The Digitization of Healthcare in Developing Countries: Examining Individuals' Willingness to Disclose Personal Health Information

A thesis submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in Information Systems

By

Ernest Kwadwo Adu

University of Canterbury

2019

DEDICATION

This thesis is dedicated to
the Blessed Virgin Mary, the Patroness of my studies,
and my late father Mike Okrah

ACKNOWLEDGEMENTS

I wish to express my profound gratitude to my supervisors, Associate Professor Annette Mills and Senior Lecturer Nelly Todorova, whose guidance, insights and constructive criticisms have been invaluable in successfully completing this thesis. Their motivation, patience and kindness have also been very helpful, especially during the days when the PhD journey was difficult to travel. I cannot forget the sacrifices they made in the latter stages of my studies to ensure this thesis was completed and submitted on time. Prof. Annette Mills, in particular, spent her entire time while on leave to work on the final chapters of the thesis, to which I am very grateful. I thank God for blessing me with such wonderful people as my supervisors.

I would also like to thank the University of Canterbury for awarding me the UC Doctoral Scholarship without which it would have been impossible for me to pursue my PhD studies. I must also acknowledge the constant support and assistance provided by the administrative, academic, and technical staff of the Accounting and Information Systems department. You helped create a supportive, friendly, and conducive environment for learning and research, and for that, I am exceedingly grateful. Thank you also to the friends and colleagues with whom I shared this journey. Your friendship, encouragement, and support helped make pleasant my PhD journey.

I am also greatly indebted to Dr Musah Adams of the Department of Information Studies, University of Ghana. Dr Adams taught me during my undergraduate studies and upon graduating, I worked as his teaching assistant. He has played a vital role throughout my academic journey by providing me with academic recommendations and offering needed advice and encouragement.

Of course, I cannot thank enough my family and friends back home in Ghana for their constant prayers, love and support. They have been a strong pillar of support throughout my life and especially during this period of intensive learning.

Finally, and most importantly, I am eternally grateful to God for his blessings and grace which have brought me this far in my academic career. To HIM be all GLORY, HONOUR, and PRAISE.

TABLE OF CONTENTS

CHAPTER FIVE: DATA ANALYSIS

CHAPTER SIX: DISCUSSION

CHAPTER SEVEN: CONTRIBUTIONS AND IMPLICATIONS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

In recent years, the increasing use of health information technologies (HITs) in support of healthcare services in developing countries has raised concerns about the privacy of digitized personal health information (PHI). However, there is little understanding of these concerns and their impact on individuals' PHI disclosure behaviours. This study seeks to improve current understanding of the factors that influence the willingness of individuals in developing countries to disclose their PHI to receive care where the disclosed PHI is digitized. To pursue this objective, this study proposes and tests a model of antecedents to PHI privacy concerns, trust in HIT, and PHI disclosure. Drawing on the procedural and interactional dimensions of justice theory and prior research it is proposed that individuals' characteristics, experiences, and perceptions form PHI privacy concerns and trust in HIT. Drawing on the privacy calculus, key factors that drive and inhibit individuals' PHI disclosure are also examined.

This study was conducted using a quantitative research design. The proposed model was tested using data collected from a survey of 276 individuals in Ghana, a Sub-Saharan African country. The data was analysed using the partial least squares approach to structural equation modelling (PLS-SEM).

The findings of the study show trust in HIT directly influence PHI disclosure and fully mediates the influence of trust in healthcare providers. Convenience and computer experience also drive PHI disclosure. Trust in HIT is further shaped by privacy risk, government regulation, computer experience, and health concern. Perceived attitude of health workers affects trust in HIT through trust in healthcare providers.

Regarding inhibitors of PHI disclosure, individuals' perceptions of the negative consequences that may result from the exposure of their disclosed PHI decrease their willingness to disclose PHI. The results further show that individuals' concerns about the collection of their PHI differ from concerns about the management of the collected and electronically stored PHI. For example, individuals' express lower PHI collection concerns but greater concerns about PHI management. The results showed that PHI collection concerns decrease PHI disclosure whereas PHI management concerns increase PHI disclosure. PHI management concerns are shaped by computer experience, privacy orientation and trust in healthcare, with trust in healthcare providers mediating the influence of government regulation and perceived attitude of health workers on PHI management concerns. On the other hand, privacy risk, age, gender, and health concern form PHI collection concerns. The results also show past experience of privacy violation has different effects on PHI collection and PHI management concerns, increasing collection concerns but decreasing the management concerns.

Overall, the findings of the study provide insights into the drivers and inhibitors of PHI disclosure, the dimensions of PHI privacy concerns and their antecedents, as well as the antecedents to trust in HIT. These findings provide useful contributions to the IS privacy literature and actionable insights for healthcare stakeholders especially in developing countries, as they leverage HITs in the provision of healthcare services.

CHAPTER ONE: INTRODUCTION

1.1 Research Background

The majority of the population in the developing countries[1] of Africa and Asia live in rural areas (United Nations [UN], 2014). The rural population, especially in Africa, often lack good access to basic healthcare services (Ministry of Health [MOH], 2010; Shiferaw & Zolfo, 2012). This stems from the lack of skilled health personnel and medical infrastructure and the fact that the distribution of the limited staff and infrastructure is skewed towards urban areas (MOH, 2010; Policy Engagement Network [PEN], 2010). Consequently, in addition to the problem of accessing care, quality of care can be poor, and the cost of healthcare expensive and unaffordable to most of the people (Mugo & Nzuki, 2014).

Besides resource challenges, developing countries also continue to be plagued by the world's deadliest epidemics such as HIV/AIDS and tuberculosis which represent the leading causes of death in these countries (Ohuabunwa, Sun, Jubanyik, & Wallis, 2016; Willyard, 2010). An efficient record-keeping system is required to ensure continuous treatment and long-term care for patients with these infectious diseases (Ohuabunwa et al., 2016; Walsham, Robey, & Sahay, 2007). However, the healthcare systems in these countries are largely paper-based (or manual) and hence, cannot meet the challenges of efficient patient data management. This is because these manual healthcare systems often fail to ensure consistent availability of important clinical information, and do not facilitate its timely delivery for effective medical decision making, causing redundancy in services and medical errors (Agarwal, Gao, DesRoches, & Jha, 2010).

The need to ensure the efficient collection and management of personal health information (PHI) and the necessity to extend geographic access to healthcare have led to increased use of information technology (IT) in the health sector of these countries (Lewis, Synowiec, Lagomarsino, & Schweitzer, 2012). For instance, telemedicine is being used to offer remote medical services in several African countries (Kifle, Mbarika, & Datta, 2006; Maiga, Makori, & Miph, 2013; Mugo & Nzuki, 2014). There is also a widespread implementation of electronic health records (EHR) in most developing countries (Ohuabunwa et al., 2016).

The digitization of health information can deliver numerous social and individual benefits including reducing medical errors, improving patient safety, improving public health monitoring, and facilitating clinical research (Anderson & Agarwal, 2011; Glaser, Henley, Downing, Brinner, & Community, 2008). Beyond increasing access to care, the efforts to digitize healthcare in developing countries have yielded other benefits. As an example, the management of patient information using an EHR system supported health workers in distributing antiretroviral drugs to HIV-infected refugees during the 2007 ethnic violence in

[1] Using the Gross National Income (GNI) per capita , the World Bank classifies countries into four income groups: low income, lower middle income, upper middle income, and high income countries (World Bank, 2016a). According to this classification, developing countries comprise low- and middle-income countries. These are countries, in which majority of the population makes far less income and often lack basic public services, when compared with populations in high-income countries.

Kenya (Willyard, 2010). EHR systems have also helped to reduce data duplication, ensure ready access of routine reports, and improve data accuracy in the management and use of patient data (Acquah-Swanzy, 2015; Gyamfi, 2016; Mugo & Nzuki, 2014).

With the benefits of digitizing healthcare however, there is increased risk of privacy loss due to the vulnerability of digitized PHI to criminal attacks as well as the ease and speed with which health information can be shared among the many participants of the healthcare system (Anderson & Agarwal, 2011; Fichman, Kohli, & Krishnan, 2011; Jena, 2015). Consequently, in developed countries where electronic healthcare (e-health) has matured, concerns about PHI privacy have heightened and represent the major barrier to the widespread diffusion of e-health (Angst & Agarwal, 2009; Chhanabhai & Holt, 2007; Kenny & Connolly, 2016).

In developing countries, especially in Africa, concerns about PHI privacy have long existed in the traditional healthcare environment. Certain diseases and sexual orientations are heavily stigmatized in these countries and as such the exposure of this sensitive information can have severe consequences for individuals including death (Gettleman, 2011; PEN, 2010). Consequently, some individuals hide their infection with stigmatized diseases (e.g., HIV/AIDS) and even avoid needed healthcare (Dapaah & Sena, 2006; Kwansa, 2013). It is thus not surprising that even though e-health is nascent in developing countries (Lewis et al., 2012), some studies indicate concerns about PHI privacy among individuals with the introduction of computer systems in support of healthcare (Bedeley & Palvia, 2014; Willyard, 2010). In the specific case of Ghana, the proliferation of cybercrimes is cited as a major reason for individuals concerns about the privacy of digitized PHI (Bedely & Palvia, 2014).

Healthcare, as an information-intensive industry, relies on the availability of individuals' PHI (Laric, Pitta, & Katsanis, 2009). Securing individuals' cooperation and willingness to allow their PHI to be stored in a digital form is thus crucial to the successful digitization of healthcare (Angst & Agarwal, 2009; Bansal, Fatemeh, & Gefen, 2010). However, without assurance of the privacy of their electronically stored health information, individuals may withhold important health information from healthcare providers (Agaku, Adisa, Ayo-Yusuf, & Connolly, 2013; Campos-Castillo & Anthony, 2014). Given the concerns about PHI privacy as developing countries migrate to e-health systems (Bedeley & Palvia, 2014; Willyard, 2010), it has become imperative to identify and understand the factors that can both support and hinder consumers' decision to disclose their PHI and allow its digitization. Toward this end, this thesis addresses the following question: *What factors influence consumer willingness to disclose PHI in order to receive care from healthcare providers in developing countries where the disclosed PHI is digitized?* PHI includes any information that a patient submits to receive care and the information that is generated in the treatment process (e.g., x-ray photo, prescription, lab test results, etc.) (Yoo, Yim, & Rao, 2013).

1.2 Digitized Healthcare and the Research Context

The stakes in healthcare are a matter of life and death. It is thus important that healthcare quality is always diligently pursued to ensure patient safety. As an information-intensive industry, effective and quality healthcare depends on the availability of accurate and up-to-date clinical information, and the processing and timely communication of this information for better coordination of care at both the individual and societal levels (Fichman et al., 2011). This requires effective and extensive use of IT across the healthcare system (Agarwal et al., 2010). The broad application of IT in support of health and health-related fields has been referred to as e-health (World Health Organization [WHO], 2016). The term *digitized healthcare* has been used in recent years in reference to the specific application of IT in the collection, management, and sharing of patients' health information as well as deriving insights from this information to enable the practice and delivery of care to be tailored to a patient's specific needs (Anderson & Agarwal, 2011). In this thesis, the terms *e-health* and *digitized healthcare* are distinguished; whereas *e-health* will be used when the broad application of IT in the health sector is considered (WHO, 2016), the term *digitized healthcare* will be used in referring to the application of IT for the collection, management, and use of health information.

The diverse set of technologies for storing, processing, sharing and managing health information for use by various stakeholders in the healthcare industry are referred to as *health information technologies (HITs)* (Blumenthal & Glaser, 2007). EHR systems are among the important HITs which are being pursued in most countries around the world (Safran, 2001). The *electronic health record (EHR)* is a record of patient health information generated electronically at the various points of care over the patient's lifetime which can be accessed by all healthcare providers attending to the patient (WHO, 2006). *EHR systems* are the software platforms that healthcare providers use to create, store, update and/or share patients' EHRs (Angst & Agarwal, 2009).

An EHR system can be stand-alone and implemented within a single institution (e.g., hospital) where a patient record is created and used by the units/departments within the institution. WHO (2006) refers to this type of implementation as a *simple EHR system.* With this implementation, it is difficult to track a patient's complete medical history as the patient's data is scattered across the various institutions where they receive care. There can also be a *networked EHR system* in which various HITs collaborate within and across institutional boundaries to allow a patient to receive care from multiple healthcare providers (Li & Slee, 2014). Thus, there is interoperability among providers which enables a complete view of a patient's health information to be maintained (Li & Slee, 2014). Networked EHR systems are more common in developed countries with some countries (e.g., Denmark) having implemented national EHR systems (Mugo & Nzuki, 2014).

The rise in open-source EHR software has increased EHR adoption in developing countries (Webster, 2011). Given that e-health is emerging in these countries, most EHR projects are stand-alone, being implemented at the institutional level even though a number of countries are working on national EHR systems (Ohuabunwa et al., 2016). For instance, whilst several

hospitals in Ghana have adopted EHR systems, the systems are not interoperable and hence patient information is not exchangeable between healthcare providers (International Institute of Communication and Development [IICD], 2014). In view of this context, this study's investigation of consumers' PHI disclosure intentions in a digitized healthcare environment will be undertaken within the context of EHR implementation in a single institution (i.e., a stand-alone/simple EHR system).

1.3 Motivation and Justification of the Research

The motivation for this study is discussed in relation to two areas: gaps in existing research and the study context.

1.3.1 Summary of Gaps in Prior Research

The digital transformation of healthcare has led to increased consumer concerns about the privacy and security of PHI (Anderson & Agarwal, 2011; Angst & Agarwal, 2009). In recent years, IS researchers have focused on understanding individuals' concerns about PHI privacy and their PHI disclosure behaviour in digitized healthcare environments. The existing research shows that PHI privacy concerns and other factors such as trust, privacy risk, and perceived benefits influence individuals' PHI disclosure behaviours (Anderson & Agarwal, 2011; Jena, 2015; Kordzadeh & Warren, 2017) and their adoption of HITs (Li & Slee, 2014; Miltgen, Popovič, & Oliveira, 2013; Mou & Cohen, 2014). The literature also indicates that PHI privacy concerns are shaped by individual characteristics (e.g., age, gender), experiences (e.g., privacy experience), and perception-related factors such as trust and risk. To date, individual characteristics including gender, age, education and health status remain the often-studied antecedents to PHI privacy concerns (e.g., King, Brankovic, & Gillard, 2012; Papoutsi et al., 2015).

The following gaps could be identified in the existing research. First, there is a paucity of research on antecedents to privacy concerns in the healthcare context (Kenny, 2016; Yun, Lee, & Kim, 2019). The majority of the studies have often focused on a small number of antecedents such as individual characteristics (e.g., age, gender, education, and health status) (e.g., Hwang, Han, Kuo, & Liu, 2012; Vodicka et al., 2013; Wilkowska & Ziefle, 2012). Other important antecedents such as privacy regulations, trust and risk perceptions have received scant attention (Kenny, 2016; Yun et al., 2019). This makes it difficult to understand the true relative impacts of the various factors that influence PHI privacy concerns and which factors healthcare stakeholders need to focus on in addressing individuals' concerns.

Second, there is an inadequate measurement of PHI privacy concerns in the majority of the existing studies in healthcare. Validated measures of privacy concerns in IS privacy research are not used and a good number of studies use a single item, examining PHI privacy concerns as a unidimensional construct (e.g., Chhanabhai & Holt, 2007; King et al., 2012; Papoutsi et

al., 2015). This limits our understanding of the different aspects (e.g., collection versus use of PHI) of individuals' concerns regarding PHI privacy (Kenny, 2016).

Third, trust in HIT has been found in some studies to strongly influence PHI disclosure behaviour even more than privacy concerns (Bansal, Zahedi, & Gefen, 2010; Jena, 2015); it also has a strong influence on the adoption of HITs (Miltgen et al., 2013). Yet, the factors that influence individuals' formation of trust in HITs have yet to be considered extensively in IS research despite calls for such investigation (e.g., Beldad, De Jong, & Steehouder, 2010; Kim, 2016).

Fourth, prior research has also not considered a dyadic conceptualization of trust in privacy empirical models. The existing studies in several IS domains have either examined trust in an organization providing an online service (e.g., Metzger, 2006) or trust in the system/technology facilitating the provision of an online service (e.g., Dinev & Hart, 2006). Similarly, in the specific context of healthcare, prior studies either focused on trust in HIT (Anderson & Agarwal, 2011; Jena, 2015) or explored the influence of trust in healthcare providers (e.g., Klein, 2007; Mou & Cohen, 2014). Due to the focus on one perspective of trust in the existing studies, the relationship between the trust dimensions and their relative impacts on behavioural outcomes are under-examined. According to Dinev, Albano, Xu, D'Atri, & Hart (2016), trust in the healthcare organization and trust in HIT are the important objects of trust in the healthcare context. Thus, a dyadic conceptualization of trust must be considered in empirical models examining PHI disclosure behaviour and adoption of HITs.

Fifth, the influence of the negative consequences associated with personal information disclosure on individuals' disclosure intentions in general, has yet to receive considerable attention. The influence of privacy risk on various behavioural outcomes has been examined in prior research. Privacy risk has often been defined as individuals' expectation of negative consequences (or a high potential for loss) associated with personal information disclosure (e.g., Malhotra, Kim, & Agarwal, 2004). However, as Karwatzki, Trenz, Tuunainen, and Veit (2017) have noted, the conceptualization of privacy risk focuses on negative consequences in general and excludes specific outcomes that individuals may perceive to occur from losing control over their personal information. This has led to calls for the examination of the diversity of negative consequences or privacy harms in IS privacy research (Karwatzki et al., 2017; Kokolakis, 2015).

Finally, prior privacy research in the healthcare context and IS privacy research, in general, have largely focused on developed countries (Hong & Thong, 2013; Kenny, 2016). The findings of this previous research may not generalize to developing countries due to factors such as differences in culture and values across countries which can lead to differences in privacy perceptions and its impacts (Bélanger & Crossler, 2011). Whilst there are some case studies that examine PHI privacy concerns among individuals in developing countries (e.g., Bedeley & Palvia, 2014; Willyard, 2010), the extent of these concerns and the degree to which they impact individuals' PHI disclosure behaviours are not known. It is thus imperative to extend current research efforts to the context of developing countries in order to identify and

address particular roadblocks that may lie in the way of successfully digitizing healthcare in these countries.

1.3.2 Importance of the Research Context

Departing from prior IS privacy research which has focused primarily on samples in developed countries, this study will test the proposed research model in Ghana, a Sub-Saharan African country. There are two major healthcare providers (which are called *hospitals*) in Ghana: public/government hospitals and private hospitals. In recent years, these hospitals have introduced various HITs including EHR systems in support of healthcare services (Acquah-Swanzy, 2015; Gyamfi, 2016). Existing EHR systems are stand-alone as they have been introduced within individual institutions. As is the case with many developing countries (see Lewis et al., 2012), the e-health field in Ghana is nascent. However, the country is considered as one of the few African countries with the needed infrastructure (e.g., IT) to implement networked health information systems solution (IICD, 2014). Ghana is thus a suitable context for this study. Additional motivations for PHI privacy studies in a developing country's context are highlighted below.

A recent review of e-health projects in developing countries by PEN (2010) found that issues about privacy and security of individuals' PHI are often completely ignored in the design and implementation of these projects. In the specific case of Ghana, IICD (2014) found that patient information is not adequately secured in the existing e-health systems. According to the review by PEN (2010), the lack of consideration of PHI privacy stems from assumptions made by various stakeholders (e.g., policy makers and system developers) in the development of e-health systems. First, these stakeholders assume that individuals in developing countries are so much in need of care that they do not care about anything else. This claim, however, is contradicted by case studies which indicate consumer concerns about privacy in both the traditional healthcare and the emerging e-health settings (e.g., Dapaah & Senah, 2016; Bedeley & Palvia, 2014). Another assumption made is that the risks of abusing IT systems are limited as individuals in developing countries lack technical computing skills. This assumption is also challenged by the recent increase in cybercrimes in Africa (Serianu, 2016) including sextortion (Debrah, 2019), electronic fraud (Myjoyonline, 2018), and leaks of medical records (Technomag, 2018). Given the increased media attention on these crimes and on other abuses of digitized information in countries such as Ghana (Darko, 2015; Kyei-Boateng, 2018), when individuals suspect they are potentially vulnerable to abuse through weak privacy protection in e-health systems, they may resist digitization of their health information.

