$ , which determines the predictive relevance of the model (Wong, 2019). We observe weak predictive relevance for PHS, better than moderate relevance for PPR and ITA, and moderate relevance for ITD.

**Table 7:** Measurement Model Test Summary (loadings > 0.70)

Latent Variable	Indicator	Convergent Validity		Internal Consistency Reliability		Discriminant Validity		
		Loadings	Indicator Reliability	AVE	Cronbach's Alpha	Composite Reliability	HTMT	
		>0.70	>0.50	>0.50	>0.60	>0.70	<0.85?	HTMT confidence level (BC) does not include 1
PTV	PTV1	0.900	0.810	0.814	0.924	0.946	Yes	Yes
	PTV2	0.925	0.856					
	PTV3	0.878	0.771					
	PTV4	0.905	0.819					
PTS	PTS1	0.949	0.901	0.914	0.953	0.970	Yes	Yes
	PTS2	0.963	0.927					
	PTS3	0.957	0.916					
REF	REF1	0.933	0.870	0.786	0.864	0.916	Yes	Yes
	REF2	0.949	0.901					
	REF3	0.765	0.585					
SEF	SEF1	0.906	0.821	0.860	0.946	0.961	Yes	Yes
	SEF2	0.938	0.880					
	SEF3	0.941	0.885					
	SEF4	0.924	0.854					
PPR	PPR1	0.888	0.789	0.814	0.773	0.897	Yes	Yes
	PPR2	0.916	0.839					
HMO	HMO1	0.954	0.910	0.823	0.927	0.949	Yes	Yes
	HMO2	0.945	0.893					
	HMO3	0.880	0.774					
	HMO4	0.846	0.716					
PEX	PEX1	0.836	0.699	0.793	0.869	0.920	Yes	Yes
	PEX2	0.918	0.843					
	PEX3	0.916	0.839					
EEX	EEX1	0.929	0.863	0.866	0.948	0.963	Yes	Yes
	EEX2	0.949	0.901					
	EEX3	0.910	0.828					
	EEX4	0.934	0.872					
SIN	SIN1	0.951	0.904	0.931	0.963	0.976	Yes	Yes
	SIN2	0.973	0.947					
	SIN3	0.970	0.941					
TSE	TSE1	0.932	0.869	0.785	0.864	0.916	Yes	Yes
	TSE2	0.908	0.824					
	TSE3	0.812	0.659					
FCG	FCG1	0.857	0.734	0.613	0.790	0.863	Yes	Yes
	FCG2	0.786	0.618					
	FCG3	0.740	0.548					
	FCG4	0.743	0.552					
PHVU	PHVU1	0.924	0.854	0.859	0.918	0.948	Yes	Yes
	PHVU2	0.950	0.903					
	PHVU3	0.906	0.821					
PHSE	PHSE1	0.955	0.912	0.942	0.970	0.980	Yes	Yes
	PHSE2	0.987	0.974					
	PHSE3	0.970	0.941					
PHS	PHS1	1.000	1.000	1.000	1.000	1.000	Yes	Yes
ITD	ITD1	0.883	0.780	0.790	0.867	0.919	Yes	Yes
	ITD2	0.908	0.824					
	ITD3	0.875	0.766					
ITA	ITA1	0.938	0.880	0.814	0.885	0.929	Yes	Yes
	ITA2	0.919	0.845					
	ITA3	0.846	0.716					



Sorted by hypotheses, Table 9 provides a summary of the inspection of exogenous variables effects on corresponding endogenous variables. This includes the moderating effects of PHS. Considering VIF values of less than 5.0, we observe that multicollinearity is not a concern for all hypothesized relationships (Hair et al., 2013). Based on path coefficients and significance, we discover support for hypotheses H2, H3, H5, H8, H9, and H20 at an alpha of 0.01 (\*\*\*), H7, H14, and H17 at an alpha of 0.05 (\*\*), and H4 at an alpha of 0.10 (\*). H6, H11 and H16 were just over the 0.10 significance level with values of 0.105, 0.114, and 0.116, respectively. H1 was somewhat beyond acceptable significance levels.

**Table 9:** Structural Model Test Summary

Hypothesis	Relationship	VIF <5.0	Path Coefficient	Confidence Interval (BC)	p-value	Effect Size (f <sup>2</sup> )
H1+	PTV -> PPR	1.817	0.118	[-0.030, 0.274]	<b>0.135</b>	0.013
H2+	PTS -> PPR	1.375	0.301	[0.187, 0.410]	0.000 ***	0.109
H3-	REF -> PPR	2.380	-0.209	[-0.362, -0.049]	0.009 ***	0.030
H4-	SEF -> PPR	2.347	-0.148	[-0.312, 0.017]	0.079 *	0.016
H5-	PPR -> ITD	1.112	-0.205	[-0.340, -0.061]	0.004 ***	0.050
H6+	HMO -> ITD	1.503	0.124	[-0.023, 0.280]	<b>0.105</b>	0.014
H7+	HMO -> ITA	1.688	0.182	[0.028, 0.349]	0.026 **	0.032
H8+	PEX -> ITD	1.585	0.265	[0.094, 0.417]	0.001 ***	0.058
H9+	PEX -> ITA	2.356	0.363	[0.156, 0.560]	0.001 ***	0.091
H10+	EEX -> ITA	1.831	-0.020	[-0.170, 0.117]	<b>0.780</b>	0.000
H11+	SIN -> ITA	1.272	0.098	[-0.024, 0.219]	<b>0.114</b>	0.012
H12+	TSE -> ITA	2.038	-0.066	[-0.257, 0.113]	<b>0.490</b>	0.003
H13+	FCG -> ITA	1.690	-0.095	[-0.253, 0.023]	<b>0.171</b>	0.009
H14-	PHVU -> PHS	1.137	-0.172	[-0.313, -0.038]	0.018 **	0.027
H15-	PHSE -> PHS	1.137	-0.018	[-0.134, 0.167]	<b>0.811</b>	0.000
H16+	PPR*PHS -> ITD	1.305	-0.116	[-0.246, 0.037]	<b>0.116</b>	0.014
H17-	HMO*PHS -> ITD	2.069	-0.155	[-0.314, -0.010]	0.048 **	0.021
H18-	PEX*PHS -> ITD	2.054	0.059	[-0.094, 0.208]	<b>0.438</b>	0.003
H19-	PHS -> ITA	1.063	0.000	[-0.108, 0.111]	<b>0.993</b>	0.000
H20+	ITD -> ITA	1.259	0.296	[0.137, 0.458]	0.000 ***	0.113