Individuals' attitudes and readiness towards the adoption of IT innovations are critical to the use and success of any IS. This is especially true for e-health applications as "the highly personal and sensitive nature of healthcare data and the associated concerns about privacy can impede the adoption of even the most efficient and technologically perfect system" (Dinev et al., 2016). Most IT innovations in the developing world fail and this has been attributed to lack of understanding of situation-specific factors including users' skills, culture, activity, etc. in

the development of IT systems (Heeks, 2002). Although consumers of healthcare services are an important HIT stakeholder (Payton, Pare, LeRouge, & Reddy, 2011), studies indicate that individuals' needs and interests including the privacy of their health information are often not considered in e-health projects in developing countries (LSE, 2010; IICD, 2014). An empirical study from the consumers' perspective is thus important in understanding individuals' perceptions and concerns about the electronic storage and use of PHI, so appropriate steps can be taken to address these.

In summary, the foregoing discussions related to the healthcare and geographic contexts of this study as well as the gaps in extant research justify the need to better understand the concerns and intentions of individuals in developing countries toward health information disclosure in a digitized healthcare environment.

1.4 Research Objectives

This study seeks to *understand the factors that influence the willingness of individuals in developing countries to disclose their PHI to receive care in a digitized healthcare environment*. This overarching aim of the study is further represented by three research objectives where the aims are to understand (i) the drivers and inhibitors of PHI disclosure, (ii) the extent and antecedents of PHI privacy concerns, and (iii) the antecedents to trust in HIT.

The first objective is to explore the factors that drive individuals' willingness to disclose PHI (which are called *drivers*), and those that inhibit their PHI disclosure (which are called *inhibitors*). The drivers explored in the study include convenience and trust (Dinev & Hart, 2006); a dyadic conceptualization of trust is considered (i.e., trust in healthcare and trust in HIT) (Dinev et al., 2016). Regarding inhibitors, in addition to PHI privacy concerns and privacy risk (Dinev & Hart, 2006), this study also explores the influence of potential negative consequences (Karwatzki et al., 2017; Kokolakis, 2015) individuals may perceive to result from PHI privacy loss on their willingness to disclose PHI.

The study draws on the privacy calculus theory to examine the influence of the drivers and inhibitors on willingness to disclose PHI. The privacy calculus suggests that individuals engage in a cognitive cost-benefit analysis when deciding on personal information disclosure and their final behaviour (i.e., personal information disclosure or non-disclosure) is determined by the outcome of this analysis (Dinev & Hart, 2006). In general, individuals disclose personal information for beneficial outcomes perceived to be worth the costs associated with disclosure (Culnan & Bies, 2003; Dinev & Hart, 2006). Prior studies using the privacy calculus have modelled benefits as the factors motivating individuals' personal information disclosure and costs as factors discouraging privacy disclosure (e.g., Dinev & Hart, 2006). As an example, Anderson and Agarwal (2011) considered trust and privacy concerns as the core relationships in the privacy calculus with trust representing the benefit side and privacy concerns representing the cost side of the calculus equation. Consistent with prior research, the drivers

considered in this study represent the benefit side of the calculus equation, whereas inhibitors represent the costs in the calculus analysis.

Prior research shows that PHI privacy concerns and trust in HIT are important factors that have a strong influence on behavioural outcomes including willingness to disclose PHI (Anderson & Agarwal, 2011; Jena, 2015; Miltgen et al., 2013). The second objective of the study is therefore to understand the extent of PHI privacy concerns among individuals in developing countries and the factors influencing these concerns. The third objective is to explore the antecedents to trust in HIT.

To examine PHI privacy concerns, this study adapts the Concern for Information Privacy (CFIP) measure (Smith, Milberg, & Burke, 1996) to the healthcare context of developing countries. Drawing on the existing literature and considering the geographic context of the study, four lesser studied factors in prior research are explored as antecedents to PHI privacy concerns and trust in HIT: perceived attitude of health workers, perceived effectiveness of government regulation, trust in healthcare providers, and privacy risk. Further, a number of individual characteristics (e.g., age, gender) and experiences (e.g., computer experience) are used as control variables on both PHI privacy concerns and trust in HIT (Esmaeilzadeh, 2018a; Perera et al., 2011).

This study draws on procedural and interactional dimensions of justice theory to explore the influence of perceived attitude of health workers and perceived effectiveness of government regulation. *Procedural justice*, in the context of information privacy, pertains to individuals' perceptions of fairness of the procedures enacted for the collection and use of personal information (Xu, Teo, Tan, & Agarwal, 2009). Government regulation can ensure that individuals' personal information is collected and used fairly and this can provide individuals with a sense of procedural justice (Xu et al., 2009). This study, therefore, explores whether procedural justice provisions through government regulation influence individuals' PHI privacy concerns and their trust in HITs.

Interactional justice refers to a party's fairness perceptions regarding the interpersonal treatment received from another party in an exchange relationship (Son & Kim, 2008). Interactional justice is represented as perceived attitude of health workers in this study. Perceived attitude of health workers reflects individuals' perceptions of the quality of interpersonal treatment received during a healthcare service encounter (Sumaedi, Yarmen, & Yuda Bakti, 2016). The justice literature shows that perceptions of fairness of interpersonal treatment increase trust beliefs (e.g., Kernan & Hanges, 2002). Some researchers have also argued that how consumers are treated interpersonally in an information transactional exchange can influence their privacy concerns (Bies, 2001; Culnan & Bies, 2003). Perceived attitude of health workers is thus explored as an antecedent to PHI privacy concerns and trust in HIT.

In summary, this study draws on the privacy calculus theory to examine the simultaneous influence of contrary factors (i.e., drivers and inhibitors) on willingness to disclose PHI. It further integrates the privacy calculus with procedural and interactional dimensions of justice

theory to explore perceived effectiveness of government regulation and perceived attitude of health workers as antecedents to PHI privacy concerns and trust in HIT. The influence of the other antecedents, trust in healthcare providers and privacy risk, are explored drawing on prior privacy research.

1.5 Research Questions

Within the framework of the main research question and the research objectives outlined above, the study poses the following specific questions:

RQ1: What factors drive or inhibit individuals' willingness to disclose PHI?

RQ2: To what extent are individuals concerned about the privacy of their PHI?

RQ3: What are the factors that influence PHI privacy concerns?

RQ4: What are the factors that influence trust in HIT?

1.6 Research Methodology

This study tests a model of antecedents to willingness to disclose PHI, PHI privacy concerns, and trust in HIT (Section 1.4). Therefore, the philosophical approach of this study is positivist as it focuses on testing relationships between phenomena which have been reduced to empirical data. The quantitative research methodology, which is predominantly associated with the positivist research philosophy (Creswell & Clark, 2017), was used to test the proposed research model. Existing validated measures were used to measure constructs in the research model. The relationships in the model were tested using data from a survey of individuals in Ghana and were analysed using the partial least squares approach to structural equation modelling (PLS-SEM) using SmartPLS 3.2.8.

1.7 Research Contributions

Individuals' willingness to disclose and allow electronic storage of their PHI is critical to the successful digitization of healthcare (Angst & Agarwal, 2009). As developing countries migrate to digitized healthcare systems, this study seeks to provide insights into the factors that both support and hinder individuals' PHI disclosure in digitized healthcare settings. This study has a number of potential implications for theory and practice.

From a theoretical perspective, this study aims to extend the privacy calculus theory to include a dyadic conceptualization of trust (i.e., trust in healthcare providers and trust in HIT). The existing studies in the healthcare context either examined trust in healthcare providers (Mou & Cohen, 2014) or trust in HIT (e.g., Dinev et al., 2016). The focus on one perspective on trust

also pertains to IS privacy research in general (Morosan and DeFranco, 2015). By examining in a single model the two recommended objects of trust in the context of online transactions (Beldad et al., 2010; Dinev et al., 2016), this study will clarify the relative influence of trust in the technology (in this case HIT) facilitating electronic transactions and trust in the organization deploying the technology (in this case healthcare providers) on personal information disclosure.

Privacy concerns and privacy risk have been examined in prior research as major deterrents of information disclosure (e.g., Dinev & Hart, 2006). Whereas privacy risk has been conceptualized as an expectation of negative outcomes associated with information disclosure (Malhotra et al., 2004), these negative outcomes are largely conceptualised in general terms with reference to potential loss of control over personal information (e.g., Dinev & Hart, 2006; Xu et al., 2009). However, the specific negative consequences that individuals may perceive to result from the privacy loss of their disclosed personal information are not considered (Karwatzki, et al., 2017). This study will explore the influence of potential negative consequences individuals may perceive to result from PHI privacy loss on their willingness to disclose PHI. Three types of negative consequences related to social, economic, and emotional consequences will be explored. This study thus aims to extend the cost side of the privacy calculus and responds to calls to examine diversity of privacy harms in empirical models (Kokolakis, 2015).

A number of studies show that trust more strongly predicts behaviour than privacy concerns when the two constructs are examined together (Dinev & Hart, 2006; Van Slyke, Shim, Johnson, & Jiang, 2006). This highlights the need to examine together the relevant risk/benefit factors in the privacy calculus depending on contextual factors including technology and users. For example, Bélanger and Crossler (2011), in their systematic review of empirical IS privacy literature called for more studies to examine trust and privacy concerns together to explore their relative influence on behavioural outcomes. By considering a dyadic conceptualization of trust and specific negative consequences associated with PHI disclosure in the privacy calculus, this study investigates a more detailed model which will provide insight into the relative importance of the calculus factors that influence PHI disclosure intentions.

Prior research shows PHI privacy concerns as a major factor which has a strong negative impact on individuals' PHI disclosure behaviours (Anderson & Agarwal, 2011) and adoption of HITs (Angst & Agarwal, 2009). However, there is a limited understanding of the factors that influence PHI privacy concerns as prior studies have largely focused on a small number of antecedents (e.g., age, gender, education, and health status) (e.g., Hwang et al., 2012; Vodicka et al., 2013). This study explores a broad range of antecedents across individual characteristics, experiences, and perceptions to improve understanding of the factors that exert significant influence on PHI privacy concerns and their relative importance.

In some prior studies, as mentioned above, trust in HIT has been found to strongly predict PHI disclosure behaviour than PHI privacy concerns (Bansal et al., 2010; Jena, 2015); it also has a strong influence on the adoption of HITs (Miltgen et al., 2013). However, like PHI privacy

concerns there is also a lack of empirical studies on factors that impact individuals' trust in HITs. Recently, Dinev, Xu, Smith, and Hart (2013) have urged researchers to move beyond the focus on formation of privacy perceptions to the examination of trust and information disclosure behaviours. Beldad et al. (2010) have also issued a specific call to study antecedents to trust in HITs. This study responds to this call and aims to improve our understanding of the important factors affecting HIT by exploring a number of antecedents related to individual characteristics, experiences, and perceptions.

The study integrates the privacy calculus theory with procedural and interactional justice to study the effects of two less studied antecedents to PHI privacy concerns and trust beliefs: perceived attitude of health workers, and perceived effectiveness of government regulation. Procedural justice and interactional justice are linked respectively with perceived effectiveness of government regulation and perceived attitude of health workers. Drawing on the two justice dimensions, it is argued that individuals' concerns about PHI privacy and their trust beliefs may be influenced by their evaluation of how fairly and respectfully they have been treated interpersonally and in the information exchange during the healthcare service encounter.

Following their systematic review of the IS privacy literature, Bélanger and Crossler (2011) called for the need to extend the boundaries of IS privacy research beyond its predominant focus on samples in developed countries (especially the USA) so as to increase its generalizability. In response to the above call, this study will develop and empirically tests a research model examining PHI disclosure intentions in the understudied context of developing countries. By maintaining the underlying theoretical framework of the privacy calculus which has been used extensively in analysing privacy concerns and its impacts on behaviour (Culnan & Bies, 2003), the study will evaluate the model's applicability to explaining privacy behaviour in developing countries.

From a practical perspective, Benbasat and Zmud (1999) have recommended the conduct of research that produce outcomes of future value to stakeholders interested in the research. Given e-health is nascent in developing countries, this study is opportune as the findings will provide insights that can help in shaping individuals' attitudes toward HITs prior to their full-fledged development and introduction. Equally as important, they will also contribute to the crafting of policies and regulations to ensure privacy by design in the development of digitized healthcare systems, as well as to protect consumer privacy in the use, retention and sharing of their health information by healthcare stakeholders.

1.8 Outline of Thesis

The thesis is organized into seven chapters as follows:

Chapter 1 – *Introduction,* provides the background and motivation for the research and outlines the study's objectives and research questions, methodology and contributions. The chapter ends with this section about how the thesis is organized.

In Chapter 2 – *Literature Review*, the existing IS privacy literature is reviewed to identify gaps in our understanding of the factors influencing PHI privacy concerns, trust in HITs, and PHI disclosure in digitized healthcare environments.

Chapter 3 – *Theoretical foundation and Proposed Research Model*, describes the theories underpinning the study and presents the research model proposed to address the gaps in existing research. The hypotheses tested in the study are discussed.

Chapter 4 – *Research Methodology,* explains the philosophical assumptions underpinning the study and the quantitative research methodology used to test the proposed research model. It also describes the research setting, the sampling procedure used in the study, and the survey conducted to collect data for the study.

Chapter 5 – *Data Analysis,* presents results from the quantitative data analysis with particular focus on the reliability and validity of the research model and testing of hypotheses using the partial least square structural equation modelling (PLS-SEM) technique.

Chapter 6 – *Discussion*, discusses findings from the quantitative data analysis in relation to the objectives of the study and previous research.

Chapter 7 – *Conclusion*, details the contributions of this study to theory and practice, acknowledges the limitations of the study and provides future research directions. It concludes with a summary of the study.

CHAPTER TWO: LITERATURE REVIEW

This chapter reviews the existing IS privacy literature. The main aim of the review is to ascertain the current knowledge level and identify the gaps in the existing studies. The chapter begins with a brief review of the origins of the information privacy construct. The conceptualizations of information privacy across various academic disciplines (including the IS discipline) are reviewed and the definition used in this study is presented. An overview of IS privacy research, in general, is provided followed by a detailed review of privacy research in the healthcare context. The gaps identified in IS privacy research in general and research specifically related to the healthcare context are presented and the justification for addressing these gaps are provided. A recap of these gaps is provided to conclude the chapter.

2.1 Information Privacy

Privacy has been an issue of discussion throughout history and a subject of study in various academic disciplines. This section first briefly traces the historical foundations of the privacy construct. Next, the different conceptualizations of privacy across various academic disciplines are presented. The section concludes with the definition of privacy chosen for this study.

2.1.1 Historical Foundations

Several contradictory accounts exist regarding the roots of the concept of privacy and as a result, it is difficult to pinpoint the history of privacy (Kenny, 2016). According to Zheng, Shi, Zeng, and Lu (2010), privacy derives from the Latin word *PRIVARE*, which means to separate. This meaning of privacy is reflected in the writings of Chinese and Greek philosophers in the 3rd and 4th centuries, respectively (Newell, 1995). These writings emphasized a clear distinction between the concepts of private and public. For instance, the Chinese philosophers related the idea of private to self-centeredness, whereas public referred to the affairs of government. The Greek philosopher Aristotle also distinguishes between public activities that individuals engage in (e.g., political activities) and private activities which they engage in alone or together with the family (DeCew, 2018).

The text of the three monotheistic ancient religions also shows that the human quest for privacy dates back to ancient societies (Acquisti, Brandimarte, & Loewenstein, 2015). In the Bible, Genesis 3:7 recounts Adam and Eve hiding in shame from the prying eyes of God when they discovered their nakedness after attaining the knowledge of good and evil by eating the fruit of knowledge (Rykwert, 2001). The Talmud also teaches that individual home-builders should not position the front doors or windows of their houses so that they directly face those of their neighbours (Enkin, 2012). Similarly, the Holy Quran teaches against spying on one another (49:12) and entering the houses of other people without the consent of the house occupants (24:27) (Hayat, 2007).

The above historical examples show that privacy has been construed in various ways. However, one important notion of privacy that emerges from the historical examples relates to territorial or physical privacy. This notion of privacy concerns "the physical access to an individual and/or the individual's surroundings and private space" (Smith, Dinev, & Xu, 2011). With the advent of the information age, however, the contemporary focus of privacy has shifted to information privacy, which concerns "access to individually identifiable personal information" (Smith et al., 2011). Privacy, as used in this study, refers to information privacy.

Information privacy began to be an issue of public deliberation and policy consideration in the 1960s (Regan, FitzGerald, & Balint, 2013). This period till the late 1980s saw the rise of computer and network systems. The potential dark sides of the new technologies were recognized and thus Fair Information Practices (FIPs) and privacy regulations were established for privacy protection (Smith et al., 2011). Since the 1990s, the prevalence of the Internet and ICTs that enable the collection and sharing of large volumes of information have led to increased concerns about privacy (Regan et al., 2013; Smith et al., 2011). The heightened concerns about privacy have generated research interests in diverse IS domains (Smith et al., 2011).

2.1.2 Privacy Definitions across Disciplines

Information privacy is a complex concept and has been studied from many perspectives including law, marketing, economics, psychology, management, and Information systems (Pavlou, 2011; Smith et al., 2011). However, the concept has been variously defined across and within academic disciplines and there is no universally accepted definition for information privacy (Pavlou, 2011). Following an extensive multidisciplinary review of the privacy literature, Smith et al. (2011) concluded that the approaches to defining privacy can be broadly classified as either *value-based* or *cognate-based*.

Value-based definitions include the views of *privacy as a right* and *privacy as a commodity*. The view of privacy as a right has largely been discussed in the law discipline. Most studies in this discipline believe that individuals have a right to privacy (e.g., Austin, 2003; Warren & Brandeis, 1890). For instance, Warren and Brandeis (1890) defined privacy as "the right to be left alone". This definition has formed the basis of most privacy legislation and has also been used in other disciplines (e.g., Phelps, Nowak, & Ferrell, 2000; Sheehan, 2002). Warren and Brandeis (1890) did not consider privacy as an absolute right and this position has been emphasized by recent scholars such as Austin (2003) and Hughes (2012). These scholars maintain that there is the need to strike a balance between the privacy rights of the individual and the public interests as well as other competing rights.

Researchers in other disciplines such as political science and economics have similarly argued that privacy is not an absolute right but that which can be assigned a negotiable economic value and be considered in a cost-benefit analysis (e.g., Cohen, 2001; Hughes, 2012; Moloney & Potìa, 2013; Posner, 1978). From this perspective, there has emerged the treatment of privacy

as a commodity whereby consumers are said to view their privacy as a commodity that can be exchanged for perceived benefits (Campbell & Carlson, 2002; Davies, 1997). The stream of research based on the privacy as a commodity perspective have sought to understand individuals' evaluation of the cost and benefits associated with the protection or revelation of personal information (Acquisti, 2009; Posner, 1978, 1981; Stigler, 1980). A major assumption of this stream of research is that individuals always act rationally in their decision to disclose private information (Acquisti, 2010; Acquisti, John, & Loewenstein, 2013).

The *cognate-based* definitions of privacy include the views of *privacy as a state* and *privacy as control*. The notion of privacy as a state has been advanced in the psychology discipline where privacy has been conceptualized as an individual's desire to exist in separation from others. According to the systematic review by Smith et al (2011), the concept of privacy as a state was introduced by Westin (1967) who defined privacy as the "voluntary and temporary withdrawal of a person from the general society through physical or psychological means". Similar definitions have been used by other scholars. For instance, Bates (1964) defined privacy as "a person's feeling that others should be excluded from something which is of concern to him, and also a recognition that others have a right to do this". Weinstein (2017) has also defined privacy as a state of "being apart from others". Weinstein (2017) argued that privacy is similar to concepts such as loneliness, alienation, ostracism and isolation; however, privacy is desired by individuals whereas the other concepts are avoided. The above conceptualization of privacy stems from the view in the psychology discipline that privacy is a critical element for a person's development (Edney & Buda, 1976; Jourard, 1966; Westin, 1967). Therefore, the ability of an individual to limit access to him/herself in different situations is vital to an individual's self-definition (Altman, 1977; Westin, 1967).

Privacy as control definitions view privacy as individuals' control of physical access to themselves and access to their personal information. The concept of privacy as control has been influenced largely by Westin (1967) and Altman (1976). Altman (1976) defined privacy as "the selective control of access to the self". Focusing on information access, Westin (1967) defined privacy as the right of individuals to decide what information about themselves should be known by others and under what conditions. The control-based definition has been used in various fields especially marketing. For example, Goodwin (1991) defined privacy as the consumer's ability to control the physical presence of others during a transaction and the sharing of their information related to or provided during such transactions with parties not present during the said transaction. According to Goodwin (1991), physical presence may be manifested by unwanted telephone, mail, or personal intrusion in the consumer's environment. As discussed below, the control-based definition has also been the dominant definition of privacy used in IS (e.g., Bellman, Johnson, Kobrin, & Lohse, 2004; Culnan & Armstrong, 1999).

2.1.3 Privacy Definition in Information Systems

Most views in the IS discipline has been influenced by other disciplines. The conceptualization of privacy is no exception. The systematic review by Smith et al. (2011) shows that IS discipline draws heavily on the privacy as a commodity and privacy as control views.

A large number of studies conducted in several IS domains show that individuals view their privacy as a commodity which they trade for certain beneficial outcomes. For instance, in the context of e-commerce, consumers share personal information with firms for monetary rewards, customized and other personal services (Grossklags & Acquisti, 2007; Phelps et al., 2000; Spiekermann, Grossklags, & Berendt, 2001; White, 2004). Regarding location-based services, Xu et al. (2009) found that individuals are willing to disclose their information for personalized services. Similarly, benefits such as enjoyment and relationship building have been shown to impact individuals' self-disclosure in online social networks (OSNs) (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Zhao, Lu, & Gupta, 2012). Further, in the healthcare context, several studies show that individuals are more willing to disclose their PHI for various purposes including care (Anderson & Agarwal, 2011), personal wellbeing (Kordzadeh & Warren, 2017) and support for scientific and medical research (Thiebes, Lyytinen, & Sunyaev, 2017).

Whilst individuals disclose personal information for various beneficial outcomes, they also desire privacy as there are risks (e.g., loss of relationships, jobs, etc) entailed in making private disclosures (Petronio, 2002), especially in online environments (Metzger, 2006). Therefore, individuals seek to control what personal information is disclosed and when this is disclosed as they balance the need for disclosure and the desire for privacy (Petronio, 2002; Westin, 2000). Several public opinion polls and empirical studies lend support to individuals' desire for control over their personal information. A 2008 poll by Consumer Reports (2008) shows that most consumers want to control how their online information is collected and used. Similarly, a recent poll by Pew Research Centre found that 93% of consumers desire control as to who can get information about them whilst 90% want to control what information is collected about them (Madden & Rainie, 2015). With specific regard to health information, Caine and Hanania (2012) found that patients want to control the type of PHI they share and with whom this information is shared. Without control over the use of PHI, some individuals withhold information from healthcare providers (Agaku et al., 2013).

Due to consumers' greater desire for control over their personal information, some scholars have argued that individuals must be able to exercise a substantial degree of control over the collection and use of their information by organizations (Clarke, 1999; Phelps et al., 2000). The concept of control, therefore, remains an essential element in the definitions of privacy in the IS discipline. Reviewing extant IS privacy literature, Bélanger and Crossler (2011) noted that the common theme of privacy across most studies is an individual's ability to control the use of their personal information. Consequently, the authors defined information privacy as "the desire of individuals to control or have some influence over the data about themselves". Similarly, in another review, Smith et al. (2011) observed that Westin's (1967) control-based

definition of privacy is often used by IS researchers. As an example, Culnan and Bies (2003) defined information privacy as "the ability of individuals to control the terms under which their personal information is acquired and use".

In the healthcare context, extant studies fail to explicitly define information privacy or adapt existing definitions (Kenny, 2016). A number of studies also fail to distinguish between privacy and related concepts such as security and confidentiality (Shaw, Kulkarni, & Mador, 2011). Addressing this gap, Kenny (2016) adapted Bélanger and Crossler's (2011) definition to the healthcare context and defined information privacy as: "the desire of citizens' to be afforded a degree of control over the collection and dissemination of their personal health information by health organizations and technology vendors". In the current study, information privacy in relation to PHI is defined as *individuals' desire to control the collection and use of their personal health information by healthcare providers*. This definition differs slightly from Kenny's (2016) definition in terms of the information practices of health organizations over which individuals desire control; as such, this study focuses on *collection and use of PHI* as opposed to *collection and dissemination of PHI* in Kenny (2016).

PHI is primarily used for the provision of care by healthcare providers who are often the primary recipients, users and custodians of this information (Anderson, 2000). Aside from the primary purpose of providing care, these providers may also use PHI for other internal purposes including assessing service quality and improving efficiency within the healthcare system (Appari & Johnson, 2010). However, there are several other secondary uses of PHI (e.g., research, social services, regulation, marketing, etc.) which necessitate dissemination or sharing of PHI across organizational and sometimes regional/national boundaries (Anderson, 2000; Appari & Johnson, 2010). By focusing on collection and use of PHI, this study's definition encompasses the broad range of uses to which PHI may be put some of which will involve sharing or dissemination of PHI among the various stakeholders interested in consumers' PHI for various purposes. The above definition is used in the thesis when referring to health information privacy or PHI privacy.

2.2 Overview of IS Privacy Research

The previous section (Section 2.1) discussed the historical roots of information privacy and its conceptualization across various academic disciplines including IS. This section provides an overview of the empirical research on information privacy in IS. In the last decade, an extensive review of IS privacy research has been conducted by several researchers (e.g., Bélanger & Crossler, 2011; Li, 2011; Smith et al., 2011; Yun et al., 2019). The review in this section is, therefore, an overview of the existing review studies. It first highlights the centrality of *privacy concerns* in the IS privacy literature and the factors that influence these concerns. Next, other salient factors that in addition to privacy concerns influence the behaviours of individuals including personal information disclosure are discussed.

The discussion in Section 2.1 highlights individuals' desire for control over the collection and use of their personal information by organizations as central to the definition of information privacy in the IS discipline. However, the ability of individuals to control the acquisition and use of their personal information is undermined with the advent of digital information making information privacy a core topic in IS research (Pavlou, 2011). IT permeates almost every aspect of our lives and at the various points of contact with IT systems, we are leaving digital footprints that will outlive us. Equally important are advancements in the ability to aggregate, analyse, and draw sensitive inferences from individual's electronically stored data (Acquisti et al., 2015; Malhotra et al., 2004). Organizations (e.g., large firms like Google, Microsoft, and Facebook) are therefore able to build comprehensive profiles about users and with the increased ability to easily and speedily share electronic information, they are able to easily share their collected customer data with their affiliates thereby increasing the risk of loss of consumer information (Smith et al., 2011). Consumer concerns about privacy have thus heightened in the information age (Pavlou, 2011).

The growing consumer concerns about privacy has garnered the attention of researchers and practitioners alike, and as a result, privacy concerns has become a critical construct in IS privacy research and is often used as a proxy for information privacy (Smith et al., 2011). Several IS studies conducted in a variety of domains such as e-commerce (Dinev & Hart, 2006), the Internet (Malhotra et al., 2004), online social networks (Jiang, Heng, & Choi, 2013), healthcare (Anderson & Agarwal, 2011), and location-based services (Xu et al., 2009) have examined both the antecedents which lead to individuals' formation of privacy concerns, and the behavioural outcomes of these concerns. Following their comprehensive review, Smith et al. (2011) summarized the extant positivist empirical privacy research in an overarching macromodel called APCO (Antecedents→Privacy Concerns→Outcomes). Other IS theory and review articles on privacy have produced similar models in terms of classification of variables that have been considered in prior research (Bélanger & Crossler, 2011; Li, 2011, 2012; Yun et al., 2019). The construct *privacy concerns* is core to all these macromodels.

In line with the control-based definition of information privacy, privacy concerns has often been defined in terms of consumers' worry and anxiety regarding organizational practices related to the collection and use of their personal information (Smith et al., 1996; Van Slyke et al., 2006). Some studies have adapted this definition to the Internet context focusing on consumers' concerns about what happens to the personal information they disclose via the Internet and how this information is used (Dinev & Hart, 2006; Malhotra et al., 2004). Both conceptualizations reflect individuals' concerns about the possibility of loss of their disclosed information (Dinev & Hart, 2006). These concerns arise from individuals' lack of ability to control the collection and use of their personal information, a situation exacerbated by the advancements in IT. Several empirical studies show that privacy concerns negatively relate to various behavioural outcomes including willingness to share personal information, and acceptance of online services (e.g., Dinev & Hart, 2006; Van Slyke et al., 2006).

Regarding antecedents to privacy concerns, a myriad of antecedents has been examined in the extant IS privacy literature. These range from individual factors (e.g., gender, age, personality

traits, etc.) to privacy-related factors such as privacy risk, past privacy experience, and disposition to privacy. However, in their recent review Yun et al. (2019) found that with the exception of a few antecedents (e.g., Internet experience, privacy risk, perceived control, and trust) most of the antecedents (e.g., privacy regulation, information sensitivity, privacy awareness, privacy orientation, etc.) have been examined only a few times. Consequently, the Antecedents→Privacy concerns research stream is still at the exploratory stage of theory development (Yun et al., 2019). There is, therefore, the need for more empirical studies which harness various theories in examining the existing antecedents as well as new ones to ensure theory development in this domain of research.

In examining outcomes in the APCO model, a large number of studies draw on the "privacy as a commodity" perspective. These studies consider consumers' privacy disclosure decision to be an outcome of a cost-benefit analysis popularly called the privacy calculus (Culnan & Armstrong, 1999). The privacy calculus suggests that when requested to provide personal information, consumers compare the cost of losing privacy against the potential gain of disclosing their private information and the outcome of the privacy trade-off determines their final behaviour (Dinev & Hart, 2006; Jiang et al., 2013; Xu et al., 2009). The calculus perspective is underlined by expectancy theory (Victor, 1964) which holds that behaviour of individuals follows from a rational choice among alternatives the purpose of which is to maximize positive outcomes (i.e., benefits) and minimize negative outcomes (i.e., costs).

Behavioural intention variables such as willingness to disclose information and intention to engage in a transaction with others online are the most prominent outcomes studied in the IS privacy literature (Smith et al., 2011; Yun et al., 2019). Drawing on the privacy calculus theory, several studies have considered other factors in addition to privacy concerns and examined their impact on the behavioural intention variables. The commonly studied factors include trust beliefs, privacy risks, and perceived benefit (Li, 2011; Smith et al., 2011). In prior research, privacy concerns and privacy risks have been modeled as the main barriers to information disclosure (i.e., the cost side of the calculus equation), whereas perceived benefits and trust represent the drivers of personal information disclosure (i.e., the benefit side of the calculus equation) (Dinev & Hart, 2006). As privacy concerns have been discussed earlier, the other three factors are briefly explained below.

Privacy risk reflects an individual's belief that there is a high possibility of loss regarding disclosure of personal information to a transacting partner (e.g., firm) (Malhotra et al., 2004). Sources of privacy risk identified in the literature include misuse of personal information, such as insider disclosure or unauthorised access and theft (Rindfleisch, 1997). Other sources relate to organizational opportunistic behaviour including selling to or sharing information with third-party institutions not involved in the original transaction with the customer (Dinev & Hart, 2006). Similar to privacy concerns, privacy risk has been found to negatively impact several behavioural outcomes, such as intention to conduct transactions (Pavlou, 2003; Pavlou & Gefen, 2004), and intention to disclose personal information (Malhotra et al., 2004; Xu, Teo, & Tan, 2005). As mentioned above, several studies support the predictive influence of privacy risk on privacy concerns (Dinev & Hart, 2004, 2006).

In addition to the cost factors (i.e., privacy risk and privacy concerns), individuals also account for the benefits they expect to gain in exchange for sacrificing their private information in the calculus analysis. Perceived benefits include an individual's perception that value will be derived from personal information disclosure in transacting with others (Wilson & Valacich, 2012). Several prior studies (e.g., Dinev & Hart, 2006; Xu et al., 2009) show that the benefits individuals perceive of disclosing personal information can override privacy risk and concerns and thereby induce privacy disclosure in return for the benefits. Some of the benefits that individuals desire in return for privacy disclosure include monetary rewards (Grossklags & Acquisti, 2007), personalized services (Xu et al., 2009), and relationship building (Krasnova et al., 2010). Reviewing prior privacy literature, Smith et al. (2011) classified the benefits of information disclosure as economic or financial benefits (Hann, Hui, Lee, & Png, 2007; Hui, Teo, & Lee, 2007; Xu et al., 2009), personalization or convenience (Hann et al., 2007; White, 2004), and social or relational benefits (Jiang et al., 2013; Lu, Tan, & Hui, 2004).

Trust is another important construct often examined alongside the above discussed cost-benefit elements in the calculus (Bélanger & Crossler, 2011; Smith et al., 2011). In general, trust reflects one's willingness to assume the risks associated with the target of trust and behaviourally depend on the target to complete a task (Li, Hess, & Valacich, 2008). Trust has been shown in several studies as having a strong impact on behavioural outcomes (Dinev & Hart, 2006; Miltgen et al., 2013). In some studies, it is considered the main factor of individuals' privacy disclosure (Belanger, Hiller, & Smith, 2002; Westin, 2000). Several other studies show that trust has a stronger impact on consumer behaviour when examined together with privacy concerns (Dinev & Hart, 2006; Van Slyke et al., 2006). Yet other studies have found trust as a mediator of the relationship between privacy concerns and willingness to engage in online transactions (Van Slyke et al., 2006). Given the critical role of trust, several researchers have called for more studies to examine the mediating or stronger effect of trust relative to privacy concerns (Bélanger & Crossler, 2011; Pavlou, 2011).

In general, the extant IS privacy research has improved our understanding of the factors that contribute to individuals' formation of privacy concerns and those that impact their privacy disclosure behaviours. As noted by Dinev, McConnell, and Smith (2015), the core assumption underlying extant studies is rooted in standard economic theory: that human beings are rational agents who always make logical decisions (Ariely, 2009). Individuals, therefore, are said to engage in deliberate and effortful analysis in forming privacy-related perceptions and in their privacy disclosure behaviours (Dinev et al., 2015). The dominant theoretical approach to studying privacy in the extant literature has thus been cognitive and consequentialist (Anderson & Agarwal, 2011; Dinev et al., 2015).

2.3 IS Privacy Research in Healthcare

The previous section provided an overview of empirical IS privacy research in general. The existing literature shows privacy concerns and trust as the most critical constructs which have a strong influence on various behavioural outcomes (Bélanger & Crossler, 2011; Dinev & Hart,

2006). They are considered the core relationships in the privacy calculus (Culnan & Bies 2003; Dinev & Hart 2006; Malhotra et al. 2004), the dominant theory used in existing IS privacy studies (Yun et al., 2019). For instance, in the Internet context, trust in the Internet is the main factor which drives consumers' willingness to disclose personal information to transact on the Internet, whereas Internet privacy concerns is the main deterrent of consumers' willingness to disclose their personal information (Dinev & Hart, 2006).

This section reviews privacy research specifically related to the healthcare context. In the healthcare context, Anderson and Agarwal (2011) similarly consider PHI privacy concerns and trust in the electronic medium as the main factors influencing individuals' willingness to disclose their PHI in digitized healthcare environments. Therefore, given the salience of privacy concerns and trust in information privacy-related contexts, the review of privacy studies in the healthcare context focused on PHI privacy concerns and trust. The sections that follow reviews the literature regarding the conceptualization of PHI privacy concerns and trust as well as their antecedents and consequences. The gaps in the existing research are highlighted.

2.3.1 PHI Privacy Concerns

Since the time of the ancient Greeks, health information has been regarded as sensitive as evident in the Hippocratic Oath taken by physicians in the 5th century B.C. (Libert, 2015). It is thus not surprising that the health informatics literature has acknowledged the highly personal and sensitive nature of health information and advocated that health information be distinguished from other forms of commercial or research-related data (Hodge Jr, Gostin, & Jacobson, 1999; Kam & Chismar, 2005; Rohm & Milne, 2004). The sensitivity of health information is emphasized by the severity of risks (e.g., loss of job or occupational licensing, life insurance, etc.) inherent in its compromise (Beckerman et al., 2008). Consumers, therefore, are more concerned about the privacy of their health information compared to other types of personal information (Gostin & Nass, 2009; Kam & Chismar, 2005).

Consumers' concerns about PHI privacy have heightened with the digital transformation of healthcare (Anderson & Agarwal, 2011; Angst & Agarwal, 2009). These concerns stem from the susceptibility of digitized PHI to criminal attacks (e.g., hacking), especially when shared over a digital medium between the various stakeholders within the healthcare ecosystem (Fichman et al., 2011), and the ease and speed with which these stakeholders entrusted with protection of consumers' PHI can carry out opportunistic activities. Lending support to this, several studies have noted that most privacy breaches of PHI come from organizations which have authorised access to PHI as well as outside attacks (Anderson, 2000; Appari & Johnson, 2010; Rindfleisch, 1997). For instance, in a recent study of 91 health organizations, Ponemon Institute (2016) found that 90% had experienced a data breach with criminal attacks and malicious insiders representing the main sources of breach.

Due to the growing concerns about PHI privacy, privacy concerns is considered a critical contextual variable in HIT research with its antecedent factors and its influence on consumer

behaviour being the focus of IS privacy researchers (Romanow, Cho, & Straub, 2012). However, as observed by Kenny and Connolly (2015), there are problems in the majority of existing research regarding the conceptualization of privacy concerns and its measurement in the healthcare context. For example, in a systematic review of studies examining privacy concerns regarding electronic health records, Shaw et al. (2011) found that none of the studies distinguished between concerns regarding security and privacy. Information privacy in relation to PHI reflects individuals' desire to control the collection and use of their PHI. Security, on the other hand, pertains to the technical measures or structures put in place to protect digitized PHI (King et al., 2012; Shaw et al., 2011). Failure, therefore, to distinguish between security and privacy can make it difficult to understand privacy and its impact in the healthcare context.

Also, most of the existing studies did not use validated measures of privacy concerns (e.g., Smith et al., 1996) often used in the IS privacy literature. These studies often use a single item, examining privacy concerns as a unidimensional construct (e.g., King et al., 2012; Laric et al., 2009; Papoutsi et al., 2015; Vodicka et al., 2013; Wilkowska & Ziefle, 2012). For example, Chhanabhai & Holt (2007) measured concerns about health records with the item: *Are you concerned about the confidentiality and privacy of your health records?*. Papoutsi et al. (2015) also measured concerns regarding security and privacy of electronic health records with the item: *If your record was part of a national electronic records system, would you worry about the security of your records?*. The use of a single item limits our understanding of concerns regarding PHI privacy. Further, the conflation of privacy with distinct concepts such as security and confidentiality in measurement items can obscure our understanding of concerns regarding PHI privacy.

Due to the lack of proper measurement of privacy concerns in the healthcare context, it is necessary to adapt a measure from the general IS privacy literature. As noted in Section 2.2, the definition of privacy concerns by Smith et al. (1996) which emphasizes individuals' concerns regarding organizational practices related to the collection and use of their personal information is commonly used by IS researchers. Smith et al. (1996) developed the Concern for Information Privacy (CFIP) instrument as a multi-dimensional measure of privacy concerns comprising of four dimensions: *collection*, *errors*, *secondary use*, and *unauthorised access*. Malhotra et al. (2004) have also proposed the Internet Users Information Privacy Concerns (IUIPC) measure which focuses on users' concerns about their inability to control and their lack of awareness of how the personal information they disclose via the Internet is used. IUIPC consists of three dimensions: *collection*, *control*, and *awareness*. Recently, combining the CFIP and IUIPC measures, Hong and Thong (2013) have created the Internet Privacy Concerns (IPC) measure.

A recent review of the empirical IS privacy literature by Yun et al. (2019) found CFIP and IUIPC as the dominant measures of privacy concerns. Of the two measures, CFIP has been used in a larger number of studies and may be considered the de facto measure of information privacy concerns (Bélanger & Crossler, 2011; Yun et al., 2019). It is argued that CFIP represents an appropriate measure of privacy concerns for this study for the following reasons. First, consistent with the definition of PHI privacy in Section 2.1.3, this study focuses on

individuals' concerns regarding healthcare providers' collection and use of PHI. Therefore, similar to Angst and Agarwal (2009), CFIP is considered an ideal measure in this case as IUIPC is more appropriate when modelling concerns about Internet-based information privacy. Second, of the existing measures, CFIP has been used in a number of studies in the healthcare context and has been found to be a valid measure of PHI privacy concerns (e.g., Dinev et al., 2016; Esmaeilzadeh, 2018a; Li & Slee, 2014).

Based on the CFIP measure adapted for this study, PHI privacy concerns is defined as *individuals' concerns regarding healthcare providers' practices related to the collection and use of their PHI*. The dimensions of CFIP adapted to the context of this study are defined as follows: (i) *collection* pertains to individuals' concerns that a great deal of their PHI is being collected and stored by healthcare providers; (ii) *secondary use* reflects individuals' concerns that their PHI collected for one purpose, are used for other secondary purposes without their authorisation; (ii) *errors* relates to individuals' concerns that healthcare providers do not put adequate measures in place to prevent and correct errors in PHI; (iv) *unauthorised access* pertains to concerns that healthcare providers fail to prevent unauthorised access to PHI stored in their computer systems (Smith, et al., 2011).