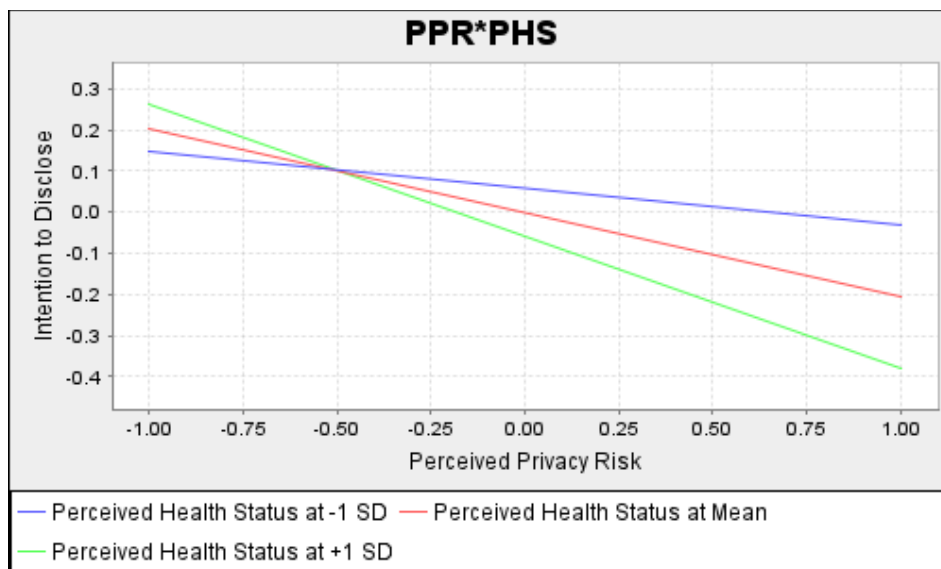
Hypotheses H10, H12, H13, H15, H18, and H19 were well beyond acceptable significance levels, indicating failure to infer any effect in the relationships between latent constructs. Effect size (f<sup>2</sup>) denotes the impact of exogenous variables on endogenous variables with 0.02, 0.15, and 0.35 being criteria for a small, medium or large impact, respectively

(Hair et al., 2013). Of the significant relationships identified, H2, H9, and H20 had a somewhat medium impact, while the others had a somewhat small impact.

### Moderator Analysis

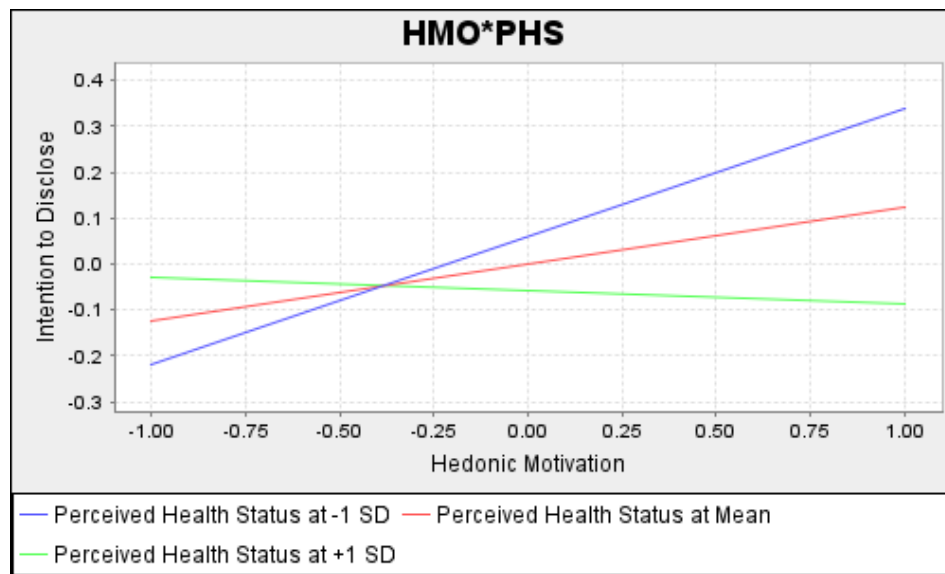
Referring to Table 9 above, H16, H17, and H18 hypothesized a moderating effect of PHS on the relationships between the exogenous variables, PPR, HMO, and PEX, and the endogenous variable ITD. Regarding moderator analysis, the path coefficient is reflective of the interaction term. The graphs shown in figures 8, 9, and 10 exhibit the slope analysis of the moderating effect of PHS on these relationships when using the two-stage approach for creating the interaction terms. The x-axis represents the exogenous variable and the y-axis represents the ITD endogenous variable. The red line represents the effect of PHS at mean, the blue line at -1 standard deviation (SD), and the green line at +1 SD.

Regarding PPR (Figure 8), which normally has a negative influence on ITD, we observe a significant decrease in the negative influence of PPR on ITD with lower levels of PHS (blue line) and a significant increase in the negative influence of PPR on ITD with higher levels of PHS (green line). This is reflected regarding the interaction term of -0.116 and directly correlates with hypothesis H16. Specific to moderator analysis, effect sizes ( $f^2$ ) of 0.005, 0.01, and 0.25 are the criteria for a small, medium or large effect, respectively (Hair et al., 2017; Kenny, 2018). Accordingly, we observe a somewhat large effect (0.014) of PHS on the PPR→ITD relationship.



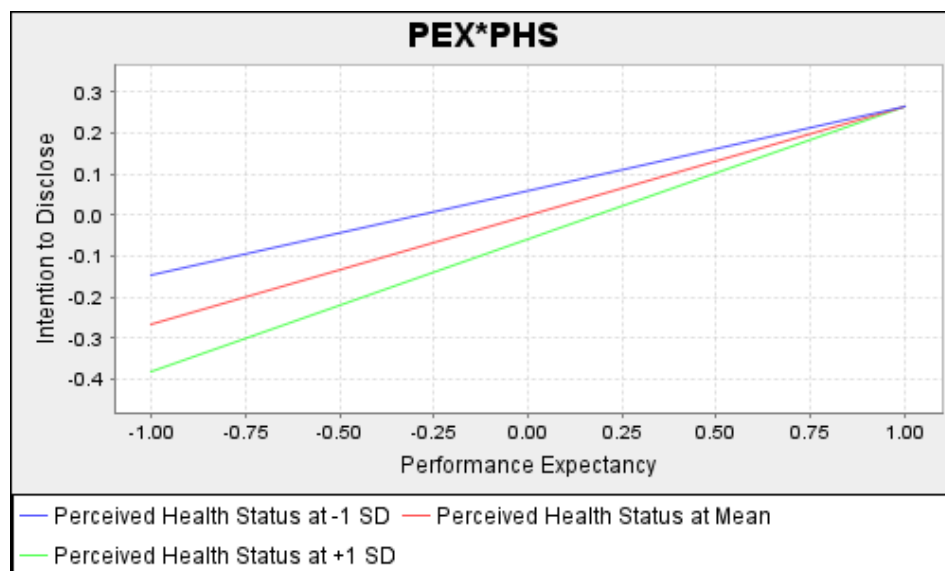
**Figure 8:** Moderating Effect of PHS on PPR→ITD

Regarding HMO (Figure 9), which normally has a positive influence on ITD, we observe a significant increase in the positive influence of HMO on ITD with lower levels of PHS (blue line) and a decrease in the positive influence with higher levels of PHS (green line). This is reflected in the interaction term of -0.155 and directly correlates with H17. We observe a somewhat large effect (0.021) of PHS on the HMO→ITD relationship.



**Figure 9:** Moderating Effect of PHS on HMO→ITD

Regarding PEX (Figure 10), which normally has a positive influence on ITD, we observe an increase in the positive influence of PEX on ITD with lower levels of PHS (blue line) and a decrease in the positive influence with higher levels of PHS (green line). This is reflected in the interaction term of 0.059 and is in alignment with H18. We observe a very small effect (0.003) of PHS on the PEX→ITD relationship; however, as referenced earlier, H18 was determined to be well outside acceptable significance levels, indicating failure to infer any effect.