Table 2.1 compares the existing studies based on their use of the CFIP instrument in measuring privacy concerns in the healthcare context. As evident, only a handful of studies have used the CFIP instrument in assessing privacy concerns regarding health information. This study thus contributes to the existing research by examining PHI privacy concerns as a multi-dimensional construct based on the CFIP in the understudied context of developing countries.

2.3.2 Antecedents to PHI Privacy Concerns

In recent years, as a result of the increasing concerns about PHI privacy, the factors influencing these concerns have been explored in a number of studies. According to Smith et al. (2011), the influential antecedents of privacy concerns will be largely determined by the specific IS context. Kenny and Connolly (2015, 2016) drawing on the systematic reviews of the IS privacy literature by Li (2011) and Smith et al. (2011) classified antecedents to PHI privacy concerns into *individual characteristics*, *individual experiences*, and *individual perceptions*. The important antecedents under each category examined to date are briefly discussed below.

2.3.2.1 Individual Characteristics

Individual characteristics have been the often-studied antecedents to PHI privacy concerns. The characteristics usually studied include gender, age, education, and health status. Tables A1 to A4 in Appendix A summarize research related to these individual characteristics.

Table 2.1 Comparing Previous Studies Based on the CFIP Instrument

Dimensions of Concern for Information Privacy (CFIP)	Flynn et al. (2003)	Chhanabhai & Holt (2007)	Angst & Agarwal (2009)	Laric et al. (2009)	Whetstone & Goldsmith (2009)	Anderson & Agarwal (2011)	Lafky and Horan (2011)	Hwang et al. (2012)	King et al. (2012)	Perera et al. (201)	Wilkowska & Ziefle (2012)	Ancker et al. (2013)	Miltgen et al. (2013)	Vodicka et al. (2013)	Ermakova et al. (2014)	Fischer et al. (2014)	Kordzadeh & Warren (2014)	Li et al. (2014)	Li & Slee (2014)	Rogith et al. (2014)	Papoutsi et al. (2015)	Bansal et al. (2010)	Dinev et al. (2016)	Kenny & Connolly (2016)*	Kordzadeh et al. (2016)	Esmaeilzadeh (2018a)	Jena (2015)
Collection	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	✓	×	×	×	✓	×	×	×	✓	✓	×	✓	×
Errors	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	✓	×	×	×	✓	×	×	×	✓	✓	×	✓	×
Secondary Use	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	✓	×	×	×	✓	×	×	×	✓	✓	×	✓	×
Unauthorised Access	×	×	✓	×	×	×	×	✓	×	×	×	×	×	×	✓	×	×	×	✓	×	×	×	✓	✓	×	✓	×

✓ CFIP dimension is used in a study, × CFIP dimension is not used

Note: *Kenny and Connolly (2016) used the IPC instrument which combines the CFIP and IUIPC instruments.

Regarding the influence of gender on PHI privacy concerns, a number of studies found no significant difference between males and females (Ancker, Silver, Miller, & Kaushal, 2013; Ermakova, Fabian, & Zarnekow, 2014; Esmaeilzadeh, 2018a). However, for studies that showed a significant difference, females consistently expressed greater PHI privacy concerns than males (Kordzadeh & Warren, 2014; Laric et al., 2009; Perera, Holbrook, Thabane, Foster, & Willison, 2011; Vodicka et al., 2013; Wilkowska & Ziefle, 2012). The majority of studies in other IS domains (e.g., the Internet and OSNs) similarly show that females have higher privacy concerns (Hoy & Milne, 2010; Joinson, Reips, Buchanan, & Schofield, 2010). Some studies show that males engage in online privacy-protective behaviours such as falsifying disclosed information and using privacy-preserving technology solutions (Chen & Rea, 2004; Joinson et al., 2010). It is likely that males believe these behaviours protect their privacy and hence the low privacy concerns (Kenny, 2016).

Age seems to exert a relatively consistent influence on PHI privacy concerns. With the exception of a few studies in which insignificant effect was observed (Ermakova et al., 2014; Kordzadeh & Warren, 2014), majority of studies show that older individuals have higher concerns about PHI privacy than younger individuals (Ancker et al., 2013; Esmaeilzadeh, 2018a; Laric et al., 2009; Wilkowska & Ziefle, 2012). Several suggestions have been made as to the positive relationship between age and PHI privacy concerns. According to Chen et al. (2001), young people are more risk-taking. Additionally, they have less to lose as they are young, less wealthy and have no reputation established. On the other hand, older individuals may have more ailments or conditions and therefore are more concerned about keeping their information private (Laric et al., 2009).

Empirical tests of the relationship between education and PHI privacy concerns have produced mixed results. In some studies, higher levels of education is associated with increased PHI privacy concerns (Hwang et al., 2012; Papoutsi et al., 2015), whereas in other studies there is a significant negative relationship between education and concerns (Esmaeilzadeh, 2018a; King et al., 2012; Vodicka et al., 2013).

Similar to education, the direction and nature of the influence of health status on PHI privacy concerns is uncertain. Poor health status is positively related to PHI privacy concerns in some studies (Flynn, Marcus, Kerber, & Alessi, 2003; Kordzadeh, Warren, & Seifi, 2016), whereas in other studies poor health status has a significant negative impact on concerns (Esmaeilzadeh, 2018a; Lafky & Horan, 2011; Wilkowska & Ziefle, 2012). Yet, in a number of studies health status has no significant impact on PHI privacy concerns (Kenny & Connolly, 2016; Vodicka et al., 2013).

2.3.2.2 Individual Experiences

Experience-related factors (e.g., Internet, computer, and privacy experience) have received scant attention in the healthcare context. The impact of Internet experience on privacy concerns has been examined in other IS domains (Yun et al., 2019) with mixed findings (Janda & Fair, 2004; Yao & Zhang, 2008). However, it has yet to be studied in the healthcare context. One

study found that computer experience reduces PHI privacy concerns (Perera et al., 2011). Previous privacy experience (i.e., an experience of privacy invasion in the past) has been found in studies in other IS domains to positively impact privacy concerns (Smith et al., 1996; Zviran, 2008). In the healthcare context, Bansal et al. (2010) found that past privacy breaches significantly increased PHI privacy concerns, whereas, in a study among U.S. and Irish samples, Kenny and Connolly (2016) found no significant impact of past privacy experience on PHI privacy concerns. Kenny and Connolly (2016), however, found that awareness of privacy media coverage has a significant impact on PHI privacy concerns among the U.S. samples.

2.3.3.3 Individual Perceptions

Similar to experience-related factors, a small number of other factors related to individuals' perceptions have been studied in the healthcare context (e.g., trust, risk, etc). Consistent with findings related to risk perceptions in other IS contexts (Dinev & Hart, 2006), Kenny and Connolly (2016) found that risk perceptions regarding health professionals and health technology vendors positively influence PHI privacy concerns. Regarding trust, Kenny and Connolly (2016) found that whereas trust in health technology vendors decreases PHI privacy concerns, trust in health professionals increase concerns about privacy. In other studies, trust in HIT (e.g., EHR, health clouds) have been found to decrease privacy concerns (Dinev et al., 2016; Ermakova et al., 2014). These findings largely support the observed negative relationship between trust perceptions or beliefs and privacy concerns in other IS contexts (Pavlou, Liang, & Xue, 2007). Other predictors of PHI privacy concerns include perceived sensitivity of health information (Esmaeilzadeh, 2018b; Kenny & Connolly, 2016) and privacy-preserving regulatory mechanisms (Ermakova et al., 2014).

Table 2.2 summarizes the key antecedents to PHI privacy concerns studied in past research. As evident, despite the growing concerns about PHI privacy, scant research efforts have focused on examining the antecedents to PHI privacy concerns. Moreover, only a small number of antecedents are examined together in the majority of the studies and as such, most of the antecedents have been examined only a few times. There is, therefore, limited understanding as to the relative impacts of the antecedent factors in relation to PHI privacy concerns.

To address this limitation, the study explores four main factors as antecedents to PHI privacy concerns. In contrast to the risk and trust perceptions regarding health professionals and technology vendors considered in past research (Ermakova et al., 2014; Kenny & Connolly, 2016), this study considers risk perceptions regarding electronic storage of PHI (i.e., privacy risk) and trust perceptions regarding healthcare providers (i.e., the healthcare organization). Additionally, the study explores perceptions regarding the attitude of health workers/professionals as an antecedent. Ermakova et al. (2014) found that privacy regulations decrease privacy concerns regarding cloud-based transmission of medical records. Therefore, this study also explores the influence of perceptions regarding the effectiveness of government regulation on PHI privacy concerns. The four main antecedents considered in the study are thus

privacy risk, trust in healthcare providers, perceived attitude of health workers, and perceived effectiveness of government regulation. The justification for considering these antecedents is discussed later in Section 2.4.

In addition to the four main antecedents, the individual characteristics and experience-related factors examined in prior research (i.e., age, gender, education, health status, computer experience, and privacy experience) are used as control variables to account for any variance they might explain in PHI privacy concerns. Though computer experience as an antecedent has received scant attention, it is considered in this study as, given the digital divide in developing countries (International Telecommunication Union [ITU], 2016, 2017), computer experience is likely to influence privacy perceptions and information disclosure behaviours among individuals.

Privacy orientation (i.e., the extent to which one wants to limit access to their personal information has been found to strongly increase privacy concerns in other IS contexts (Taylor, Ferguson, & Ellen, 2015; Yao, Rice, & Wallis, 2007). Given the focus on PHI privacy concerns as a core variable in the study, the influence of privacy orientation is also controlled for (Li, 2011). By considering a broad range of antecedents, the study responds to calls for more research in examining and clarifying the influence of the existing antecedents to PHI privacy concerns as well as identifying new antecedents in diverse HIT, user, and geographic contexts (e.g., Kenny & Connolly, 2015; Yun et al., 2019).

2.3.3 Trust

The preceding two sections reviewed the literature on PHI privacy concerns and the factors influencing these concerns. This section briefly reviews the targets/objects of trust considered in prior research and concludes with the conceptualization of trust in this study.

Risks and uncertainties characterize online services or transactions as a result of their faceless and intangible nature (Beldad et al., 2010; Mou, Shin, & Cohen, 2017). Trust is therefore considered as a necessary precondition for consumers' adoption of online services (Beldad et al., 2010; Gefen, 2002). In IS privacy research, trust is also considered a critical construct which has a strong influence on individuals' personal information disclosure behaviours in online environments (Anderson & Agarwal, 2011; Dinev & Hart, 2006).

Due to the strong influence of trust on behavioural outcomes, it has been studied in diverse IS contexts including the Internet (Dinev & Hart, 2006), healthcare (Anderson & Agarwal, 2011), and e-commerce (Bhattacherjee, 2002). The classic conceptualization of trust is used in most past studies; the target of trust in this case is the technology/system which facilitate the provision of online services (Anderson & Agarwal, 2011; Bansal et al., 2010; Bansal, Zahedi, & Gefen, 2016; Dinev et al., 2016; Dinev & Hart, 2006; Jena, 2015; Miltgen et al., 2013; Wirtz & Lwin, 2009).

Table 2.2 Antecedents to PHI Privacy concerns – Comparing Past Studies

Antecedents to PHI Privacy Concerns	Flynn et al. (2003)	Laric et al. (2009)	Lafky and Horan (2011)	Hwang et al. (2012)	King et al. (2012)	Perera et al. (2011)	Wilkowska & Ziefle (2012)	Ancker et al. (2013)	Vodicka et al. (2013)	Ermakova et al. (2014)	Kordzadeh & Warren (2014)	Rogith et al. (2014)	Papoutsi et al. (2015)	Bansal et al. (2010)	Dinev et al. (2016)	Kenny & Connolly (2016)	Kordzadeh et al. (2016)	Esmaeilzadeh (2018a)
Age	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×	×	✓	✓	✓
Gender	×	✓	×	✓	×	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	×	✓
Education	×	×	×	✓	✓	✓	×	×	✓	×	×	✓	✓	×	×	×	×	✓
Health Status	✓	×	✓	×	✓	×	✓	×	✓	✓	✓	×	×	×	×	✓	✓	✓
Computer Experience	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×
Privacy Experience	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	✓	×	×
Risk Perceptions	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×
Trust Perceptions	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	✓	✓	×	×
Privacy Regulation	×	×	×	×	×	×	×	×	×	✓	×	×	×	×	×	×	×	×
Perceived Sensitivity of PHI	×	✓	×	×	✓	×	×	×	×	×	×	×	×	✓	×	✓	×	✓

✓ Antecedent is explored in a study, × Antecedent is not used

A number of studies have also considered other trust targets such as healthcare providers (Klein, 2007), healthcare professionals (Kenny & Connolly, 2016) and online service providers (Mou & Cohen, 2014). Thus, as Morosan and DeFranco (2015) have noted, the existing studies either focused on trust in the technology/system facilitating transactions or on trust in the organization deploying the technology.

However, in the context of online services, the technology which facilitates the provision of the services and the entity/organization deploying the technology are considered as the proper objects of trust (Beldad et al., 2010; Morosan & DeFranco, 2015; Tan & Thoen, 2000). For instance, consumers' willingness to disclose sensitive information such as credit card information does not only depend on their assessment of the trustworthiness of sellers but also on the functionality and reliability of the e-commerce system (Grabner-Kraeuter, 2002). In the specific context of healthcare, Dinev et al. (2016) have similarly argued that trust includes both trust in the healthcare institution and trust in the HIT facilitating e-health services even though the authors considered only the latter dimension of trust in their study. Following the recommendation in these studies, this study considers both trust in healthcare providers and trust in HIT.

Trust is often defined in IS privacy research in terms of the trusting beliefs an individual (i.e., trustor) holds about the target of trust (i.e., trustee) that drive the trustor to depend on the trustee to perform a task important to the trustor (Bhattacherjee, 2002; Gefen, 2002). Two targets of trust are considered in this study: healthcare providers, and HIT. The three trusting beliefs identified by McKnight, Choudhury and Kacmar (2002) are commonly used in past studies: *benevolence*, *competence* (or ability), and *integrity*. Adapted to the context of this study, trust in healthcare providers thus reflects beliefs that healthcare providers act in the best interest of individuals (benevolence), that the providers are capable in providing services required of them (competence), and that they are honest and keep their promises (integrity) (McKnight et al., 2002).

The trusting beliefs of benevolence, competence, and integrity are most applicable when the target of trust is a person or an organization (Bhattacherjee, 2002; McKnight, 2005). In the case of trust in a technological artefact, the trusting beliefs considered in prior IS privacy research include *competence*, *reliability*, and *safety* (Dinev & Hart, 2006). The technological artefact considered in this study is HIT which supports healthcare providers in performing PHI related transactions including storing, updating, and sharing PHI. Trust in HIT therefore pertains to individuals' believe that HIT has the functionality to support the conduct of PHI-related transactions (competence), that these transactions are performed without frequent problems (reliability), and that PHI submitted via or to the HIT is kept safe (safety) (Dinev & Hart, 2006; McKnight, 2005).

In contrast to past studies that either focused on trust in technology or trust in organization, this study considers a dyadic conceptualization of trust; i.e., trust in healthcare providers and trust in HIT. It explores their relative influence on individuals' willingness to disclose PHI. As trust in HIT has been found in several studies to strongly influence individuals' PHI disclosure

behaviour (Anderson & Agarwal, 2011; Jena, 2015) and adoption of HITs (Miltgen et al., 2013), the study also explores the antecedents to trust in HIT. The antecedents considered in prior research are reviewed in the next section.

2.3.4 Antecedents to Trust in HIT

There is scant research on factors that influence individuals' trust in online services or technologies in the healthcare context (Beldad et al., 2010; Kim, 2016). In the existing limited studies, gender was found to have no significant effect on trust in a national identification system (Li et al., 2008). However, in the Internet context, women were found to express less trust in the use of the Internet for credit card purchases (Dickerson, 2003). Regarding age, older individuals expressed low trusting beliefs in the competence, benevolence, and integrity of a national identification system (Li et al., 2008). In contrast, younger individuals were found to be more trusting of health websites (Dutta-Bergman, 2003). These studies suggest a negative influence of age on trust in health-related technologies. Regarding education, Dutta-Bergman (2003) found that individuals who were more educated trusted health websites more compared to those with less education. Bansal et al. (2010) also examined the influence of health status on trust in health websites and found individuals with good health to be more trusting of health websites than those with poor health.

Dinev et al. (2016) explored individuals' perception of the effectiveness of technologies used by electronic health records and of privacy regulations as antecedents to trust in electronic health records. These two factors were found to increase trust in electronic health records. A number of antecedents to trust in a technological artefact have also been examined in other IS contexts (e.g., Internet, and e-commerce) which may influence individuals' trust in HIT. For example, Dinev and Hart (2006) found that perceived Internet risk decreases trust in the Internet. Morosan and DeFranco (2015) also found that trust in a hotel has a strong positive influence on the hotel's mobile app. In the e-commerce context, Corbitt, Thanasankit, and Yi (2003) found that more experienced Internet users have a higher level of trust in e-commerce websites. In contrast, Aiken and Boush (2006) found that the relationship between online trust and Internet experience is positive for novice and intermediate users but negative for highly experienced users. As a possible explanation for their findings, Aiken and Boush (2006) suggest online trust may decline as highly experienced Internet users accumulate knowledge about the risks of using the Internet which can increase their concerns about privacy.

In general, as noted earlier in this section, there is a paucity of IS research examining antecedents to trust in technology/system (e.g., the Internet, EHR system, websites, etc.). This is quite surprising given that in some studies trust in technology has been found to exert a stronger influence on individuals' personal information disclosure behaviour than privacy concerns (Dinev & Hart, 2006; Jena, 2015). In the specific context of healthcare, the few existing studies have largely focused on demographic factors as antecedents. To address this limitation, recent studies have called for more studies to examine antecedents to trust in HITs (Beldad et al. 2010; Kim, 2016).

This study responds to the above call by examining antecedents to trust in HIT. The limited studies in the Internet and e-commerce contexts suggest that risk perceptions regarding a particular technology, and trust in the organization deploying the technology influence trust in the technology (Dinev & Hart, 2006; Morosan & DeFranco, 2015). The study extends these antecedents to the healthcare context and thus explores risk perceptions regarding storing PHI using HIT (i.e., privacy risk) and trust in healthcare providers as antecedents to HIT. Perceived effectiveness of government regulation is another antecedent considered as privacy regulation is found to affect trust in electronic health records (Dinev et al., 2016). The study also explores the influence of perceived attitude of health workers on trust in HIT. Further justification for these four proposed antecedents is provided in Section 2.4.

In addition to the four proposed antecedents, the study also controls for the influence of the demographic factors (i.e., age, gender, education, and health status) examined in prior research (Bansal et al., 2010; Li et al., 2008). Computer experience is also considered as a control variable, instead of Internet experience which has been examined in prior research (e.g., Corbitt et al., 2003). Given the digital divide in developing countries (ITU, 2016, 2017), it is expected that computer experience may influence individuals' trust perceptions regarding computer systems including HITs. Besides, it is likely that individuals in these countries may not be more familiar with the Internet given that about 75% of the people are not using the Internet (ITU, 2016).

2.3.5 Outcomes of PHI Privacy Concerns and Trust

Privacy concerns and trust are important constructs in IS privacy research which have a strong influence on several behavioural outcomes such as personal information disclosure (Anderson & Agarwal, 2011; Dinev & Hart, 2006). The preceding sections reviewed the literature on PHI privacy concerns and trust, and their antecedents. This section continues the literature review with a focus on the consequences of PHI privacy concerns and trust.

A number of outcomes have been studied as consequences of consumers' PHI privacy concerns, trust, and other factors (e.g., risk and benefits of PHI disclosure). These include intention to adopt/use HITs and willingness to disclose or share PHI. Though the outcome of focus in this study is willingness to disclose PHI, to ensure an extensive review of the extant literature, the review in this section also includes studies examining attitudes toward and/or adoption of HITs where such studies used constructs often studied in IS privacy research. The findings of the studies reviewed in this section are summarized in Appendix B.

Regarding intention to use or attitude toward HITs, a large number of studies have examined renowned technology acceptance variables such as perceived usefulness, perceived ease of use, compatibility, and facilitating conditions as predictors (Lishan, Chiuan, Choolani, & Chuan, 2009; Maass & Varshney, 2012; Sun, Wang, Guo, & Peng, 2013). Drawing on the traditional adoption models such as technology acceptance model (TAM)(Davis, 1989), unified theory of acceptance and use of technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003), and

diffusion of innovation (DOI) (Rogers, 1995), these studies focused on usability of HITs as opposed to their privacy implications.

Building on the HIT adoption studies focused on usability, some studies combined constructs from the technology adoption research with those from the IS privacy literature to assess their relative impacts on user acceptance of HITs. In one of these studies, Klein (2007) found that trust in both healthcare providers and website vendors had a stronger impact on patients' acceptance of Internet-based patient-physician communication application than perceived usefulness. Perceived ease of use was insignificant. Miltgen et al. (2013) similarly found trust in technology and perceived risk as more important in explaining individuals' acceptance of biometric identification systems than technology adoption constructs such as compatibility, perceived usefulness, and facilitating conditions. Further, privacy concerns is a stronger predictor of intention to opt in to an EHR system than perceived usefulness (Li & Slee, 2014). The findings in these studies show that the privacy-related constructs are important predictors of HIT adoption than the frequently studied constructs in the technology acceptance literature.

Studies focusing only on the constructs from the IS privacy literature have confirmed the significance of these constructs in predicting HIT adoption. For instance, Mou and Cohen (2014) found trust in an online health service provider, perceived risk barriers, perceived benefit and health belief variables (i.e., perceived susceptibility and perceived severity) as significant predictors of intention to use online health service. Trust in the online health service provider had the strongest effect on usage intention. Regarding healthcare wearable devices, Li, Wu, Gao, and Shi (2016) found perceived privacy risk and perceived benefit as significant predictors of adoption intention. Dinev et al. (2016) also found that perceived benefits, convenience, and privacy concerns significantly predict attitude toward EHR. Trust in EHR had an indirect effect on attitude toward EHR via privacy concerns. In another study examining attitudes toward EHR, drawing on the elaboration likelihood model, Angst and Agarwal (2009) found privacy concerns, argument framing and issue involvement as significant predictors both as main effects and as interactions with each other. The authors found that in the presence of high privacy concerns, attitudes of individuals can be positively altered with messages that endorse the use of EHRs.

A significant number of studies have examined the determinants of individuals' willingness to share or disclose PHI for various outcomes. A few of these studies have focused on individuals' information disclosure behaviour in online health communities (OHCs). In one study, Kordzadeh and Warren (2014) found among U.S. students that PHI privacy concerns is negatively related to the likelihood of joining OHCs. In another study, Kordzadeh and Warren (2017) found that privacy concerns, expected personal benefits, and community-related outcomes significantly influence individuals' willingness to communicate PHI in virtual health communities. Zhou (2018) also found among a Chinese online cancer community that perceived usefulness, financial risk, and privacy risk predict PHI disclosure behaviour in OHCs. Emotional support had no direct impact on PHI disclosure. However, in a more severe disease situation, the study found that people risk financial loss and disclose PHI to seek emotional support. Focusing on health information exchanges, Esmaeilzadeh (2018a) found

that perceived poor health status significantly reduces the negative effect of privacy concerns on opt-in intention toward health information exchanges. In another study, perceived benefits and perceived risk significantly predicted opt-in intention toward health information exchanges with the effect of these constructs mediated by perceived value (Esmaeilzadeh, 2018b).

Other studies have examined consumers' willingness to disclose PHI in various digitized healthcare environments. In a study among college students in the U.S., Bansal et al. (2010) found that trust in a health website, PHI privacy concerns, and prior positive experience with a website significantly predict individuals' intention to disclose health information online. Ermakova et al. (2014) also found among German and Switzerland respondents that perceived benefits and privacy concerns have a significant effect on individuals' willingness to allow sharing of their medical records in cloud computing environments. Similarly, Thiebes et al. (2017) found personal benefits (e.g., identifying predisposition to diseases) and altruistic factors such as contribution to scientific and medical research as motivators for individuals' willingness to donate their genomic data to human genomic research. However, the study found privacy concerns, especially regarding secondary use (e.g., unethical use and governmental abuse), as discouraging genomic data donation. Jena (2015) also found value for personalization and trust in the electronic medium as significant predictors of individuals' willingness to share PHI in a digitized format. Privacy concerns had no direct effect on willingness to share PHI; however, its interaction with value for personalization was significant.

Much of the extant research examined the direct effects of the predictors of PHI disclosure intentions. Extending these works, Anderson and Agarwal (2011) examined the combined moderating effects of type of PHI, the purpose of PHI request, and the stakeholder requesting PHI on the influence of privacy concerns and trust in the electronic medium on willingness to provide access to PHI. The study found both privacy concerns and trust in the electronic medium as significant predictors of willingness to provide access to PHI; these relationships are significantly moderated by the purpose of PHI request (marketing, research, patient care) and the stakeholder requesting PHI (hospital, government, pharmaceutical companies). However, no significant support was found for the moderating effect of type of PHI (general health, mental health, genetic information) which suggests consumers may consider these types of health information as equally sensitive.

Similarly, extending extant IS privacy research based on rational cognitive models, a few recent studies have examined the role of emotion on a number of outcomes. Drawing on the risk-as-feelings perspective, Anderson and Agarwal (2011) found that individuals who feel sad, angry, and anxious about their health are more willing to provide access to their PHI. Rahman (2017) also found health status emotion significantly predict individuals' intention to use a patient portal. These scant research efforts contribute to the emerging IS privacy research stream based on behavioural economics and psychology (Acquisti, 2004; Dinev et al., 2015; Tsai, Egelman, Cranor, & Acquisti, 2011) that advocate for consideration of factors (e.g., affect, biases, heuristics, etc.) that can introduce irrationality in the privacy disclosure decision.

In summary, consistent with the general IS privacy research, privacy research in the healthcare context has been largely cognitive and consequentialist, and the privacy calculus remains the foundational theory in a good number of the studies (Appendix B). The extant studies show that the often-studied constructs in the privacy calculus in other IS contexts (i.e., risk, concerns, trust, and benefits) are also important determinants of individuals' PHI privacy disclosure decisions. Additionally, these constructs are more important in explaining users' acceptance of HITs than the prominent constructs in technology adoption research. Security and privacy of health information are said to be of greatest concern to consumers regarding HITs (Kaelber, Jha, Johnston, Middleton, & Bates, 2008). This may explain the prominence of privacy-related factors in predicting adoption of HITs.

The following two limitations could be identified in the existing literature. First, the risk factor considered in prior studies largely focuses on individuals' perceptions of the likelihood of losing privacy of disclosed PHI. However, the negative consequences that may result from the loss of PHI privacy have yet to be considered in privacy empirical models. This has led to recent calls for the study of diversity of negative consequences or privacy harms in IS privacy research (Karwatzki et al., 2017; Kokolakis, 2015). This study responds to these calls by exploring the influence of potential negative consequences that individuals perceive may arise from PHI privacy loss on their PHI disclosure behaviours.

Second, several scholars have recommended two important targets or objects of trust in the context of online transactions: trust in the technology facilitating the transactions and trust in the organization deploying the technology (Beldad et al., 2010; Dinev et al., 2016; Tan & Thoen, 2000). However, the existing IS privacy studies either focus on trust in technology or trust in organization and hence fail to adequately represent the context of online transactions (Morosan & DeFranco, 2015). Addressing this limitation, this study considers both trust in healthcare providers and trust in HIT; it explores the relationship between them as well as their relative influence on individuals' willingness to disclose PHI. Thus, the study extends the privacy calculus model to include negative consequences associated with PHI disclosure and a dyadic conceptualization of trust; i.e., trust in healthcare providers and trust in technology.

2.4 Gaps in Prior Research

The literature review in the preceding sections identified a number of gaps in the existing literature. This section reiterates these gaps across four sections: measuring PHI privacy concerns, antecedents to PHI privacy concerns and trust in HIT, antecedents to willingness to disclose PHI, and research context.

2.4.1 Measuring PHI Privacy Concerns

The review in Section 2.3.1 shows that many studies use one-dimensional measures to measure privacy concerns in the healthcare context (e.g., Chhanabhai & Holt, 2007; Papoutsi et al., 2015). This limits our understanding of individuals' PHI privacy concerns. In response, this

study uses the CFIP instrument (Smith et al., 1996) and measures PHI privacy concerns as a multi-dimensional construct comprising of four dimensions: collection, errors, secondary use, and unauthorised access. Some of the few studies that have adopted CFIP either focused on the consequences of PHI privacy concerns (e.g., Angst & Agarwal, 2009; Li & Slee, 2014) or explored a small number of antecedents (e.g., Dinev et al., 2016; Hwang et al., 2012). This study seeks to offer a more comprehensive assessment of PHI privacy concerns and its antecedents and consequence factors.

2.4.2 Antecedents: PHI Privacy Concerns & Trust in HIT

There is limited research focused on the factors that influence PHI privacy concerns (Kenny, 2016; Yun et al., 2019) and trust in HIT (Beldad et al., 2010; Kim, 2016). This study explores four lesser studied factors in prior research as antecedents to both PHI privacy concerns and trust in HIT, namely trust in healthcare providers, perceived effectiveness of government regulation, perceived attitude of health workers, and privacy risk. The justification for these factors, especially given the geographic context of this study, is described below.

Trust in Healthcare Providers

Trust in healthcare providers has yet to be examined as an antecedent to both PHI privacy concerns and trust in HIT. Westin (2000) found from several public opinion polls that distrust in institutions is a major factor driving individuals' privacy concerns. On the other hand, the trustworthiness of an organization is seen as an important factor that can impact trust in an organization's e-services; individuals may rely on familiarity or experience with the organization in forming trust in the online services provided by the organization (Beldad et al., 2010). As HITs have only recently been introduced in many developing countries, it is likely that individuals' trust in healthcare providers will impact their trust and privacy beliefs regarding the HITs used by the providers.

Perceived Effectiveness of Government Regulation

Consumers often desire consent and seek assurance of privacy and security regarding the collection and use of their PHI (Willison et al., 2007; Willison et al., 2009). One way of empowering consumers with the right to consent and protect the privacy of their personal information is through regulations (Hodge Jr et al., 1999). However, despite the importance of privacy regulations, research examining their impact on individuals' privacy beliefs and behavioural choices has been sparse (Miltgen & Smith, 2015; Yun et al., 2019).

The sensitive nature of health information has necessitated the formulation of stringent legislation, e.g., HIPAA (Health Insurance Portability and Accountability Act of 1996), for its protection in most developed countries. However, the influence of privacy regulations has been examined in a few studies. Dinev et al. (2016) found a direct positive effect of perceived effectiveness of regulatory mechanisms on trust in EHR, whereas Ermakova et al. (2014) found

that trust in privacy-preserving regulations reduces privacy concerns regarding cloud-based transmission of medical records. Building on these studies, this study examines the influence of perceived effectiveness of government regulation on both trust in HIT and PHI privacy concerns. In addition, the study explores the mechanism of these relationships through a mediator variable, trust in healthcare providers.

Compared to the developed world, in most developing countries, stringent regulations often do not exist to protect the privacy of consumers' health information as they migrate to digitized healthcare systems (PEN, 2010). As Willyard (2010) observed, only a few countries have passed laws to ensure that patient information remains confidential. Even where some regulations exist, healthcare providers are found not to comply with them. For instance, studies show that in some African countries (e.g., Ghana) healthcare practitioners are highly paternalistic and consumers are subjected to various forms of abuses including unauthorised disclosure of their sensitive information (Dapaah & Senah, 2016). It is thus important that individuals' perceptions of the effectiveness of government regulations are studied in empirical models examining PHI privacy disclosure behaviours.

Perceived Attitude of Health Workers

In the healthcare service literature, individuals' perceptions of the attitude of health workers reflect their (individuals) perception of the quality of interpersonal treatment received from health workers throughout the process of accessing healthcare services (Sumaedi et al., 2016). In effect, it is the interactional justice (Bies & Moag, 1986) that an individual perceives to have received from health workers.

Literature on customer service shows that consumers place much importance on the interpersonal treatment received in a transactional exchange (Clemmer & Schneider, 1996) and perceptions of fair interpersonal treatment is found to be a strong predictor of trust in organizations and of service satisfaction (Chiu, Lin, Sun, & Hsu, 2009; Schneider & Bowen, 1995). An essential component of healthcare service delivery is the interpersonal interaction that takes place between patients and health professionals. This interpersonal interaction is a critical factor in consumers' evaluation of healthcare service quality (Sumaedi et al., 2016). Similar to the findings in the customer service context (Chiu et al., 2009), it is likely that individuals' beliefs about healthcare institutions and their willingness to entrust them with their PHI will be shaped by the quality of interpersonal treatment received in the process of receiving care.

The importance of interpersonal treatment is strongly emphasized in some of the ethical guides for health workers. For instance, in the modern version of the Hippocratic Oath by Louis Lasagna (Hajar, 2017), demonstration of warmth, sympathy, and understanding are seen as important factors that "may outweigh the surgeon's knife or the chemist's drug" in administering care to patients. However, in Africa, abuse of patient rights and poor interpersonal relationship with patients have been reported in several studies (Andersen, 2004; Badu, Opoku, & Appiah, 2016; Kwansa, 2013; Maya et al., 2018). Mistreatments experienced

by patients range from verbal abuse (e.g., shouting, insults, derogatory remarks), abandonment, to physical abuse such as pinching and slapping (Maya et al., 2018). Some studies report that poor interpersonal treatment serves as a barrier to patients' adherence to treatment (Ibrahim et al., 2014) and prevents pregnant women from seeking facility-based childbirth (Maya et al., 2018; Moyer, Adongo, Aborigo, Hodgson, & Engmann, 2014). Health workers' breach of confidentiality of sensitive PHI such as HIV status also prevents HIV patients from going for treatment (Dapaah & Senah, 2016). The above empirical studies justify the need to examine the impact of perceptions of the attitude of health workers on individuals' trust and privacy beliefs in the context of developing countries.

Privacy Risk

As the review in Sections 2.3.2 and 2.3.4 indicates, the influence of privacy risk perceptions on PHI privacy concerns and on trust in HIT has received scant attention. This is surprising given the highly sensitive nature of PHI and the fact that individuals are said to perceive greater risks for disclosing more sensitive information (Dinev et al., 2013). In the Internet context, Dinev and Hart (2006) found that perceived Internet risk decrease trust in the Internet and increase Internet privacy concerns. Xu, Dinev, Smith, and Hart (2008) also found that privacy risk perceptions regarding websites significantly increase privacy concerns related to websites in the healthcare, e-commerce, finance, and social networking contexts. These studies suggest the need to study the influence of risk perceptions regarding the use of HIT to store PHI on both PHI privacy concerns and trust in HIT.

2.4.3 Antecedents to Willingness to Disclose PHI

Prior information privacy research in the healthcare context has improved our understanding of the salient factors (e.g., trust, concerns, risks, and benefits) that influence various behavioural outcomes such as intention to disclose PHI or adopt/use HITs. The existing research, however, has failed to consider a dyadic conceptualization of trust and specific negative consequences associated with PHI disclosure in empirical models examining individuals' PHI disclosure behaviours. These gaps also pertain to IS privacy research in general. The justification for their study is described next.

Dyadic Conceptualization of Trust

Prior research fails to adequately capture the context of online transactions regarding trust as the studies either focused on the technology which facilitates online transactions (e.g., Miltgen et al., 2013) or the organization deploying the technology (e.g., Klein, 2007). This limits our understanding of the individual effects of the two targets of trust on various behaviours and the relationship between them. Therefore, following calls to study both organizational trust and technology trust (Beldad et al., 2010; Tan & Thoen, 2000), this study examines the relative influence of trust in healthcare providers and trust in HIT on willingness to disclose PHI.

Negative Consequences of PHI disclosure

Privacy risk has been identified in prior privacy studies as one of the major deterrents of personal information disclosure by consumers. An individual's risk calculation is said to involve an evaluation of the adverse consequences or negative outcomes of a situation, and the likelihood of their occurrence (Dowling, 1986; Mitchell, 1999; Peter & Tarpey, 1975). As briefly discussed in Section 2.2, the dominant conceptualization of risk in the IS privacy literature focuses on the likelihood of loss associated with personal information disclosure (Dinev et al., 2013; Featherman & Pavlou, 2003; Malhotra et al., 2004; Smith et al., 2011). The negative consequence or loss considered in the existing literature is the loss of control over one's personal information (Dinev & Hart, 2006; Xu et al., 2009). However, as noted by Karwatzki, Trenz, Tuunainen, and Veit (2017), specific negative consequences (e.g., job or relationship loss) that individuals may perceive to result from privacy loss are not considered. Whilst some specific adverse consequences (e.g., social, material, and physical) have been identified in prior research (Karwatzki et al., 2017; Smith et al., 2011), their impact in relation to personal information disclosure in online environments has yet to be examined.

In a recent review, Kokolakis (2015) recommended the study of diversity of privacy harms in IS privacy empirical models. Considering the negative consequences of PHI disclosure is especially important in developing countries given the heavy stigmatization of a number of health conditions in these countries. A major reason for the stigma around certain diseases is that religion and morals play important roles in the social lives of the people (PEN, 2010). Consequently, exposure of information that indicates a person's deviation from accepted social and religious morals can have serious ramifications for the person including death (PEN, 2010). HIV/AIDS, for instance, is perceived as resulting from norm-violating behaviour such as commercial sex work and homosexuality (Dapaah & Senah, 2016; Duffy, 2005). Consequently, some HIV patients hide their infections and avoid needed care for fear of the negative consequences (e.g., job/relationships loss, etc.) that can result from the disclosure of their infection (Dapaah & Senah, 2016; Kwansa, 2013). Therefore, as developing countries migrate to e-health systems in which the risk of privacy loss is significant, it is important to examine the impact that the potential negative consequences individuals perceive may arise from PHI privacy loss has on individuals' willingness to disclose PHI to healthcare providers where the information is digitized.

2.4.4 Research Context

The literature reviewed in this study (Appendices A & B) confirms observation in prior studies that extant IS privacy research has focused mainly on samples in developed countries, especially the U.S. (Bélanger & Crossler, 2011; Hong & Thong, 2013). Due to the exclusive focus on developed countries, Bélanger and Crossler (2011) argued that the findings of extant research may be of limited generalizability. One reason cited by the authors is the differences in values, cultures, and laws across countries which may cause differences in individuals' privacy perceptions and its impacts. Religion and morals play important roles in the cultures of many developing countries (PEN, 2010). Therefore, compared to their counterparts in

developed countries, individuals in developing countries may be more concerned about the disclosure of certain PHI, especially PHI that violates accepted social and religious morals.

Aside from the focus on developed countries, the reviewed studies (Appendices A & B) also show that prior healthcare privacy studies have often used tech-savvy user samples that have experience in online environments as most of the studies were conducted online. This is consistent with Kokolakis' (2015) finding that most IS privacy studies used online surveys. A recent study by Pew Research Center [PRC] (2015) shows that fewer people have access to the Internet in developing countries, especially Africa, compared to developed countries. For example, about 75% of people in Africa are not using the Internet compared to 21% in Europe (ITU, 2016). Also, the gender digital gap is wider in Africa compared to other regions in the world (ITU, 2017). A lower proportion of women than men are using the Internet (25% lower). In contrast, in the Americas, a higher percentage of women than men are using the Internet (ITU, 2017). Given the digital divide and gender digital gap in developing countries, it is likely that privacy concerns and privacy disclosure behaviours of individuals in these countries may differ from their counterparts in developed countries who have greater digital experience. This study, therefore, extends the boundaries of existing IS privacy research to examine privacy perceptions and PHI disclosure behaviours of individuals in a developing country.

2.5 Chapter Summary

This chapter reviewed the existing IS privacy research in general and research specifically related to the healthcare context. Consistent with the observation in Yun et al. (2019), the healthcare context is an understudied area and much of the privacy research has been conducted only in recent years. Consequently, the review has identified important gaps in the literature that need to be addressed. These gaps include the limited understanding regarding antecedents to PHI privacy concerns and trust in HIT, as well as the lack of consideration of negative consequences associated with PHI disclosure, and dyadic conceptualization of trust in empirical models examining PHI disclosure behaviours. There is also an inadequate measurement of PHI privacy concerns in the existing studies. This study aims to address these gaps in the understudied context of a developing country. The next chapter discusses the approach for addressing these gaps.

CHAPTER THREE: THEORETICAL FOUNDATION AND PROPOSED RESEARCH MODEL

This study adopts the privacy calculus perspective as the overarching theoretical framework in examining willingness to disclose PHI among individuals in developing countries. It extends the privacy calculus by integrating it with the procedural and interactional dimensions of justice theory to explore antecedents to PHI privacy concerns and trust. This chapter first discusses the theories underpinning this thesis. Next, the proposed research model based on these theories, which addresses the gaps in prior research discussed in the previous chapter, is presented including a discussion of the hypotheses presented in the study.