**Figure 10:** Moderating Effect of PHS on PEX→ITD

## CHAPTER 6

### DISCUSSION

The objective of the research model was to emphasize the multi-dimensional role of privacy regarding the acceptance of healthcare wearables. This has been accomplished via the assimilation of well-established theories in the realm of technology acceptance and privacy. The results of this study afford significant evidence that privacy is truly a critical concern for potential users, and, joined with benefits to disclosure, are moderated by the perceived health status of the individual. Specific to the research questions guiding this endeavor, we observe significant evidence regarding the impact of the privacy calculus on intentions to disclose information on the healthcare wearables adoption decision process (RQ1). In addition, we observe participation of the privacy paradox in the context of healthcare wearable decisions (RQ2). The following narrative provides an explanation of the findings.

The influence of PTV on PPR is somewhat inconclusive with a p-value of 0.135; however, PTS has the greatest significant positive effect, REF has a significant negative effect, and SEF has a somewhat negative effect on PPR. The inconclusiveness of PTV on PPR may be ascribed to a lack of knowledge by participants regarding threats to privacy specific to wearables, an emerging health technology (Sun et al., 2013). Even so, the net validation of H2 through H4 supports the existence of the risk calculus where the balance of threats, joined with the ability to cope, determine concerns of privacy (Zhang et al., 2018). The construct PPR has a significant negative effect on ITD, concluding that threats to one's privacy, and the ability to respond, influences one's concern with privacy and their willingness to disclose personal information.

The construct HMO is reservedly confirmed to have a somewhat significant positive effect on ITD. The same construct is found to have a significant positive effect on ITA. Construct PEX is discovered to have the greatest significant positive effect on both ITD and ITA. Accordingly, we understand that the pleasure of using a wearable device, and the expectation that the device will deliver the benefit expected, encourages disclosure of one's private information as well as wearable acceptance. Referring to RQ1, the confirmation of H5, H6, and H8 provides evidence of the privacy calculus, the conceptualization of the



privacy trade-off process where privacy risks, the balance of threats and coping appraisals, are weighed with the benefits associated with disclosure (Kehr et al., 2015). This aligns with other health/privacy-oriented research (Zhang et al., 2018). Additionally, the net confirmation of H2 through H8 supports the conceptualization of the dual-calculus model, which jointly contemplates the risk calculus and the privacy calculus in the disclosure decision process (Li, 2012).

Of the four constructs, EEX, SIN, TSE, and FCG, only SIN has a somewhat significant positive influence on ITA. Consequently, H10, H12, and H13 are not supported and H11 is somewhat supported. We conclude that the effort required, one's confidence in their ability to use the device, and the perceived suitability to satisfy expectations have no significant effect on adopting a wearable device; however, the effect of others, somewhat influences wearable adoption, but only at minimal levels. This corresponds to past wearable research, such as (Patton, 2018), which also found inconclusive evidence of similar constructs to ITA. One potential explanation could be due to the fairly even distribution of ages between 24 and 64 years of age (see Table 1 above), which could also account for decreased levels of normality discovered for the noted constructs. Age has been shown to significantly effect factors related to technology acceptance (Morris & Venkatesh, 2000; Venkatesh et al., 2012), potentially skewing results when corporately analyzed.

Another potential explanation for the low performance of EEX, TSE, and FCG concerns the type of wearable device, whether it be for fitness or medical purposes. 96% of the participants of this study were in fair to excellent health, 88% were neither recommended nor mandated to use a device, and 77% had no chronic condition, suggesting a fairly healthy pool of respondents. We infer from these demographics that the larger population of participants were considering the use of fitness-oriented devices. Prior research (Gao et al., 2015) discovered that fitness wearable device users were more concerned with privacy and what others thought versus device effectiveness, the amount of effort required, and their ability to operate the device. Age has also been found to be a mitigating factor (Gao et al., 2015), possibly because an older population generally has more health concerns and might be more likely to seek a healthcare-oriented wearable device to address a specific medical issue. Consequently, we recognize that the type of device considered and/or age of the participant

might also provide explanation of the low performance of EEX, TSE, and FCG as well as confirm somewhat significant findings for SIN.

Construct PHVU is discovered to have a significant negative influence on PHS, confirming H14; however, the same influence is not confirmed for PHSE, rejecting H15. We conclude vulnerability to health issues does negatively affect one's perception of health status. Hypotheses H16, H17, and H18 focus on the moderating influence of one's perceived health status on their intention to disclose. We observe that higher levels of PHS have a somewhat significant positive effect on the influence of PPR on ITD at a significance level just above 0.10, meaning that increases in the perception of one's health increases the effect of their perception of privacy risk on disclosing private information, confirming H16. In regards to healthcare wearables, people are more concerned with the cost or risk of disclosure of their personal and private information with increased levels of perceived health status. We witness that higher levels of PHS also have a significant negative impact on the influence of HMO on ITD, confirming H17. People place less emphasis on the benefit of pleasure with increased levels of perceived health status. Finally, we observe no significant impact of PHS on PEX, rejecting H18. We conclude, that with higher perceptions of health status, a user's concern for privacy has a higher negative influence on intentions to disclose, while the expected enjoyment they expect to receive from using a healthcare wearable device is less of a positive influence on the decision to disclose their personal information. Referring to RQ2, we discover the acuity of one's health status does moderate the disclosure decision process, confirming the presence of the privacy paradox.

We observe no significant influence of PHS on ITA, discounting H19. However, we do note a significant positive effect of ITD on ITA, supporting H20. We accept that one's intentions to disclose private information does affect whether or not they intend to adopt a wearable device. This aligns with findings associated with Gao et al.'s (2015) research, where the single construct of privacy was found to significantly contribute to explaining wearable acceptance. In the current study, the construct of privacy was expanded in order to capture the intricate behavioral progressions surrounding its presence, conceptualized by the risk calculus, the privacy calculus, and the privacy paradox. Not only did the results align with the aforementioned study, we observe a greater influence with ITD explaining 29.6% of the

variance of ITA in the current study, as opposed to the singular construct of perceived privacy accounting for 21.5% in the former.

## CHAPTER 7

### CONCLUSIONS

The wearable device acceptance process is wrought with a plethora of various influences and thought processes, partially attributed to the sensitivity of the information captured. This is especially apropos in the realm of healthcare. While past research has focused on specific aspects of privacy and acceptance (Gao et al., 2015; Harmon, 2019; Scott, 2020), there remained a gap as to a comprehensive analysis of privacy in the realm of healthcare-related wearables. Utilizing established research in the area of technology acceptance, PMT, HBM, and privacy calculus theories, this study sought to fill this gap by conceptualizing these influences and thought processes into a research model that could be measured and assessed based on a representative sample of the populace. The objective was particularly focused on the role of privacy in the form of the privacy calculus (RQ1) and the privacy paradox (RQ2) in the realm of wearable acceptance. Using survey research and PLS-SEM analysis, this study successfully confirmed the presence of both theories in the context of wearable acceptance.