3.1 The Privacy Calculus Theory

The privacy calculus theory is a major perspective employed by the stream of IS privacy research devoted to explaining the problem of the privacy paradox (Culnan & Armstrong, 1999). This paradox suggests that despite consumers' high levels of concerns about privacy their behaviours do not mirror these concerns in that they still disclose much of their sensitive information. According to the calculus perspective, privacy disclosure decision results from a cost-benefit analysis in which the risk and cost of personal information disclosure are weighed against the benefits to be gained from disclosure (Culnan & Bies, 2003). When the perceived overall benefits of disclosure match or exceed the anticipated negative consequences of disclosure (i.e., risks), individuals disclose personal information for outcomes perceived to worth the risk of information disclosure (Culnan & Bies, 2003; Dinev & Hart, 2006).

The concept of the privacy calculus was first considered in the seminal work of Laufer and Wolfe (1977). According to the authors, a *calculus of behaviour* (i.e., a conscious process involving an evaluation of costs and benefits) impacts an individual's decision whether to disclose personal information. Following Laufer and Wolfe (1977), IS researchers (e.g., Dinev & Hart, 2006) have developed and tested empirical models based on the privacy calculus often drawing on two of the primary components of the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980) and the theory of planned behaviour (TBP)(Ajzen, 1988); these components are beliefs and behavioural intention. Thus, these researchers have focused on individual beliefs or perceptions that influence their behavioural intention to disclose personal information for certain outcomes that are of interest or benefit to them.

Prior studies have modelled benefits in the privacy calculus as factors that drive individuals' intentions to disclose personal information, whereas costs and risks have been modelled as factors which discourage or inhibit privacy disclosure by individuals (e.g., Anderson & Agarwal, 2011; Dinev & Hart, 2006). A key benefit factor commonly considered in the existing research is the benefits individuals expect to gain from disclosing their personal information in order to use a particular electronic service or system, often in transacting with others. Personalized services (Xu et al., 2009) and relationship building (Krasnova et al., 2010) are examples of benefits which individuals desire in return for personal information disclosure.

Trust is also an important factor in IS privacy research, which has been found to strongly motivate personal information disclosure (Bélanger & Crossler, 2011). Consequently, some studies have modelled trust as representing the benefit side of the calculus equation (e.g., Anderson & Agarwal, 2011), whereas others have examined trust in addition to the benefits individuals expect from privacy disclosure (e.g., Dinev et al., 2006). In terms of the cost factors in the privacy calculus, privacy concerns and privacy risk have been frequently examined in the existing literature (e.g., Dinev et al., 2006; Xu et al., 2009).

Factors that drive or motivate individuals' privacy disclosure intentions (e.g., benefits, trust) and those that inhibit their disclosure intentions (e.g., privacy risk, privacy concerns) are respectively referred to as *drivers* and *inhibitors* (Dinev et al., 2016). Thus, unlike most empirical models that test the relative strength of non-contrary factors on behavioural intention, the privacy calculus consists of an examination of the cumulative influence of contrary beliefs (i.e., drivers and inhibitors) on information disclosure (Dinev & Hart, 2006).

Several empirical studies support the influence of a set of contrary beliefs on information disclosure intentions. Dinev and Hart (2006) examined the simultaneous effect of risk beliefs (including internet privacy risk and internet privacy concerns), and confidence and enticement beliefs (comprising internet trust and personal internet interest) associated with the intention to disclose personal information to transact on the Internet. Consistent with the calculus perspective, the study found the risk beliefs as discouraging information disclosure whilst the confidence and enticement beliefs served as drivers of the intention to disclose information. Other studies conducted in diverse IS domains including healthcare (Anderson & Agarwal, 2011) and location-based services (Xu et al., 2009) have similarly demonstrated the impact of contrary beliefs on consumers' privacy disclosure decision making.

A number of studies also indicate that attitude formation is similarly influenced by a set of contrary beliefs. For example, Dinev, Hu, and Yayla (2008) found that confidence and enticement beliefs (e.g., perceived benefits, trust in such engines) and risk belief (e.g., perceived risk) influence attitude toward online advertising. Similarly, Dinev et al. (2016) found perceived benefits of EHR and convenience as positively influencing attitude toward EHR whilst privacy concerns was a negative influence. In general, prior studies have confirmed the need to account for the relative influence of opposing factors in attempting to understand consumers' attitudes and intention regarding privacy disclosure.

The privacy calculus theory was chosen as the core theoretical framework as this study seeks to explore both the drivers and inhibitors of individuals' willingness to disclose PHI in a digitized healthcare environment. Also, the calculus perspective of privacy is considered "the most useful framework for analysing contemporary consumer privacy concerns" (Culnan & Bies, 2003). Moreover, the privacy calculus has been rigorously tested and empirically validated in numerous studies in investigating simultaneous impacts of contradictory factors on information disclosure in various IS domains (e.g., Dinev & Hart, 2006). Further, given that prior IS privacy research based on the privacy calculus has been conducted mostly in developed countries (Bélanger & Crossler, 2011; Hong & Thong, 2013), using the privacy calculus model

will help evaluate its applicability to explaining privacy disclosure behaviour in a developing country's context.

3.2 The Justice Theory

The notion of justice (also known as fairness) reflects individuals' perceptions of fairness in relation to outcomes and the means (i.e., procedures/processes) by which the outcomes are obtained in a transactional exchange relationship (Cropanzano & Greenberg, 1997). The extent to which an individual believes he has been treated fairly by a transacting party over the course of the exchange relationship has an impact on how the individual interacts with the transacting party (Son & Kim, 2008). The justice perspective has been well studied in a variety of domains including sociology, psychology, ethics, and economics (Ashworth & Free, 2006). It has been widely applied in explaining various phenomena, including employees' retaliation against their organizations (Skarlicki & Folger, 1997), their reactions to pay raise decisions (Folger & Konovsky, 1989), and customer satisfaction (Martínez-Tur, Peiró, Ramos, & Moliner, 2006). For example, customers' perception of fairness regarding procedures and outcomes associated with the purchase of products and services have a significant impact on customer satisfaction (Martínez-Tur et al., 2006).

In recent years, justice theory has been used as a framework for analysing consumer privacy concerns (e.g., Culnan & Bies, 2003; Xu et al., 2009; Culnan & Armstrong, 1999). This stream of research argues that a critical component of consumers' privacy concerns is their fairness judgements (Ashworth & Free, 2006). In general, consumers are concerned about the online collection and use of their personal information by firms because they perceive them to be unfair (Ashworth & Free, 2006). However, when consumers perceived that companies would deal fairly with their personal information, they are more willing to disclose their personal information (Culnan & Armstrong, 1999).

Several dimensions of justice have been studied in the literature. However, in examining consumer privacy, three types of justice perceptions are relevant, namely *distributive*, *procedural*, and *interactional* (Culnan & Bies, 2003). According to Culnan and Bies (2003), violation of any of the three justice factors may arouse consumers' concerns about privacy. These justice dimensions are briefly explained below.

3.2.1 Distributive Justice

Distributive justice refers to the perceived fairness of the outcomes an individual receives (Culnan & Bies, 2003). In the information privacy context, it reflects one's assessment of the fairness of outcomes received in exchange for disclosing personal information (Xu et al., 2009). In evaluating fairness of outcomes, there is a cost-benefit analysis as individuals assess whether the personal information they disclose is commensurate with the outcome received in return (Culnan & Bies, 2003). The key premise underlying distributive justice as it relates to

information privacy is thus quite similar to the cost-benefit analysis of the privacy calculus that underpins this study.

3.2.2 Procedural Justice

In a transactional exchange relationship, aside from outcomes, the parties also evaluate justice received based on the procedures used in attaining the outcome (Martínez-Tur et al., 2006; Thibaut & Walker, 1975). Procedural justice refers to the fairness of the procedures used to arrive at outcomes (Thibaut & Walker, 1975).

According to some researchers, if outcomes are considered unfair but fair procedures were employed in attaining the outcomes, consumers are less likely to be dissatisfied with the outcomes (Folger & Bies, 1989; Lind & Tyler, 1988). Others even suggest that the process by which outcomes are achieved may be more important than the actual outcomes (Folger & Greenberg, 1985). Lending support to these suggestions, the fairness of procedures (or practices) have been shown to be more important than outcomes in predicting several important variables (e.g., satisfaction) in diverse domains (Ashworth & Free, 2006). In the organizational context, Folger and Konovsky (1989) also found that procedures used in raising pay are of the same importance as the actual pay raise when it comes to employee satisfaction, and more important in engendering organizational commitment and trust in authorities (e.g., one's supervisor) (Folger & Konovsky, 1989). According to Ashworth and Free (2006), individuals place much importance on procedures because fair procedures used in attaining outcomes communicate to individuals that they are valued and respected.

In the context of information privacy, procedural justice concerns the perceived fairness of the procedures enacted for the collection and use of personal information (Xu et al., 2009). A variety of factors can shape consumers' perceptions of procedural fairness (i.e., perceptions as to whether procedures are just and fair) (Culnan & Bies, 2003; Lind & Tyler, 1988). One important factor relates to consumers' control over the use of their information (Culnan & Bies, 2003; Malhotra et al., 2004). Individuals perceive information privacy procedures of online firms as fair when they are vested with control of these procedures (Son & Kim, 2008). One way organizations offer consumers control is allowing them to consent to additional uses of their information aside from the original purpose for which the information was collected (Culnan & Bies, 2003). In addition to control, Internet users' awareness of the procedures for the handling of their information also influences their perceptions of procedural fairness (Culnan & Bies, 2003; Malhotra et al., 2004; Son & Kim, 2008). In a field experiment, Hui et al. (2007) found that Internet users who are aware of a privacy statement detailing information practices of online firms are more likely to disclose their information. In another study, Culnan (1995) found that consumers who were aware of procedures to remove their names from a direct mail list expressed lower privacy concerns than those who were not aware of these procedures.

It is evident from the above that control and awareness play an important role in shaping individuals' fairness perceptions regarding procedures for the handling of their information and in influencing their privacy concerns. It is argued in this study that procedural justice provisions through government regulation which directs the handling of PHI by healthcare providers can alleviate consumers' privacy risk perceptions by granting them control over and awareness of how their health information is used. Thus, the study draws on procedural justice to further explore the influence of individuals' perceptions regarding the effectiveness of government regulation on their privacy concerns and trust beliefs.

3.2.3 Interactional Justice

Aside from outcomes and the procedures used in attaining outcomes, individuals also evaluate the overall justice received based on the quality of interpersonal treatment (Bies & Moag, 1986; Colquitt, 2001). Interactional justice refers to a party's fairness perceptions of the interpersonal treatment received from another party in an exchange relationship (Son & Kim, 2008). The extent to which a person is treated with respect, dignity, and propriety are considered influential in shaping a party's perceptions about the fairness of interpersonal treatment received from another party (Colquitt, 2001). In a study to understand events in everyday life that people regard as unjust, Mikula, Petri, and Tanzer (1990) found that a "considerable proportion of injustice perceived by individuals did not concern distributional or procedural issues in the narrow sense but referred to the manner in which people were treated in interpersonal interactions and encounters". This attests to the importance of interactional justice in individuals' justice evaluations.

Several studies show that interactional justice has a positive impact on customer satisfaction (Chiu et al., 2009; Harris, 2003; Teo & Lim, 2001) and on trust (Aryee, Budhwar, & Chen, 2002; Chiu et al., 2009; Fang & Chiu, 2010). In the information privacy context, some have argued that aside from the methods used by organizations in the collection of consumers' information, the interpersonal treatment consumers receive can shape their reactions (Culnan & Bies, 2003). According to Bies (2001), interactional factors such as honesty in dealing with others, unwarranted disclosure of personal information can influence consumers' privacy concerns. It is argued that the extent to which individuals believe they have been treated with respect, dignity and empathy in the process of seeking care will impact their privacy concerns and trust beliefs. Interactional justice is mapped as individuals' perception of the attitude of health workers in this study.

3.4 Research Model and Hypotheses

The proposed research model based on the discussion of the privacy calculus and justice theory is provided in Figure 3.1.

The dependent variable of interest is *willingness to disclose PHI*. An individual may disclose PHI to various institutions (e.g., hospitals, the government, pharmaceutical companies) for

various purposes including patient care, medical research, and marketing services (Anderson & Agarwal, 2011). This study considers an individual's PHI disclosure to healthcare providers for the purpose of receiving care. Willingness to disclose PHI is thus defined as an individual's willingness to disclose their PHI to healthcare providers for the purpose of care where the disclosed health information is stored in an electronic format. Willingness to disclose PHI as a condition for receiving care is consistent with behavioural intention dependent variables considered in prior information privacy research (e.g., Anderson & Agarwal, 2011; Dinev & Hart, 2006; Malhotra et al., 2004).

Consistent with the privacy calculus, the research model examines the influence of a set of drivers and inhibitors on willingness to disclose PHI. Convenience and trust represent the main set of drivers considered in this study. Similar to past studies (e.g., Yoo et al., 2013; Dinev et al., 2016), convenience is considered as a key benefit or value that an individual expects to gain from the digitization of his PHI, and from the use of HIT in the performance of basic functions such as test ordering, prescription writing, etc. in the care delivery process.

Prior studies have incorporated trust in the privacy calculus as a key factor driving individuals' personal information disclosure (e.g., Anderson & Agarwal, 2011; Dinev & Hart, 2006). In line with these studies, this study considers trust as a driver of individuals' willingness to disclose PHI. The existing studies have largely focused on trust in the technology facilitating the provision of an online service (e.g., Anderson & Agarwal, 2011; Dinev et al., 2016; Dinev & Hart, 2006). However, in the context of online services, the technology facilitating the service provision and the organization deploying the technology are considered as the proper objects of trust (Beldad et al., 2010; Dinev et al., 2016; Tan & Thoen, 2000). Therefore, extending prior research, a dyadic conceptualization of trust is considered in this study; i.e., trust in healthcare providers and trust in HIT. Thus, the study explores the relative influence of the two dimensions of trust on willingness to disclose PHI. The literature on trust transfer suggests that individuals develop trust in an entity because of their trust in a related entity (Pavlou & Gefen, 2004; Sirdeshmukh, Singh, & Sabol, 2002). Drawing on this literature, the study also explores the association between the two dimensions of trust.

The core inhibitors, PHI privacy concerns and privacy risk, often studied in extant studies are included in the research model. Following Dinev and Hart (2006), privacy risk is modelled as an antecedent to PHI privacy concerns and willingness to disclose PHI. Also, following recent calls to examine the influence of risk perception on the formation of online trust (e.g., Beldad et al., 2010), privacy risk is considered as an antecedent to trust in HIT.

The conceptualization of privacy risk used in this study follows past research (e.g., Malhotra et al., 2004); i.e., individuals' expectation of potential loss of control over their PHI. In addition to this unidimensional conceptualization of risk which covers potential losses in general, this study also considers specific negative consequences that individuals may perceive to occur from PHI privacy loss and examine their influence on individuals' PHI disclosure intentions. Following Karwatzki et al. (2017), individuals' perception of the potential negative consequences that may arise from the privacy loss of PHI disclosed to receive care is referred to in this study as *perceived negative consequences of PHI disclosure*.

There can be several negative consequences associated with PHI disclosure. These negative consequences can be classified into social, economic, and emotional consequences (Kordzadeh & Warren, 2017; Laric et al., 2009; Rindfleisch, 1997). The negative consequences of a given disclosure vary depending on the sensitivity of the information to be disclosed (Laric et al., 2009; White, 2004). Several studies show that HIV/AIDS is a heavily stigmatized disease in developing countries and several adverse consequences can result from its disclosure (e.g., Kwansa, 2013; Sprague, Simon, & Sprague, 2011). Consequently, in this study, individuals' perceived negative consequences of PHI disclosure in relation to HIV/AIDS are considered. Reviewing relevant literature, the following specific negative consequences of PHI disclosure are considered: perceived inferiority (emotional) (Goss, Gilbert, & Allan, 1994), employment discrimination (economic) (Laric et al., 2009; Sprague et al., 2011), and family rejection (social) (Kwansa, 2013). The above consequences are considered as they are deemed relevant given the geographic context of this study.

Drawing on procedural justice, interactional justice, and prior research, perceived effectiveness of government regulation and perceived attitude of health workers are examined as antecedents to PHI privacy concerns and the trust dimensions considered in the study. The hypothesized relationships between the constructs in the research model are discussed below.

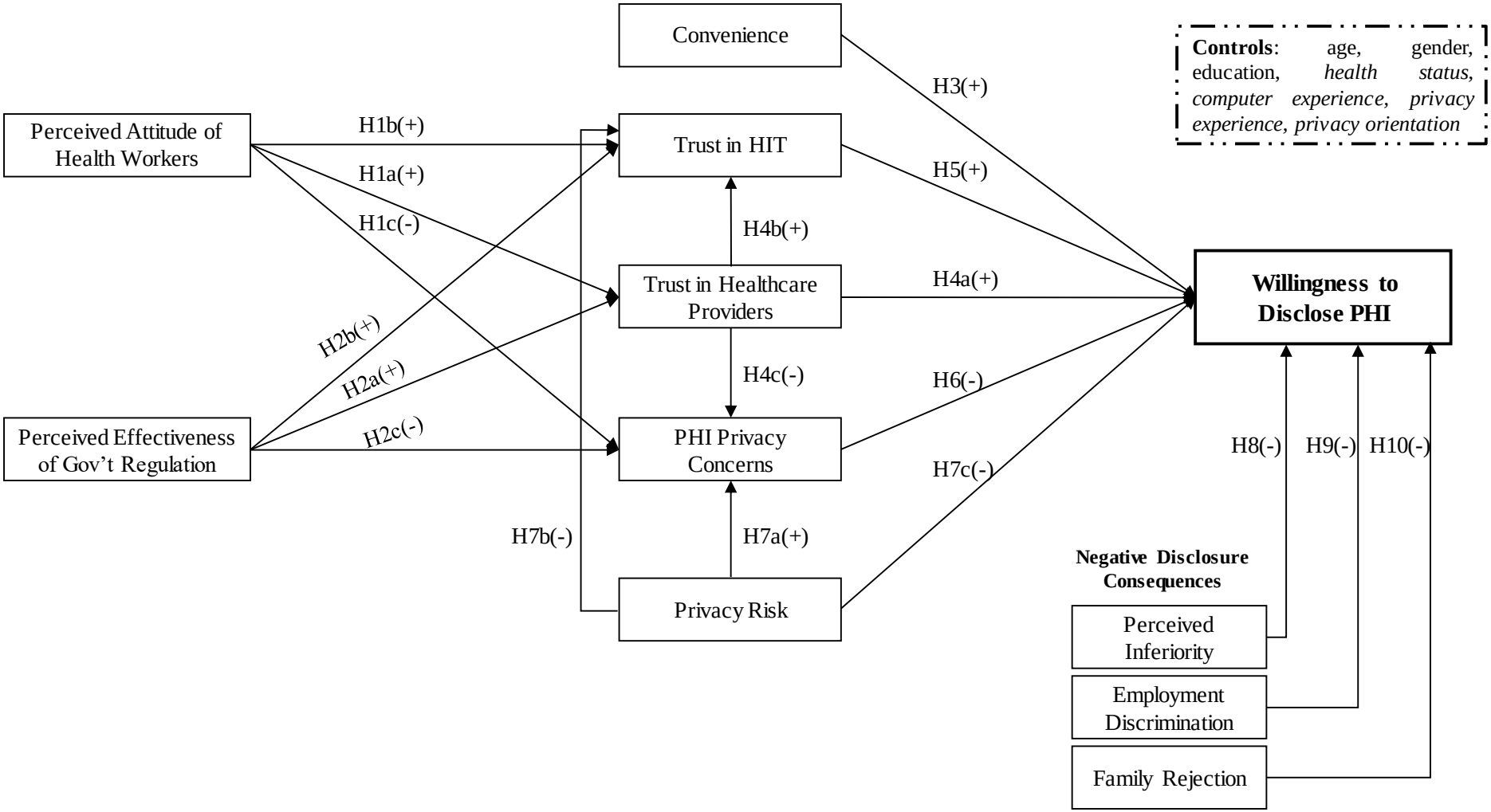


Figure 3.1: Proposed Research Model

3.4.1 Privacy Antecedents

This section discusses hypotheses related to the influence of perceived attitude of health workers and perceived effectiveness of government regulation on the core calculus constructs: PHI privacy concerns and the two trust dimensions (trust in healthcare providers and trust in HIT).

Perceived Attitude of Health workers

The employee-customer interaction during a service transaction is considered an essential component of service quality evaluation by customers in diverse contexts including tourism (Caro & García, 2008), marketing (Brady & Cronin, 2001), and healthcare (Sumaedi et al., 2016). This interaction has been referred to by labels, such as soft interaction (Sumaedi et al., 2016), conduct (Baltussen & Ye, 2005; Caro & García, 2008) or attitude (Brady & Cronin, 2001; Rakhmawati et al., 2013) of the employee(s) delivering a service. However, regardless of the context, the essential feature of this customer-employee interaction is a customer's perception of the quality of interpersonal treatment (i.e., interactional justice) received from an employee providing a service. Individuals' perception of the attitude of health workers is thus defined as the extent to which individuals believe that health workers treat them with dignity, politeness, and respect throughout the process of receiving care.