This effort significantly expands what is currently known regarding the healthcare wearables' privacy/acceptance paradigm and thus notably contributes to our understanding regarding the influences effecting the healthcare wearables' acceptance process. Contributions include understanding and generalization in the healthcare wearables knowledge space as well as practical implications for wearable manufacturers and consumers. Specifically, this research endeavor furthers knowledge regarding the intersection of privacy and healthcare wearables acceptance and use. While many previous efforts such as (Gao et al., 2015; Li et al., 2016; Zhang et al., 2018) focused on specific research domains of the wearables paradigm and/or health privacy, the current research capitalized on the success of those prior initiatives and expanded on their findings. This research combined antecedents to privacy disclosure with antecedents to technology acceptance. In addition, the construct of perceived health status was introduced in order to capture how one feels about their health and how that perception contributed to their acceptance of the technology. Consequently, this study facilitated a more complete understanding of the decision processes inherent in the use of an

emerging technology, such as wearables, that is proving to add significance and practical value to those who utilize it.

Wearable devices are no longer just a fad procured simply for the sake of curiosity, as demonstrated by 2022 projected sales of 189.9 million (Ubrani et al., 2018). This statistic suggests that consumers are indeed discovering sincere value in their use, especially in the realm of health-related wearables, which offer increased management and success over one's health and wellbeing; however, their use is not without risk, especially in the realm of privacy. It is imperative that researchers and healthcare organizations understand the role the risk calculus, the privacy calculus, and the privacy paradox play regarding the decision of consumers to disclose or not to disclose personal information. This is particularly important in the realm of healthcare wearable devices due to the potential negative impact on the health and wellbeing of the individual, should they choose to avoid the technology, and the risk to privacy should they choose to accept it. The current research sought to conceptualize and address this imperative.

For researchers, understanding the role of the privacy calculus theories facilitates sound conclusions and guides future research endeavors. This is especially apropos regarding the privacy paradox, which is still surrounded by a shroud of obscurity and complexity (Gerber et al., 2018; Kokolakis, 2017). For healthcare organizations, understanding informs the process of capturing, managing, and communicating personal information, including health-related data. Understanding will also highlight the importance of transparency and ethics regarding what information is captured and who will have access to it. This study further enlightens the privacy and healthcare wearable space, enhancing the value proposition of this recent and promising area of technology.

As previously noted in the discussion, the privacy paradox was observed regarding the moderating effect of perceived health status on perceived privacy risk and hedonic motivation. In light of this significant observation and contribution in the realm of privacy and healthcare wearables, this study could be enhanced with continued research regarding the privacy paradox and health status, with a recommended focus on various types of wearable devices as well as different health concerns. Regarding health status, none of the respondents reported very poor health. Consequently, our study is incomplete when considering the full

spectrum of one's health. The same insufficiency exists for education, where respondents with no degree were absent from the sample.

There are multiple opportunities for future research resulting from the current study. First, it would be advantageous to resample the population followed by similar analysis with the intention to address this study's shortcomings regarding health status, device type, and education. Health status and device type would be particularly helpful to shed light on those hypotheses with insignificant results. Second, we observe opportunity related to categorical moderation analysis (PLS-MGA) (Wong, 2019) based on participant demographics such as usage, chronic health condition, age, and education. This would offer opportunity to compare the moderating effect of each category. Finally, an opportunity arises regarding the variety of wearable devices currently on the market. Theoretical understanding would benefit by applying an adjusted research model (based on the findings of this study) and narrowing the target to specific categories of wearables.

## REFERENCES

- Amft, O. (2018). How wearable computing is shaping digital health. *IEEE Pervasive Computing*, 17(1), 92-98. <https://doi.org/10.1109/MPRV.2018.011591067>
- Anaya, S. L. H., Alsadoon, A., Costadopoulos, N., & Prasad, P. W. C. (2018). Ethical implications of user perceptions of wearable devices. *Science Engineering Ethics*, 24, 1-28. <https://doi.org/10.1007/s11948-017-9872-8>
- Arthur, L. (2013, August 15). What is Big Data. *Forbes*. <https://www.forbes.com>
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038-1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Bélangier, F., & Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017. <https://doi.org/10.2307/41409971>
- Bergenstock, J. (2017). *Internet of Things: Ease of life vs. demolition of personal privacy* [Master's thesis, Utica College]. ProQuest Dissertations Publishing, 10686190. <https://search.proquest.com/openview/3a553ae219295ca3c0d858475dc7c741/>
- Bhattacharjee, A. (2012). *Social science research: Principles, methods, and practices* (Vol. 3). University of South Florida.
- Bott, G. (2017). *A privacy calculus model for personal mobile devices* [Doctoral dissertation, Mississippi State University]. ProQuest Dissertations Publishing, 10272836. <https://search.proquest.com/openview/b5d2f9a75ff3aa9e62e20b8498505f18/>
- Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. (2019). Refining the threat calculus of technology threat avoidance theory. *Communications of the Association for Information Systems*, 45(5), 95-115. <https://doi.org/10.17705/1CAIS.04505>
- Brown, S. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. *MIS Quarterly*, 29(3), 399-426. <https://doi.org/10.2307/25148690>

- Catteddu, D., Hogben, G., Haeberlen, T., & Dupre, L. (2012). *Cloud computing: benefits, risks and recommendations for information security* (Vol. Rev.B). European Network and Information Security Agency. <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications>
- Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60-67. <https://doi.org/10.1145/293411.293475>
- Costello, K. (2018, November 29). Gartner says worldwide wearable device sales to grow 26 percent in 2019 *Newsroom*. <https://www.gartner.com/en/newsroom/press-releases>
- Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two. *Management Science*, 35(8), 982. <https://doi.org/10.1287/mnsc.35.8.982>
- Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [Unpublished doctoral dissertation]. Massachusetts Institute of Technology.
- De Mooy, M., & Yuen, S. (2017). Toward privacy aware research and development in wearable health. *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii, USA, 3658-3667. <http://hdl.handle.net/10125/41600>.
- Deng, Z., & Liu, S. (2017). Understanding consumer health information-seeking behavior from the perspective of the risk perception attitude framework and social support in mobile social media websites. *International Journal of Medical Informatics*, 105, 98-109. <https://doi.org/10.1016/j.ijmedinf.2017.05.014>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. *Information Systems Research*, 17(1), 61-80,100. <https://doi.org/10.1287/isre.1060.0080>
- Dittrich, R., Francis, B., Hatzinger, R., & Katzenbeisser, W. (2007). A paired comparison approach for the analysis of sets of Likert-scale responses. *Statistical Modelling*, 7(1), 3-28. <https://doi.org/10.1177/1471082X0600700102>
- Doyle, M. (2019). *Comprehending the safety paradox and privacy concerns with medical device remote patient monitoring* [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations Publishing, 27544007. <https://search.proquest.com/openview/59d8ad68c6e1ced128c24ae52d6d8bea/>



- Drost, E. (2011). Validity and reliability in social science research. *Education Research and Perspectives*, 38(1), 105-124.
- Ferraro, V., & Ugur, S. (2011). Designing wearable technologies through a user centered approach. *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces*, Milano, IT, 1-8. New York, NY: ACM.  
<https://doi.org/10.1145/2347504.2347510>.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley.
- GAO. (2017). Internet of Things: Status and implications of an increasingly connected world.  
<https://www.gao.gov/assets/690/684590.pdf>
- Gao, Y., He, L., & 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>
- Ge, C., Yin, C., Liu, Z., Fang, L., Zhu, J., & Ling, H. (2020). A privacy preserve big data analysis system for wearable wireless sensor network. *Computers & Security*, 96.  
<https://doi.org/10.1016/j.cose.2020.101887>
- Gefen, D., Straub, D., & Boudreau, M. (2000). Structural Equation Modeling and Regression: Guidelines fo Research Practice. *Communications of the Association for Information Systems*, 4(7), 1-77. <https://doi.org/10.17705/1CAIS.00407>
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226-261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Glenn, T., & Monteith, S. (2014). Privacy in the digital world: Medical and health data outside of HIPAA protections. *Curr Psychiatry Rep*, 16(494), 1-11.  
<https://doi.org/10.1007/s11920-014-0494-4>
- Hae-Young, K. (2013). Statistical notes for clinical researchers: Assessing normal distribution (2) using skewness and kurtosis. *Restorative dentistry & endodontics*, 38(1), 52-54.  
<https://doi.org/10.5395/rde.2013.38.1.52>
- Hahanov, V., & Miz, V. (2015). Big data driven healthcare services and wearables. *The Experience of Designing and Application of CAD Systems in Microelectronics*, Lviv, Ukraine, 310-312. <https://doi.org/10.1109/CADSM.2015.7230864>.

- Hair, J. F., Hult, G. T. M., Gingle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM), 2nd edition*. Sage Publications.
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of marketing theory and practice*, 19(2), 139-152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hair, J. F., Sarstedt, M., & Ringle, C. M. (2019). Rethinking some of the rethinking of partial least squares. *European Journal of Marketing*, 53(4), 556-584. <https://doi.org/10.1108/EJM-10-2018-0665>
- Hair, J. F. J., Ringle, C. M., & Sarstedt, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance [Editorial]. *Long Range Planning*, 46(1-2), 1-12. <http://dx.doi.org/10.1016/j.lrp.2013.01.001>
- Hair, J. J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis [Article]. *Journal of Business Research*, 109, 101-110. <https://doi.org/10.1016/j.jbusres.2019.11.069>
- Harmon, A. (2019). *A quantitative predictive study of U.S. Fitbit owners' intentions to use activity trackers* [Doctoral dissertation, Capella University]. ProQuest Dissertations Publishing, 13899674. <https://search.proquest.com/openview/0c7e68a944eb2a507b0935a71a992269/>
- Harper, A. (2016). *The impact of consumer security awareness on adopting the Internet of things: A correlational study* [Doctoral dissertation, Capella University]. ProQuest Dissertations Publishing, 10196140. <https://search.proquest.com/openview/473cbff993e6291f217d64af59234949/>
- Herath, T., & Rao, H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125. <https://doi.org/10.1057/ejis.2009.6>
- Hsu, J. (2018, January 29). The Strava heat map and the end of secrets. *Security*. <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/>
- Huber, F., Vollhardt, K., Matthes, I., & Vogel, J. (2010). Brand misconduct: Consequences on consumer–brand relationships [Article]. *Journal of Business Research*, 63(11), 1113-1120. <https://doi.org/10.1016/j.jbusres.2009.10.006>

- Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. *Health Education, 11*(1), 1-47.
- Jayden, K. (2018). Tapping into the wearable device revolution in the work environment: A systematic review. *Information Technology & People, 31*(3), 791-818.  
<https://doi.org/10.1108/ITP-03-2017-0076>
- Jernejcic, T., & Kettani, H. (2019). On the Intersection of Big Data and Privacy. *Proceedings of the International Conference on Big Data and Internet of Things (BDIoT'19)*, Rabat, Morocco, 1-4. New York, NY: ACM.  
<https://doi.org/10.1145/3372938.3372939>.
- Jung A Kim, P., Sook Ja Yang, P., Yeon Kyung Chee, P., Kyoung Ja Kwon, P., & Jisook An, P. (2015). Effects of health status and health behaviors on depression among married female immigrants in South Korea. *Asian nursing research, 9*(2), 125-131.  
<https://doi.org/10.1016/j.anr.2015.01.003>
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635. <https://doi.org/10.1111/isj.12062>
- Kenny, D. A. (2018, September 15). Moderation. <http://davidakenny.net/cm/moderation.htm>
- Kianto, A., Shujahat, M., Hussain, S., Nawaz, F., & Ali, M. (2019). The impact of knowledge management on knowledge worker productivity. *Baltic Journal of Management, 14*(2), 178-197.
- Kim, J. A., Yang, S. J., Chee, Y. K., Kwon, K. J., & An, J. (2015). Effects of health status and health behaviors on depression among married female immigrants in South Korea. *Asian nursing research, 9*(2), 125-131. <https://doi.org/10.1016/j.anr.2015.01.003>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.
- Kritzler, M., Tenfält, A., Bäckman, M., & Michahelles, F. (2015). Wearable technology as a solution for workplace safety. *The 14th International Conference on Mobile and Ubiquitous Multimedia*, Linz, Austria, 213-217.  
<https://doi.org/10.1145/2836041.2836062>.

- Lehto, M., & Lehto, M. (2017). *Health information privacy of activity trackers*. Academic Conferences International Limited.  
<http://www.ezproxy.dsu.edu:2048/login?url=https://search.proquest.com/docview/1966794697?accountid=27073>
- Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, 88, 8-17.  
<https://doi.org/10.1016/j.ijmedinf.2015.12.010>
- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-482.  
<https://doi.org/10.1016/j.dss.2012.06.010>
- Lidynia, C., Brauner, P., & Ziefle, M. (2017). A step in the right direction – Understanding privacy concerns and perceived sensitivity of fitness trackers. *Advances in Intelligent Systems and Computing*, 608, 42-53. [https://doi.org/10.1007/978-3-319-60639-2\\_5](https://doi.org/10.1007/978-3-319-60639-2_5)
- Machi, L., & McEvoy, B. (2016). *The literature review six steps to success*. Corwin.
- 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>
- Merriam-Webster. (2017). Merriam-Webster. In *Merriam-Webster Dictionary*.  
<https://www.merriam-webster.com/dictionary>
- Meyer, J., Fortmann, J., Wasmann, M., & Heuten, W. (2015). Making lifelogging usable: Design guidelines for activity trackers. In X. He, S. Luo, D. Tao, C. Xu, J. Yang, & M. A. Hasan, *MultiMedia Modeling 2015 International Conference on MultiMedia Modeling*, Sydney, NSW, Australia, 323–334. [https://doi.org/10.1007/978-3-319-14442-9\\_39](https://doi.org/10.1007/978-3-319-14442-9_39).
- Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. *Personnel Psychology*, 53(2), 375-403.  
<https://doi.org/10.1111/j.1744-6570.2000.tb00206.x>
- Muaremi, A., Arnrich, B., & Tröster, G. (2013). Towards measuring stress with smartphones and wearable devices during workday and sleep. *Bio Nano Science*, 3(2), 172-183.  
<https://doi.org/10.1007/s12668-013-0089-2>