Individuals are interested in the respect conveyed by the quality of interpersonal treatment and this fosters trust in a transacting party. For instance, in the organizational context, Folger and Konovsky (1989) found that when supervisors show respect for the rights and dignity of employees through communication and high-quality interactions (e.g., allowing employees' input in decisions and considering their views), employees feel valued and respected which engender their trust in the supervisors. Perceived fairness of interpersonal treatment (i.e., being treated with respect, dignity, politeness, and friendliness) has also been found to be positively associated with trust in management (Kernan & Hanges, 2002), and trust in members in a virtual community (Fang & Chiu, 2010).

Individuals expect to be treated with respect and dignity when receiving care and hence the quality of interpersonal treatment is critical to their overall assessment of healthcare service quality (Sumaedi et al., 2016). In addition, they expect their disclosed PHI to be kept confidential (Rindfleisch, 1997; Willison et al., 2009). To assess whether the conduct of healthcare providers are consistent with their expectations, individuals compare their treatment to some normative standards of respectful behaviour (Xu et al., 2009). In the healthcare context, this may include the various ethical guides for health workers such as the modern version of the Hippocratic Oath (see Hajar, 2017) which strongly emphasize the importance of interpersonal treatment in the care delivery process and the confidentiality of patient disclosed PHI.

Given the strong relationship observed between perception of fair interpersonal treatment and trust in the existing literature, when individuals assess the interpersonal treatment received

from health workers as fair (i.e., they adhere to standards of acceptable behaviour), their trust in these workers is expected to increase. The trust transfer literature suggests a representative effect as one mechanism for the transfer of trust between entities (Belanche, Casaló, Flavián, & Schepers, 2014; Stewart, 2003). In this case, trust placed in an *entity A* likely gets assigned to an *entity B* because *entity A* is seen as a representative of *entity B* (Belanche et al., 2014). Drawing on this idea, as health workers act as representative for their healthcare providers, it is expected that individuals will generalize their trust beliefs about the health workers to the providers. Thus, if individuals trust health workers, they are likely also to trust the healthcare providers which the health workers represent. Similarly, if individuals trust health workers, they are likely to believe that the health workers and (through the process of trust transfer) the healthcare providers represented by the health workers, will protect the privacy of PHI disclosed to healthcare providers. Thus, trust beliefs about health workers are also expected to decrease individuals' concerns about PHI privacy.

The trust transfer literature also suggests that trust can transfer from well-known targets (e.g., offline firm) to less familiar or unknown targets (e.g., online service of the firm) (Stewart, 2003). Due to the lack of ability to directly interact with certain HITs such as EHR systems, it is expected that individuals will use their impressions or beliefs formed over time about health workers as a basis for their trust in the HITs which facilitate healthcare service delivery by the health workers. The following hypotheses are therefore proposed:

> ***H1a****: Perceived attitude of health workers will have a positive effect on trust in healthcare providers.*
>
> ***H1b****: Perceived attitude of health workers will have a positive effect on trust in HIT.*
>
> ***H1c****: Perceived attitude of health workers will have a negative effect on PHI privacy concerns.*

Perceived Effectiveness of Government Regulation

The reviewed literature in the previous chapter shows that consumers' primary concerns regarding the privacy of personal information stem from their lack of control over the collection and use of their personal information. According to Bandura (1982), when individuals lack the ability to exert direct control they rely on the competencies of others for control. One major way of ensuring individuals gain needed control over their personal information is through government regulation which establishes the procedures for collection, use, storage and sharing of personal information. Perceived effectiveness of government regulation is defined as the extent to which individuals believe that regulations are able to provide effective and reliable protection against privacy breaches on their PHI (Dinev et al., 2016).

Regulations meant to protect the privacy of individuals' PHI would require individuals are informed of the purpose of collection of their health information and that their consent is sought if their PHI is used for purposes other than that allowed by law. They are also expected to ensure healthcare stakeholders put safeguards in place to protect individuals' PHI from loss, misuse, or unauthorised modification. Thus, essentially, regulations ensure organizations

comply with Fair Information Practices (i.e., global standards for the ethical use of personal information (Culnan & Armstrong, 1999)) and deter non-compliance through the threat of punishment (Tittle, 1980). They also empower individuals with the ability to seek redress in case of privacy breaches on their medical data. The deterrent value of regulations may make individuals believe that healthcare providers would comply with Fair Information Practices and would, therefore, collect and use information appropriately (Xu et al., 2009). This likely will lead to higher levels of individuals' procedural justice perceptions toward healthcare providers' information practices.

Since perception of fairness of procedures used in attaining outcomes (i.e., procedural justice) is positively associated with individuals' trust in a transacting party (Chiu et al., 2009; Fang & Chiu, 2010), it is expected that if individuals perceive the information practices of healthcare providers as fair, they are likely to trust these providers and to have decreased concerns about privacy of PHI disclosed to the providers. Individuals may also believe that healthcare providers who observe fair information practices will introduce HITs that will ensure that individuals' PHI are well-managed and protected against unauthorised use and access. Individuals are thus expected to have increased trust in providers' HITs.

Dinev et al. (2016) found that perceived effectiveness of privacy-enhancing regulatory mechanisms positively influence trust in EHR systems. Miltgen and Smith (2015) also found that privacy regulation reduces privacy risk concerns and increase trust in organizations. From the above argument and empirical evidence in the literature, it is hypothesized that:

> ***H2a**: Perceived effectiveness of government regulation will have a positive effect on trust in healthcare providers.*
>
> ***H2b**: Perceived effectiveness of government regulation will have a positive effect on trust in HIT.*
>
> ***H2c**: Perceived effectiveness of government regulation will have a negative effect on PHI privacy concerns.*

3.4.2 Drivers of PHI Disclosure

Convenience

Convenience has been a subject of much research in the marketing discipline and is often defined as the perceived time and effort consumers spend in purchasing or using a service (Seiders, Voss, Godfrey, & Grewal, 2007). Convenience has a positive impact on behavioural intentions such repurchase behaviour and also moderates the influence of customer satisfaction on repurchase behaviours (Seiders et al., 2007; Seiders, Voss, Grewal, & Godfrey, 2005).

Similar to the above definition in marketing, convenience is defined in this study as individuals' perception of the time and effort that will be spent in receiving care in a digitized healthcare environment. Though e-health is nascent in developing countries, the introduction of EHR systems has helped in the collection and management of PHI (Mugo & Nzuki, 2014). In some countries (e.g., Ghana), this has helped address the problem of missing patient data and ensure

easy access to past medical records (Acquah-Swanzy, 2015; Gyamfi, 2016). This can reduce the time a patient takes to receive care, lessen documentations and repeated medical tests enabling patients to expend less effort in the process of receiving care.

An individual's perceived convenience of the healthcare service may be influenced by direct experience with digitized healthcare systems or other electronic records management systems, indirect experience of others (e.g., family, friends, etc.), or expectations from having relevant knowledge (Yoo et al., 2013). In a study among the U.S. and Italian citizens, Dinev et al. (2016) found that convenience in terms of easy access to one's medical records when needed has a significant positive impact on attitudes toward EHR. Consistent with the expectancy theory's notion that individuals act to maximise benefits (Victor, 1964), it is expected that the convenience of accessing care afforded by digitized healthcare will cause consumers to be favourably disposed toward PHI disclosure for digitization.

***H3**: Convenience will have a positive effect on willingness to disclose PHI.*

Trust

The review in Chapter 2 shows that trust is an important construct in IS privacy research and its continuous examination alongside privacy concerns has been recommended in a number of studies (e.g., Bélanger & Crossler, 2011; Pavlou, 2011). Trust refers to a set of beliefs (i.e., trusting beliefs) about the target of trust (i.e., trustee) that positively influence an individual's (i.e., trustor) intention to depend on the actions of the trustee with the expectation that the trustee will complete a task important to the trustor (Bhattacherjee, 2002; Gefen, 2002). Following several calls to account for the multi-dimensional nature of trust (Beldad et al., 2010; Tan & Thoen, 2000), this study examines the influence of trust in healthcare providers (i.e., organizations providing healthcare services), and trust in HIT (i.e, the technology used in support of healthcare service delivery by healthcare providers) on willingness to disclose PHI. Also, the influence of trust in healthcare providers on both trust in HIT and PHI privacy concerns are examined.

Trust in Healthcare Providers

Trust in healthcare providers is defined as individuals' belief in the benevolence, competence (or ability), and integrity of healthcare providers (Bhattacherjee, 2002; McKnight et al., 2002) and their willingness to depend on the actions of the providers based on their expectations that the providers will fulfil their commitments to the individuals (Gefen, 2002; Mayer, Davis, & Schoorman, 1995). Benevolence refers to the motivation of healthcare providers to act in the best interest of individuals (McKnight et al., 2002). Competence refers to individuals' belief that healthcare providers have the competency and knowledge to perform the services required of them (Bhattacherjee, 2002; McKnight et al., 2002). Integrity, on the hand, reflects individuals' belief that healthcare providers will be honest and keep their promises (McKnight et al., 2002).

Several researchers have proposed that trusting beliefs (i.e., benevolence, competence, and integrity) lead to corresponding trusting intentions, i.e., the intent to engage in behaviours or actions that demonstrate a trustor's willingness to in fact depend on the trustee (Mayer et al., 1995; McKnight, Cummings, & Chervany, 1998). In the context of e-commerce, trusting intention reflects individuals' willingness to engage in transactions with the trustee organizations (i.e., online vendors/firms) (Bhattacherjee, 2002; Jarvenpaa, Tractinsky, & Vitale, 2000). In the marketing and IS contexts, trusting intentions include willingness to provide information to firms (Schoenbachler & Gordon, 2002) or intention to use IT innovations (Morosan & DeFranco, 2015; Mou et al., 2017).

Several studies support the relationship between trusting beliefs and trusting intention. For example, in the e-commerce context, Bhattacherjee (2002) found that trust in an online firm has a significant positive impact on consumers' willingness to transact online with that firm. Customers' trust in a firm also reduces their concerns about privacy and increases their willingness to provide personal information to the firm (Schoenbachler & Gordon, 2002). Similarly, trust in the e-service provider positively impacts individuals' intention to use online health services for health information (Mou et al., 2017).

When consumers believe that healthcare providers are capable of providing healthcare services, they are likely to trust the providers and provide them with their PHI to seek needed care. Also, when higher levels of benevolent trust and integrity exist, consumers are likely to disclose PHI as they are confident that disclosed information will not be used opportunistically or manipulatively. Based on this argument and on the observed relationship in past research between organizational-based trust and behavioural intention, the following hypothesis is proposed.

> ***H4a****: Trust in healthcare providers will have a positive effect on willingness to disclose PHI.*

Studies in the IS context focused on either organizational trust (Chiu et al., 2009; Klein, 2007; Krasnova, Veltri, & Günther, 2012; Metzger, 2006; Mou & Cohen, 2014) or system/technology trust (Anderson & Agarwal, 2011; Dinev et al., 2016; Dinev & Hart, 2006). Consequently, the relationship between organizational and technology-based trust is under-explored. Similar to the discussion in Hypothesis 1, the literature on trust transfer (e.g., Stewart, 2003) suggest that if individuals assess that healthcare providers are trustworthy (i.e., have the favourable attributes of benevolence, competence, and integrity) they are likely to believe that these providers will introduce safe and reliable HITs that will ensure the privacy and security of consumers' PHI. This will likely reduce individuals' concerns about privacy of PHI stored and managed in the HITs. Individuals' trust in providers is thus expected to lead to their trust in HITs and reduce their concerns about PHI privacy.

> ***H4b****: Trust in healthcare providers will have a positive effect on trust in HIT.*
>
> ***H4c****: Trust in healthcare providers will have a negative effect on PHI privacy concerns.*

Trust in Health Information Technology (HIT)

Trust in technology is defined similarly as trust in other targets such as peoples or organizations. The trusting beliefs often considered in the extant research in the case of trust in technology are competence, reliability, and safety (Dinev & Hart, 2006). Trust in a technology's competence or ability means the technology is perceived to have the functionality to do the task individuals want accomplished (McKnight, 2005). Reliability clusters with integrity in the analysis of trusting beliefs by McKnight et al. (2002). A technology is perceived as reliable when it does what it is designed to do without frequent problems or unexpected results (McKnight, 2005). Trusting belief in a technology's safety refers to the belief that information submitted via or to the technology will be kept safe (Dinev & Hart, 2006).

Similar to past studies (Anderson & Agarwal, 2011; Dinev & Hart, 2006), trust in HIT is conceptualized as a multi-dimensional construct comprising of the trusting beliefs of competence, reliability, and safety. It thus reflects the individual's belief that HIT provides a reliable and safe environment and has the necessary components to facilitate the conduct of PHI-related transactions including storing, updating, and sharing PHI. As indicated in Section 2.4, trust in technology is the dimension of trust often studied in IS privacy research. It is shown as a key predictor of online service adoption (Carter & Bélanger, 2005; McKnight et al., 2002). It has also been found to strongly influence willingness to disclose personal information (Anderson & Agarwal, 2011; Dinev & Hart, 2006). Based on the empirical evidence in past studies, it is expected that individuals' trusting belief in a HIT's competency, reliability, and safety will positively influence their PHI disclosure intentions.

***H5**: Trust in HIT will have a positive effect on willingness to disclose PHI.*

3.4.3 Inhibitors of PHI Disclosure

PHI Privacy Concerns

Privacy concerns, discussed in detail in Chapter 2, is often defined as individuals' generalized concerns regarding how organizations collect, store, protect, and use personal information (Smith et al., 1996). Adapted to the healthcare context, PHI privacy concerns reflects individuals' concerns regarding healthcare providers' practices related to the collection, storage and use of their PHI. Smith et al. (1996) conceptualized privacy concerns as a multi-dimensional construct consisting of four dimensions: collection, errors, secondary use, and unauthorised access. These dimensions when adapted to the context of this study refers to individuals' concerns that 1) too much of their PHI are being collected and stored by healthcare providers, 2) healthcare providers do not have adequate measures to prevent against errors in PHI, 3) their PHI are used for other purposes without their authorisation, and 4) healthcare providers fail to prevent unauthorised access to PHI stored in their computer systems.

Several empirical studies in the healthcare context show that the four data-related dimensions of privacy concerns represent a reliable scale for measuring individuals' concerns toward healthcare providers' privacy practices (e.g., Angst & Agarwal, 2009; Dinev et al., 2016; Hwang et al., 2012; Li & Slee, 2014). As reviewed in Chapter 2, privacy concerns has received

strong empirical support in IS privacy research as the major deterrent of consumers' engagement in several behaviours. In the healthcare context, these behaviours include willingness to disclose or share PHI in an e-health environment (Anderson & Agarwal, 2011) and intention to use HITs (Li & Slee, 2014).

The influence of PHI privacy concerns on behavioural outcomes has yet to receive considerable empirical examination in the context of developing countries. A number of case studies suggest that individuals are generally concerned about the privacy of PHI related to heavily stigmatized diseases such as HIV/AIDS (e.g., Dapaah & Senah, 2016; Kwansa, 2013). Also, the introduction of HITs by healthcare providers has raised individuals' concerns about PHI privacy (Bedeley & Palvia, 2014; Willyard, 2010). It is therefore likely that individuals may be concerned about the collection of large volumes of their PHI for storage in HITs in which the risk of privacy loss is perceived by individuals as greater compared with non-digital forms (Fichman et al., 2011). The negative consequences individuals in developing countries can suffer from the exposure of certain PHI are quite severe including even death (Gettleman, 2011; PEN, 2010). Consequently, individuals may also be concerned about unauthorised use of and access to their digitized PHI. Errors in medical data can lead to problems including wrong diagnoses and prescriptions. It is thus likely that individuals in developing countries may be concerned about inaccuracies in their PHI.

In line with the consistently observed negative relationship between privacy concerns and behavioural outcomes, it is expected that individuals who express higher misgivings about healthcare providers' collection and unauthorised uses of PHI, the potential for errors in their PHI, and the possibility of unauthorised access to their PHI are likely to be less willing to disclose their PHI to the providers.

H6: *PHI privacy concerns will have a negative effect on willingness to disclose PHI.*

Privacy Risk

Following the popular definition of privacy risk in the IS privacy literature, privacy risk is defined as the extent to which an individual believes that a high potential for loss is associated with the disclosure of PHI for electronic storage (Featherman & Pavlou, 2003; Malhotra et al., 2004). Unlike privacy concerns, privacy risk is treated in IS privacy research as a unidimensional construct which concerns the potential loss of control over personal information (Xu et al., 2009).

Digitized healthcare can help in the accumulation of a large variety of PHI to support continuing and efficient care. Also, it increases the ease and speed with which large volumes of medical data can be shared among various stakeholders within the healthcare industry. However, there is increased risk of PHI privacy loss as any electronic transfer of information involves the risk that "the information could fall into the wrong hands" (Fichman et al., 2011). Lending support to this, in a recent study, Ponemon Institute (2016) found criminal attacks (e.g., hacking) represent the major source of PHI privacy breaches.

In addition to criminal attacks, organizations may also engage in opportunistic activities such as the surreptitious collection of consumer information and customer profiling, and the unauthorised access and selling of personal data (Dinev & Hart, 2004, 2006; Xu et al., 2009) which can lead to exposure of individuals' personal information. For instance, in the healthcare context, malicious insiders have been identified as a major source of PHI privacy breach (Ponemon Institute, 2016). Prior privacy research has therefore considered the opportunistic activities of the custodians of personal information as an important source of privacy risk (Dinev & Hart, 2004; Featherman & Pavlou, 2003; Xu et al., 2009).

There have been increased cybercrimes in Africa in recent years (e.g., Debrah, 2019; Serianu, 2016). The media attention on these crimes (e.g., Darko, 2015; Kyei-Boateng, 2018) is likely to sensitize individuals to the threats posed to privacy of digitized information. Lending support to this, in Ghana, due to the proliferation of cybercrimes individuals are concerned about the electronic storage of their PHI (Bedeley & Palvia, 2014). Aside from threats to PHI privacy posed by cybercrimes, as digitized healthcare can facilitate the opportunistic activities of various healthcare stakeholders (e.g., easy sharing of large volumes of PHI with third party organizations), it is argued that individuals who perceive high risk of PHI privacy loss in digitized healthcare environments may be more concerned about the privacy of digitized PHI.

Whilst the growing cybercrimes, including breaches of PHI privacy (Ponemon Institute, 2016; Technomag, 2018), and the increased opportunities for opportunistic activities regarding PHI may increase individuals' PHI privacy risk perceptions, they may also cause individuals to be less trusting of the functionality, reliability and safety of HITs for the protection and management of PHI. For instance, in the Internet context, Dinev and Hart (2006) found that perceptions of privacy risk arising from unauthorised access to personal information and from opportunistic activities (e.g., selling personal information to third parties) are strongly associated with low trust in the Internet. Therefore, if individuals perceive high risk of privacy loss as a result of digitizing PHI they are likely to have low trust beliefs in HITs.

In general, individuals are said to perceive a higher level of risk for disclosing more sensitive information (Dinev et al., 2013). Given the highly personal and sensitive nature of PHI, if individuals' sense that their information may not effectively be protected and there exist high risks of privacy invasion, they may not want to disclose their PHI in digitized healthcare settings. Past studies show that privacy risk increases individuals' concerns about privacy and decreases their willingness to disclose personal information (e.g., Dinev & Hart, 2006; Malhotra et al., 2004). Following the empirical evidence and the above arguments, the following hypotheses are proposed:

H7a: *Privacy risk will have a positive influence on PHI privacy concerns.*

H7b: *Privacy risk will have a negative influence on trust in HIT.*

H7c*: Privacy risk will have a negative effect on willingness to disclose PHI.*

Perceived Negative Consequences of PHI Disclosure

As defined earlier, perceived negative consequences of PHI disclosure reflects individuals' perception of potential negative consequences that can result from the exposure of PHI which an individual discloses to receive care. The negative consequences of privacy exposure vary depending on the sensitivity of the information to be disclosed (Laric et al., 2009; White, 2004). Though all types of PHI are sensitive, some PHI are considered more sensitive than others as evident by the legal protection offered to some health information (e.g., sexual health, mental health, etc.) (Anderson & Agarwal, 2011; Beckerman et al., 2008). In this study, the negative consequences associated with disclosing HIV-related PHI are considered. Indeed, HIV is especially relevant with 36.7 million people worldwide living with HIV in 2017, and 75% knowing their status (UNAIDS, 2018). The epidemic is most pronounced in Africa where about 26 million people live with HIV (UNAIDS, 2018). The situation is exacerbated further as HIV is heavily stigmatized, especially in Sub-Saharan Africa, and as a result, some individuals go to extremes to hide their infections to avoid negative consequences such as loss of job or relationships (Dapaah & Senah, 2016; Kwansa, 2013).