- Nadeem, A., Hussain, M. A., Owais, O., Salam, A., Iqbal, S., & Ahsan, K. (2015). Application specific study, analysis and classification of body area wireless sensor network applications. *Computer Networks*, 83, 363-380.  
<https://doi.org/10.1016/j.comnet.2015.03.002>
- NIST. (2013). *NIST/SEMATECH e-Handbook of statistical methods*. NIST.  
<https://doi.org/10.18434/M32189>
- Norberg, P., Horne, D., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, 41(1), 100-126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Padyab, A., & Ståhlbröst, A. (2018). Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. *Digital Policy, Regulation and Governance*, 20(6), 528-544. <https://doi.org/10.1108/DPRG-05-2018-0023>
- Page, T. (2015). Privacy issues surrounding wearable technology. *I-Manager's Journal on Information Technology*, 4(4), 1-16.
- Patton, W. (2018). *Application of UTAUT2 to the adoption of smartwatch technology by american consumers* [Doctoral dissertation, Capella University]. ProQuest Dissertations Publishing, 10936639.  
<https://search.proquest.com/docview/2126644916?pq-origsite=primo>
- Peppet, S. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, 93(1), 85-176.
- Perez, A. J., & Zeadally, S. (2018). Privacy issues and solutions for consumer wearables. *IT Professional*, 20(4), 46-56. <https://doi.org/10.1109/MITP.2017.265105905>
- Petursdottir, A. I., & Carr, J. E. (2018). Applying the taxonomy of validity threats from mainstream research design to single-case experiments in applied behavior analysis. *Behavior Analysis in Practice*, 11(3), 228-240. <https://doi.org/10.1007/s40617-018-00294-6>
- Polonetsky, J., & Gray, S. (2017). The Internet of Things as a tool for inclusion and equality. *Federal Communications Law Journal*, 69(2), 103-118.

- Preusse, K. C., Mitzner, T. L., Fausset, C. B., & Rogers, W. A. (2017). Older adults' acceptance of activity trackers. *Journal of applied gerontology : the official journal of the Southern Gerontological Society*, 36(2), 127-155.  
<https://doi.org/10.1177/0733464815624151>
- Pulipaka, S. (2019). *Impact of privacy concerns and user perceptions on the usage intention of wearable smart medical devices: A correlational study* [Doctoral dissertation, Capella University]. ProQuest Dissertations Publishing, 22619514.  
<https://search.proquest.com/openview/91d05ea8c36ad9be1ca074cf44f3c55f/>
- Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013, September 5). Anonymity, Privacy, and Security Online. *Pew Internet & American Life Project*. <https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/>
- Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3*. In Boenningstedt: SmartPLS GmbH. <http://www.smartpls.com>
- Roberts, T. (2012). Understanding survey research: Applications and processes. *British Journal of Midwifery*, 20(2), 114-120.  
<http://libproxy.calbaptist.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=ccm&AN=104553190&site=eds-live&scope=site>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.  
<https://doi.org/10.1080/00223980.1975.9915803>
- Sarstedt, M., Hair, J. F., Ringle, C. M., Thiele, K. O., & Gudergan, S. P. (2016). Estimation issues with PLS and CBSEM: Where the bias lies! *Journal of Business Research*, 69(10), 3998-4010. <https://doi.org/10.1016/j.jbusres.2016.06.007>
- Scott, D. (2020). *A correlation study of smartwatch adoption and privacy concerns with U.S. consumers using the UTAUT2* [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations Publishing, 27837468.  
<https://search.proquest.com/openview/bf2acb7ddb06f4e9867652fce3125ee2/>

- Shen, N. (2019). *The eHealth trust model: Understanding the patient privacy perspective in a digital health environment* [Doctoral dissertation, University of Toronto]. ProQuest Dissertations Publishing, 10196140.  
<https://search.proquest.com/openview/6e20c27ab6cecf467479b031cd5bce05/>
- Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989. <https://doi.org/10.2307/41409970>
- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM Conference on Electronic Commerce*, Florida, USA, 38-47. New York, NY: ACM.  
<https://doi.org/10.1145/501158.501163>.
- Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13, 380-427.
- Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and integration of alternative models. *Journal of Electronic Commerce Research*, 14(2), 183-200.
- Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting american consumers and opening them up to exploitation*.  
[https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy\\_1.pdf](https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf)
- Ubrani, J., Llamas, R., & Shirer, M. (2018, December 17). IDC forecasts sustained double-digit growth for wearable devices led by steady adoption of smartwatches. *Business Wire*. <https://www.businesswire.com/news/home/20181217005099/en/IDC-Forecasts-Sustained-Double-Digit-Growth-Wearable-Devices>
- Uzialko, A. C. (2018, June 17). How businesses are collecting data (and what they're doing with it). *Business News Daily*. <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.  
<https://doi.org/10.1287/mnsc.46.2.186.11926>

- 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. [http://www.vvenkatesh.com/wp-content/uploads/2015/11/2003\(3\)\\_MISQ\\_Venkatesh\\_etal.pdf](http://www.vvenkatesh.com/wp-content/uploads/2015/11/2003(3)_MISQ_Venkatesh_etal.pdf)
- Venkatesh, V., Thong, J., & 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. <https://doi.org/10.2307/41410412>
- Vitak, J., Liao, Y., Kumar, A., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. *iConference 2018*, Sheffield, UK, 229-239. [https://doi.org/10.1007/978-3-319-78105-1\\_27](https://doi.org/10.1007/978-3-319-78105-1_27).
- Wei, Z., & Piramuthu, S. (2014). Security/privacy of wearable fitness tracking IoT devices. *2014 9th Iberian Conference on Information Systems and Technologies*, Barcelona, Spain, 1-5. <https://doi.org/10.1109/CISTI.2014.6877073>.
- Wenling, W., Rajneesh, S., & Shan, F. (2015). The role of product personalization in effects of self-congruity versus functional congruity. *Journal of Travel Research*, 38, 340-352. [https://doi.org/10.1007/978-3-319-24184-5\\_74](https://doi.org/10.1007/978-3-319-24184-5_74)
- Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-Things. *2016 11th International Conference on Availability, Reliability and Security*, Salzburg, Austria, 644-652. <https://doi.org/10.1109/ARES.2016.25>.
- Wilson, D. W., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. *Thirty Third International Conference on Information Systems*, Orlando, Florida, 1-11. <https://aisel.aisnet.org/icis2012/proceedings/ResearchInProgress/101/>.
- Wong, K. K.-K. (2019). *Mastering partial least squares structural equation modeling (PLS-SEM) with SmartPLS in 38 hours*. iUniverse.
- Wong, K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24, 1-32. [http://marketing-bulletin.massey.ac.nz/v24/mb\\_v24\\_t1\\_wong.pdf](http://marketing-bulletin.massey.ac.nz/v24/mb_v24_t1_wong.pdf)



- Woon, I., Tan, G., & Low, R. (2005). A protection motivation theory approach to home wireless security. *26th International Conference on Information Systems 2005 Proceedings*, Las Vegas, Nevada, 367-380. <http://aisel.aisnet.org/icis2005/31>.
- Yang, K., Ahn, C. R., Vuran, M. C., & Aria, S. S. (2016). Semi-supervised near-miss fall detection for ironworkers with a wearable inertial measurement unit. *Automation in Construction*, 68, 194-202. <https://doi.org/10.1016/j.autcon.2016.04.007>
- Yuchen, Y., Longfei, W., Guisheng, Y., Lijie, L., & Hongbin, Z. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250-1258. <https://doi.org/10.1109/JIOT.2017.2694844>
- Zenonos, A., Khan, A., Kalogridis, G., Vatsikas, S., Lewis, T., & Sooriyabandara, M. (2016, 14-18 March 2016). HealthyOffice: Mood recognition at work using smartphones and wearable sensors. *The Second IEEE International Workshop on Sensing Systems and Applications Using Wrist Worn Smart Devices, 2016*, Sydney, NSW, Australia, 1-6. <https://doi.org/10.1109/PERCOMW.2016.7457166>.
- 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(4), 482-493. <https://doi.org/10.1016/j.im.2017.11.003>
- Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, 6(2), 1606-1616. <https://doi.org/10.1109/JIOT.2018.2847733>

## APPENDICES

### APPENDIX A: RESEARH MODEL CONSTRUCTS MEASUREMENTS

#### Seven-point Likert scale

*Perceived Threat Vulnerability (PTV)* – Sourced from Zhang et al. (2018)

- PTV1: My information privacy is at risk of being invaded.
- PTV2: It is likely that my information privacy will be invaded.
- PTV3: It is possible that my information privacy will be invaded.
- PTV4: My information privacy is not safe from being invaded.

*Perceived Threat Severity (PTS)* – Sourced from Zhang et al. (2018)

- PTS1: If my information privacy is invaded, it would be severe.
- PTS2: If my information privacy is invaded, it would be serious.
- PTS3: If my information privacy is invaded, it would be significant.
- PTS4: If my information privacy is invaded, it would not be irrelevant.

*Response Efficacy (REF)* – Adapted from Zhang et al. (2018)

- REF1: The privacy protection measures provided by healthcare wearable manufacturers are suitable for protecting my personal information.
- REF2: The privacy protection measures provided by healthcare wearable manufacturers can effectively protect my personal information.
- REF3: My personal information is more likely to be protected when using privacy protection measures provided by healthcare wearable manufacturers.

*Task Self-Efficacy (SEF)* – Sourced from Zhang et al. (2018)

- SEF1: Protecting my information privacy is easy for me when using healthcare wearable devices.
- SEF2: I have the capability to protect my information privacy when using healthcare wearable devices.
- SEF3: I am able to protect my information privacy without much effort when using healthcare wearable devices.
- SEF4: Protecting my information privacy is not difficult when using healthcare wearable devices.

*Perceived Privacy Risk (PPR)* – Adapted from Zhang et al. (2018)

- PPR1: I believe that submitting health and other privacy information for the purpose of using wearable devices is not advisable at all.
- PPR2: Health and other privacy information submitted for the purpose of using wearable devices will be abused for sure once submitted.
- PPR3: Health and other privacy information submitted for the purpose of using wearable devices could be shared or sold to others once submitted.

*Hedonic Motivation (HMO)* – Adapted from Gao et al. (2015)

- HMO1: Healthcare wearable devices are fun to use.
- HMO2: Healthcare wearable devices are enjoyable to use.
- HMO3: Healthcare wearable devices are entertaining to use.
- HMO4: Healthcare wearable devices are not boring to use.

*Performance Expectancy (PEX)* – Adapted from Gao et al. (2015)

- PEX1: Healthcare wearable devices add value to my personal life.
- PEX2: Using healthcare wearable devices helps me to achieve my healthcare goals more quickly.
- PEX3: Using healthcare wearable devices enhances the quality of my daily healthcare requirements.

*Effort Expectancy (EEX)* – Adapted from Gao et al. (2015)

- EEX1: It is easy for me to learn how to use healthcare wearable devices.
- EEX2: Healthcare wearable devices are easy to use.
- EEX3: Becoming skillful at using healthcare wearable devices is easy for me.
- EEX4: Healthcare wearable device are not difficult to use.

*Social Influence (SIN)* – Adapted from Gao et al. (2015)

- SIN1: Others who are important to me would feel that I should use a healthcare wearable device.
- SIN2: Others who influence me would feel that I should use a healthcare wearable device.
- SIN3: Others whose opinions I value would prefer that I should use a healthcare wearable device.

*Technology Self-Efficacy (TSE)* – Adapted from Gao et al. (2015)

- TSE1: Using wearable devices make it easy for me to self-monitor my health-related conditions.
- TSE2: I am capable to use healthcare wearable devices to self-monitor my health-related conditions.
- TSE3: It takes little effort to use healthcare wearable devices to self-monitor my health-related conditions.

*Functional Congruence (FCG)* – Adapted from Gao et al. (2015)

- FCG1: Healthcare wearable devices are anticipated to be comfortable to use.
- FCG2: Healthcare wearable devices are anticipated to be fashionable.
- FCG3: Healthcare wearable devices are anticipated to be priced appropriately according to device quality.
- FCG4: Healthcare wearable devices are not anticipated to be unpleasant to use.

*Perceived Health Vulnerability (PHVU)* – Source/adapted from Gao et al. (2015)

- PHVU1: I am at risk of suffering one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.
- PHVU2: It is likely that I will suffer one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.
- PHVU3: It is possible for me to suffer one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

*Perceived Health Severity (PHSE)* – Adapted from Gao et al. (2015)

- PHSE1: It would be severe if I suffered one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.
- PHSE2: It would be serious if I suffered one or more of the following concerns: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.
- PHSE3: It would be significant if I suffered one or more of the following problems: having little knowledge about self-healthcare, monitoring personal daily healthcare, and/or suffering health-related diseases.

*Intention to Disclose (ITD)* – Adapted from Zhang et al. (2018)

- ITD1: I am likely to provide general personal information in the use of healthcare wearable devices (e.g., such as name, email, profile image, etc.).
- ITD2: I am likely to provide specific personal information in the use of healthcare wearable devices (e.g., such as DOB, gender, ethnicity, race, etc.).
- ITD3: I am likely to provide personal fitness and health information in the use of healthcare wearable devices (e.g., such as fitness activity, exercise routines, medications, health history, vital signs, etc.).

*Intention to Adopt Healthcare Wearable Devices (ITA)* – Adapted from Gao et al. (2015)

- ITA1: I anticipate using a healthcare wearable device in the future.
- ITA2: I have plans to use a healthcare wearable device whenever possible.
- ITA3: I foresee increasing use of healthcare wearable devices in the future.
- ITA4: I do not anticipate avoiding the use of healthcare wearable devices in the future.

## **Interval Scale Measurements**

*Perceived Health Status (PHS)* – From Kim et al. (2015)

- 1 = Very poor  
 2 = Poor  
 3 = Fair  
 4 = Good  
 5 = Excellent

**Demographic**

*Use recommended, mandated, or neither (USE)*

- 1: Recommended
- 2: Mandated
- 3: Neither

*Current chronic health condition (CHC)*

- 1: Yes
- 2: No

*Gender (GDR)*

- 1: Male
- 2: Female

*Age (AGE)* – From Malhotra et al. (2004).

- 1: 24 or under
- 2: 25-34
- 3: 35-44
- 4: 45-54
- 5: 55-64
- 6: 65 or older

*Highest level of education completed (EDU)* – From Malhotra et al. (2004)

- 1: Some school, no degree
- 2: Highschool graduate
- 3: Some college, no degree
- 4: Bachelor's degree
- 5: Master's degree
- 6: Professional degree
- 7: Doctoral degree

## APPENDIX B: SMARTPLS PARAMETERS

### PLS Algorithm

#### Partial Least Squares Algorithm

The PLS path modeling method was developed by Wold (1982). In essence, the PLS algorithm is a sequence of regressions in terms of weight vectors. The weight vectors obtained at convergence satisfy fixed point equations (see Dijkstra, 2010, for a general analysis of these equations).

[Read more!](#)

Setup

Missing Values

Weighting

Basic Settings

Weighting Scheme

☐ Centroid
☐ Factor
☒ Path

Maximum Iterations:

300

Stop Criterion ( $10^{-X}$ ):

5

Advanced Settings

Configure [individual initial weights](#)

Basic Settings

Weighting Scheme

PLS-SEM allows the user to apply three structural model weighting schemes:

(1) centroid weighting scheme,

(2) factor weighting scheme, and

(3) path weighting scheme (default).

While the results differ little for the alternative weighting schemes, path weighting is the recommended approach. This weighting scheme provides the highest  $R^2$  value for endogenous latent variables and is generally applicable for all kinds of PLS path model specifications and estimations. Moreover, when the path model includes higher-order constructs (often called second-order models), researchers should usually not use the centroid weighting scheme.

Maximum Iterations

This parameter represents the maximum number of iterations that will be used for calculating the PLS results. This number should be sufficiently large (e.g., 300 iterations). When checking the PLS-SEM result, one must make sure that the algorithm did not stop because the maximum number of iterations was reached but due to the stop criterion. Note: The selection of 0 for the maximum number of iterations allows you to obtain results of the sum scores approach.

Stop Criterion

The PLS algorithm stops when the change in the outer weights between two consecutive iterations is smaller than this stop criterion value (or the maximum number of iterations is reached). This value should be sufficiently small (e.g.,  $10^{-5}$  or  $10^{-7}$ ).

After Calculation:

Open Full Report

Close

Start Calculation

### Bootstrapping

#### Bootstrapping

Bootstrapping is a nonparametric procedure that allows testing the statistical significance of various PLS-SEM results such path coefficients, Cronbach's alpha, HTMT, and  $R^2$  values.

[Read more!](#)

Setup

Partial Least Squares

Missing Values

Weighting

Basic Settings

Subsamples

5000

Do Parallel Processing

☒

Amount of Results

☐ Basic Bootstrapping
☒ Complete Bootstrapping

Advanced Settings

Confidence Interval Method

☐ Percentile Bootstrap
☐ Studentized Bootstrap
☒ Bias-Corrected and Accelerated (BCa) Bootstrap

Test Type

☐ One Tailed
☒ Two Tailed

Significance Level

0.05

Basic Settings

Subsamples

In bootstrapping, subsamples are created with observations randomly drawn (with replacement) from the original set of data. To ensure stability of results, the number of subsamples should be large. For an initial assessment, one may use a smaller number of bootstrap subsamples (e.g., 500). For the final results preparation, however, one should use a large number of bootstrap subsamples (e.g., 5,000).  
Note: Larger numbers of bootstrap subsamples increase the computation time.

Do Parallel Processing

This option runs the bootstrapping routine on multiple processors (if your computer device offers more than one core). Using parallel computing will reduce computation time.

Amount of Results

(1) Basic Bootstrapping (default)

Only a basic set of results for bootstrapping is assembled. This includes: *Path Coefficients, Indirect Effects, Total Effects, Outer Loadings, and Outer Weights*. This option is much faster if a large number of resamples is drawn and useful for preliminary data analysis.

(2) Complete Bootstrapping

All available results for bootstrapping are assembled. For example, this includes: *Path Coefficients, Indirect Effects, Total Effects, Outer Loadings, Outer Weights, R Square, Average Variance Extracted (AVE), Composite Reliability, Cronbach's Alpha, and Heterotrait-Monotrait Ratio (HTMT)*. It uses a Bollen-Stine type bootstrapping for the goodness-of-fit measures. Note: This option needs more time to compute the results. Also, this option needs more computer memory (how to assign more memory to SmartPLS, see the [FAQ on www.smartpls.com](#))

After Calculation:

Open Full Report

Close

Start Calculation

## Blindfolding

### Blindfolding

Blindfolding is a sample re-use technique. It allows calculating Stone-Geisser's  $Q^2$  value (Stone, 1974; Geisser, 1974), which represents an evaluation criterion for the cross-validated predictive relevance of the PLS path model.

[Read more!](#)

Setup

Partial Least Squares

Missing Values

Weighting

Basic Settings

Omission Distance

7

Basic Settings

Omission Distance

Default: 7

The systematic pattern of data point elimination and prediction in the blindfolding procedure depends on the omission distance (D). The user must select a value for D when running the blindfolding procedure. Suggested values of D are between 5 and 12.

An omission distance of seven (D=7), for example, implies that every seventh data point of the target construct's indicators are eliminated in a single blindfolding round. Since the blindfolding procedure has to omit and predict every data point of the indicators used in the measurement model of a certain latent variable, it comprises seven blindfolding rounds. Hence, the number of blindfolding rounds always equals the omission distance D.

It is important to note that the omission distance has to be chosen so that the number of observations in the data set divided by the omission distance D is not an integer. If the number of observations divided by D results in an integer, the procedure would delete full observations (i.e., entire rows of the data set). Hence, the number of observations used per blindfolding round would be smaller than the number of observations in the original data set. However, the goal of the blindfolding procedure is to use all observations for prediction and, thus, not to delete entire observations per blindfolding round. For this reason, the number of observations used in the original data set divided by the omission distance D must not be integer.

[Link to Literature](#)

After Calculation:

Open Full Report

Close

Start Calculation

### Blindfolding

Blindfolding is a sample re-use technique. It allows calculating Stone-Geisser's  $Q^2$  value (Stone, 1974; Geisser, 1974), which represents an evaluation criterion for the cross-validated predictive relevance of the PLS path model.

[Read more!](#)

Setup

Partial Least Squares

Missing Values

Weighting

Basic Settings

Weighting Scheme

☐ Centroid
☐ Factor
☒ Path

Maximum Iterations:

300

Stop Criterion ( $10^{-X}$ ):

5

Advanced Settings

Configure [individual initial weights](#)

Basic Settings

Weighting Scheme

PLS-SEM allows the user to apply three structural model weighting schemes:

(1) centroid weighting scheme,  
(2) factor weighting scheme, and  
(3) path weighting scheme (default).

While the results differ little for the alternative weighting schemes, path weighting is the recommended approach. This weighting scheme provides the highest  $R^2$  value for endogenous latent variables and is generally applicable for all kinds of PLS path model specifications and estimations. Moreover, when the path model includes higher-order constructs (often called second-order models), researchers should usually not use the centroid weighting scheme.

Maximum Iterations

This parameter represents the maximum number of iterations that will be used for calculating the PLS results. This number should be sufficiently large (e.g., 300 iterations). When checking the PLS-SEM result, one must make sure that the algorithm did not stop because the maximum number of iterations was reached but due to the stop criterion. Note: The selection of 0 for the maximum number of iterations allows you to obtain results of the sum scores approach.

Stop Criterion

The PLS algorithm stops when the change in the outer weights between two consecutive iterations is smaller than this stop criterion value (or the maximum number of iterations is reached). This value should be sufficiently small (e.g.,  $10^{-5}$  or  $10^{-7}$ ).

After Calculation:

Open Full Report

Close

Start Calculation