The exposure of PHI privacy could bring about adverse emotional, economic, and social consequences for an individual (Kordzadeh & Warren, 2017; Laric et al., 2009; Rindfleisch, 1997; Schwartz, 1997). An individual can suffer several adverse emotional consequences (e.g., shame, embarrassment, distress, etc.) from PHI privacy breach. An example of emotional consequence considered in this study is perceived inferiority; it is an important dimension of shame and refers to beliefs about the negative evaluation of the self by others (Goss et al., 1994). Economic adverse consequences reflect the potential impaired economic opportunities (i.e., opportunities to make a living or income) that can result from PHI privacy breach (Laric et al., 2009). Employment discrimination is the economic consequence considered in this study. Social consequences, on the other hand, relate to the potential damage to social relationships that can result from PHI privacy breach (Karwatzki et al., 2017). An example of social consequence considered is family rejection.

Individuals account for the negative consequences associated with a given personal information disclosure and the perception of the negative consequences influences their expectations and behaviour at a time when the actual consequences have not yet occurred (Karwatzki et al., 2017). However, the dread of the negative consequences "may lead to preventive actions or coping strategies" (Karwatzki et al., 2017). One main preventive action individuals may take (to avoid negative consequences) is refusing disclosure of their information. As Petronio (2002) notes, individuals keep certain information private due to fear of the "real or imagined repercussions the hidden information would bring with exposure". With specific regard to health information, Dowling and Staelin (1994) similarly argue that the negative consequences individuals may endure are important factors in their desire to protect the privacy of their PHI.

Individuals may refuse to disclose PHI for various purposes. However, the refusal to disclose accurate PHI to seek needed care can compromise diagnoses and treatment decisions (Anderson, 2000) which can have a damaging impact on one's health. Yet, some studies show that the dread of the negative consequences associated with PHI prevents some individuals

from disclosing their health information to seek needed care. For instance, in a 1993 survey in the U.S., 7% of the public had decided not to seek care due to fear that disclosure of their PHI might hurt their "job prospects or other life opportunities" (Goldman, 1998). Similarly, in Ghana, Kwansa (2013) found that some HIV infected individuals avoid treatment because they dread the negative consequences that may result from the disclosure of their status when they seek care; eventually, these persons may commit suicide or die from living secretly with the disease.

Although extant case studies examining negative consequences associated with PHI in developing countries were based on paper-based healthcare environment (Kwansa, 2013), given that individuals' beliefs of the likelihood of privacy loss is greater with digitized healthcare (Fichman et al., 2011), they may be more discouraged to disclose and allow digitization of their PHI due to the negative consequences they perceive should their digitized PHI be exposed. Lending support to this, some studies suggest that due to fear of negative consequences people lie to physicians, withhold certain information or avoid seeking care to prevent the creation and accumulation of their sensitive health information in computer systems (e.g., Anderson, 2000; Appari & Johnson, 2010; Rindfleisch, 1997; Schwartz, 1997). Thus, it is argued that perceived negative consequences of PHI disclosure will have a negative influence on individuals' willingness to disclose PHI. Specific hypotheses related to the negative consequences considered in this study (i.e., perceived inferiority, employment discrimination, and family rejection) are discussed next. Given the focus on negative consequences related to HIV/AIDS, some examples related to HIV/AIDS are provided in discussing the hypotheses.

Perceived Inferiority

Perceived inferiority reflects beliefs about the potential negative evaluation of the self by others that can result from the exposure of one's PHI. This definition is based on the dimension of the *Other As Shamer Scale* that measures individuals' perception of being seen as inferior by others (e.g., Goss et al., 1994).

Several studies show that people have negative attitudes toward HIV positives and therefore subject them to negative treatments and discrimination of various forms (Anafi, Mprah, & Asiamah, 2014; Dapaah, 2012; Duffy, 2005; Kwansa, 2013). For instance, people avoid HIV positives, refuse to share clothes or eat with them (Anafi et al. 2014). These ill-treatments cause damage to one's sense of self-worth and therefore people do not easily disclose their diagnosis (Dapaah & Senah, 2016; Mbonu, van den Borne, & De Vries, 2009). Some studies have also found consumers' reluctance to disclose information such as plastic surgery procedures (Laric et al. 2009) and purchase history of condoms (White, 2004) due to the negative impressions such disclosure could create about them.

Due to the high potential for privacy loss with digitized healthcare systems, it is expected that individuals who perceived that the exposure of the PHI they disclose to receive care will cause others to evaluate them negatively will be unwilling to disclose their PHI. This is consistent

with expectancy theory's notion that individuals behave in ways to minimize negative outcomes (Victor, 1964).

H8: *Perceived Inferiority will have a negative effect on willingness to disclose PHI.*

Employment Discrimination

Employment discrimination refers to beliefs about the potential impaired employment opportunities (e.g., job loss, denial of employment or promotion) that can result from PHI exposure (Karwatzki et al., 2017; Ulasi et al., 2009). In a recent study, Sprague et al. (2011) found that high levels of employment discrimination based on HIV status exists in all African sub-regions. These include refusals to hire or promote, and terminations of people with HIV. In Ghana, Kwansa (2013) and Dapaah (2012) have observed job loss as one of the consequences of contracting HIV/AIDs. In the USA, Schwartz (1997) found that testing for sickle cell anaemia led some African-Americans to lose their jobs.

In general, the evidence suggests that organizations use medical records in employment decision making and any disorders or diseases can impair employment opportunities of individuals (Laric et al. 2009(Pitta, Franzak, & Laric, 2003)). Therefore, to avoid employment risks, HIV positives conceal their infection unless they are forced to disclose (Sprague et al. 2011). Some pregnant women have also been found to hide their condition in order to stay employed (Laric et al., 2009). In another study, Flynn et al. (2003) found that patients refused to have an electronic psychiatric record due to fear that the record might hurt their job prospects

In line with the above studies, if individuals believe that the exposure of their PHI will adversely impact their job opportunities, they may refuse PHI disclosure to seek care in a digitized healthcare environment in which the risk of privacy loss is generally considered significant. Therefore, consistent with expectancy theory's explanation that individuals act to minimize risk (Victor, 1964), a negative relationship is proposed between employment discrimination and willingness to disclose PHI.

H9: *Employment discrimination will have a negative effect on willingness to disclose PHI.*

Family Rejection

Family rejection reflects beliefs about the potential neglect by one's family that can result from exposure of an individual's PHI. Social acceptance and social relationships affect the quality of one's life. However, they can be adversely affected by the extent to which information about one's health is disclosed (Laric et al., 2009; Pitta et al., 2003). Lending support to this, in many African countries, being HIV positive carries a strong sense of shame, with the disgrace also felt by one's family because of the disease's association with morally abhorrent behaviours including promiscuity and prostitution (Dapaah, 2012; Duffy, 2005). Therefore, to prevent stigma by association, some families abandon HIV infected members and evict them from their homes (Kahn, 2004). Other families also deny basic needs such as medicine to HIV relatives

because they consider their death warrant signed with the infection (Kwansa, 2013). Due to the anticipated negative reactions from family and friends, some HIV positives commit suicide or hide their infections (Kwansa, 2013).

In many African cultures, the family remains an important source of support and protection for individuals. Therefore, if the exposure of an individual's PHI will elicit adverse reaction from his family, individuals may be reluctant to disclose certain health information even to seek needed healthcare, especially in digitized healthcare environments given the high risk of privacy loss in such environments. It is thus proposed that:

H10: *Family Rejection will have a negative effect on willingness to disclose PHI.*

3.4.4 Control Variables

As was noted in Section 2.3.2, this study controls for the influence of the following individual characteristics and experience-related factors on PHI privacy concerns as they have been found to influence privacy concerns in the healthcare and other IS contexts (e.g., Esmaeilzadeh, 2018a; Kenny & Connolly, 2016; Perera et al., 2011; Taylor et al., 2015): gender, age, education, health status, computer experience, past privacy experience, and privacy orientation.

Similarly, following the literature review in Section 2.3.4, the following demographic factors which have been found to influence trust in technology are used as control variables on trust in HIT (Bansal et al., 2010; Corbitt, Thanasankit, & Yi, 2003; Dickerson, 2003; Dutta-Bergman, 2003): age, gender, education, computer experience, and health status.

Demographic factors are often used as control variables on behavioural intention dependent variables in the healthcare context (e.g., Anderson & Agarwal, 2011; Esmaeilzadeh, 2018a; Frost, Vermeulen, & Beekers, 2014; Jena, 2015; Rahman, 2017). Consequently, the influence of the seven demographic factors on willingness to disclose PHI are also controlled for to exclude any variance they might explain in this dependent variable.

3.5 Chapter Summary

This chapter has presented the proposed research model for this study and discussed the hypothesized relationships in the model. The proposed model extends the core privacy calculus model to incorporate important factors that affect individuals' willingness to disclose PHI in digitized healthcare settings. The model also examines factors that influence individuals' trust in HIT and PHI privacy concerns. In addition to the privacy calculus as the overarching theoretical framework, justice theory and the trust transfer theory were leveraged in the research model and hypotheses development. The quantitative research methodology followed in testing the research model is discussed in the next chapter.

CHAPTER FOUR: RESEARCH METHODOLOGY

This chapter discusses the research methodology used to address the research questions raised in this study. It begins with a brief outline of the research philosophies and methodologies often used in IS research highlighting the research philosophy employed in this study. Next, the context of the study is described. This is followed by an outline of the sampling strategy used in the study as well as a discussion of the method of data collection. The chapter concludes with a brief description of the data analysis strategy used in analysing the collected data.

4.1 Research Philosophy and Methodology

Research philosophies concern "the development of knowledge and the nature of that knowledge" (Saunders, Lewis, & Thornhill, 2011). They contain important assumptions about how the researcher views the world (Saunders et al., 2011). The researcher's worldview influences what is considered as valid knowledge and how this knowledge can be constructed and evaluated.

Two of the major research philosophies used in the IS discipline are positivist and interpretivist research philosophies. Research that adheres to a positivist philosophy assumes that an objective reality exists independent of humans that can be observed and measured (Orlikowski & Baroudi, 1991). This research philosophy has its roots in the natural sciences and thus considers the scientific method the best way to understand reality. Based on this perspective, researchers often examine the effects of one or more variables on another (Kaplan & Duchon, 1988). Hypotheses are proposed between these variables often based on theory; objective and quantifiable data is collected to test the hypotheses and generalizations are made about the population whose sample data was collected. Therefore, IS studies are classified as positivist if there is evidence of "formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from a representative sample to a stated population" (Orlikowski & Baroudi, 1991).

An interpretive study, on the other hand, "assumes that people create and associate their own subjective and intersubjective meanings as they interact with the world around them" (Orlikowski & Baroudi, 1991). Reality and our knowledge of it are therefore social products that cannot be understood separate from the social actors that construct and make sense of that reality (Orlikowski & Baroudi, 1991). Interpretive research seeks to understand phenomena through the meanings that people assign to them and does not predefine the relationship between independent and dependent variables (Klein & Myers, 1999). The purpose of an interpretive study is not to generalize from the setting or phenomenon being studied to a population; rather, the objective is to understand in depth the deeper structure of the phenomenon and use this knowledge to inform other settings (Orlikowski & Baroudi, 1991).

Traditionally, two research methodologies, quantitative and qualitative, have dominated IS research. In recent years, mixed methods research has also been introduced as an approach that combines quantitative and qualitative research methodologies in the same research inquiry

(Venkatesh, Brown, & Bala, 2013). The traditional research methodologies are associated with a number of research philosophies. A qualitative research methodology is often associated with interpretivist research philosophy (Creswell & Clark, 2017). In IS and other social sciences, qualitative methods are typically used for exploratory research in order to develop an in-depth understanding of a phenomenon and/or to inductively generate new theoretical insights (Venkatesh et al., 2013).

On the other hand, the quantitative methodology, which has been the dominant methodology in several disciplines including IS, is predominantly associated with the positivist research philosophy (Creswell & Clark, 2017). Quantitative research, therefore, involves objective measurement of variables (with numbers) and the statistical analysis of data to test hypothesized relationships between the variables within a population. This allows for inferences about the behaviour of the studied population (Creswell, 2009). A quantitative research methodology is usually used in the IS field for theory testing (Venkatesh et al., 2013).

The purpose of this study is to test an apriori model which seeks to explain individuals' intention to disclose personal health information in a digitized healthcare setting. Consequently, this research adopts a positivist worldview using a quantitative approach to data collection and analysis. The data for quantitative research can be obtained through various methods including surveys, experiments, etc. The survey represents the most widely used data collection method (Venkatesh et al., 2013). A major advantage of surveys is that they help "bring breadth to a study by helping researchers gather data about different aspects of a phenomenon from many participants" (Venkatesh et al., 2013). By studying a representative sample of a phenomenon, the survey aims to enable the researcher to discover relationships that are common across the phenomenon and provide generalizations about the object of study (Gable, 1994). Likewise, this study aims to examine the perceptions of individuals of various backgrounds regarding their privacy and trust beliefs as well as their PHI disclosure intentions in a digitized healthcare environment. A survey approach fits this purpose and was therefore used as the method in collecting data to test the proposed research model.

4.2 Research Setting

This study focuses on the willingness of individual consumers of healthcare services in developing countries to disclose their PHI for the purpose of receiving care from healthcare providers where the disclosed PHI is digitized. All people are potential consumers of healthcare services as they may need to seek care some stage in their life (Payton et al., 2011). To gain a better understanding of PHI disclosure intentions among individuals in a developing country, this study explored the views of individuals (18 years and over) in Ghana, a Sub-Saharan African country. The profile of Ghana and the healthcare system in the country including the digitized healthcare setting which is the focus of the survey conducted in this study are described next.

4.2.1 Brief Profile of the Study Country

Ghana is used as a case setting for addressing the questions posed in this study. Previously named "Gold Coast" and a former British colony, Ghana is situated on the coast of West Africa. It is bordered on the east by Togo, on the west by Cote d'Ivoire, on the north by Burkina Faso and on the south by Gulf of Guinea. Ghana gained independence on 6th March 1957, the first sub-Saharan country to achieve this in colonial Africa. As a diglossic country, over 250 languages and dialects are spoken in Ghana. However, English was adopted as the country's official language and it is the standard language used for educational instruction.

The population of Ghana is estimated at 28,308,301 people (Ghana Statistical Service [GSS], 2016) and its geographic size is 238,533 square kilometres. The country is endowed with natural resources including gold, oil, bauxite, and diamonds. It is the world's second-largest exporter of cocoa, behind Côte d'Ivoire and the nation's economy depends on the production of the crop (Oxford Business Group [OBG], 2014). Administratively, Ghana is divided into 16 regions, 275 constituencies, and 254 districts (including metropolitan and municipal assemblies) (GhanaDistricts, 2018). Accra in the Greater Accra region serves as the country's capital. The geographical map of Ghana is provided in Figure 4.1.

4.2.2 The Ghana Healthcare System

Two major actors are involved in the provision of healthcare in Ghana; public and private healthcare providers. Public healthcare providers are usually referred to as public/government hospitals as they are managed by the government. Private healthcare providers (or private hospitals), on the other hand, comprise privately-owned commercial institutions. Other healthcare service providers include traditional, non-governmental, and faith-based/religious institutions. The majority of the Ghanaian population seek healthcare from public hospitals as private hospitals are quite few and located mainly in the country's largest cities.

The public health services in Ghana are organized in a hierarchy ranging from the sub-district to the national level. Health centres, health posts, and clinics constitute healthcare delivery channels at the sub-district level. To extend access to health services to marginalized communities, community-based health facilities also exist at the sub-district level to provide public health and basic clinical care services at the community level. The services and activities of sub-district healthcare providers are coordinated at the district level. A hospital is designated at the district level as the first referral point for the sub-district healthcare providers. Regional hospitals serve as second referral points and complex cases are referred to national care providers. Referral facilities at the national level include two teaching hospitals, three psychiatric hospitals and a large military hospital (Acquah-Swanzy, 2015).

The Ministry of Health (MOH) serves as an executive regulatory body that regulates the activities of the various public and private healthcare providers in Ghana. Among its core functions include formulating health policy, setting standards for the delivery of health care, and providing strategic direction for health delivery services. The implementation of national

policies and the management of resources for healthcare delivery are, however, carried out by the Ghana Health Service (GHS), an autonomous and apolitical institution established by Act 525 of 1996 (Ghana Health Service [GHS], 2015).

Figure 4.1. Map of Ghana (GhanaDistricts, 2018)

Healthcare in Ghana is financed by the government, the National Health Insurance Scheme (NHIS), out-of-pocket payments, and donor budget support (Acquah-Swanzy, 2015). With regard to the NHIS, aside from the premium paid by registered members of the scheme, the main sources of finance include the formal sector, government and Ghanaian citizens through value-added tax. About 35% of Ghana's population are registered paying subscribers (IICD,

2014). Both public and private healthcare providers are accredited by the scheme to provide services to registered clients. It must be noted that not all healthcare services (e.g., HIV antiretroviral medicines, cancer treatment except cervical and breast cancer, etc.) are covered under the scheme and hence require payment by clients. For people not registered under the scheme, upfront payment must be made for needed healthcare services. Prior to the introduction of the NHIS, this cash-and-carry system constituted the main payment method for healthcare services.

Among the challenges facing the Ghana healthcare system include lack of skilled health personnel and inadequate infrastructure. Similar to many developing countries, Ghana has a very low physician to population ratio. In 2010, the ratio of doctors and nurses per 1000 population stood at 0.11 and 1.14, respectively (Bedeley & Palvia, 2014). Coupled with this, the distribution of health workers and advanced medical infrastructure is skewed towards urban areas (MOH, 2010). Consequently, people in marginalized communities must travel to urban areas to access specialist care (Saleh, 2012). Lack of appropriate transport system makes it extremely difficult for the people in remote communities to access timely care in emergency situations contributing to the loss of lives in the country. These challenges are among the factors driving the effort to leverage HITs to ensure quality of care and increase geographic access to healthcare services (MOH, 2010).

4.2.3 Current State of e-health in Ghana

Ghana, like many other developing countries, in recent years has been transforming its healthcare services using IT to improve the quality and standard of care delivery as well as increase access to care. The country's commitment to digitize healthcare started with the government's launch of a national e-health strategy in July 2010, which provides a framework for the design and rolling-out of e-health projects in Ghana (MOH, 2010). Four main strategies are outlined for arriving at this broad objective: 1) streamlining the regulatory framework for health information management, 2) building capacity for wider application of e-health solutions in the health sector, 3) increasing access to healthcare through the use of IT, and 4) achieving a paperless records and reporting system.

As part of implementing the strategy, the government has rolled out a major fibre optic network accessible for health services (IICD, 2014). This coupled with the current high mobile penetration rate (over 90%) in the country has contributed to the development of IT services in the health sector by government, international organizations and the private sector. For example, as another area of advancement in implementing the e-health strategy, the government has introduced a nationwide e-health system called district health information management system (DHIMS II) which district hospitals use to generate and report on routine service data on health service utilization, morbidity, and disease patterns. Using this system, the GHS collates and analyses health data from the district hospitals to generate a nationwide health monitoring and evaluation data for public health management (Afarikumah, 2014; IICD, 2014).

Aside from DHIMS II, other locally developed EHR systems (e.g., HAMS, iHOST, Healthfore) have been introduced in hospitals across the country (e.g., Acquah-Swanzy, 2015; IICD, 2014). Some hospitals have also adopted and customised low-cost open-source EHRs (e.g., OpenEMR) to support their operations (e.g., Gyamfi, 2016). Also, there are several other e-health projects which involved the use of mobile phones, web-based applications, etc. to offer various healthcare services ranging from health information management and communication to offering online consultations and advice to patients (Afarikumah, 2014).

In general, like many other developing countries (see Lewis et al., 2012), Ghana is still at the embryonic stage of leveraging HITs to improve care delivery. There is a lack of regulatory frameworks and standards to ensure interoperability between the various EHR systems introduced in hospitals across the country (IICD, 2014). Even within a hospital, many of the functionalities of adopted EHR systems have not been activated to achieve service integration at the institutional level. Existing EHR systems can thus be considered as stand-alone or simple systems based on the types of EHR systems described in Section 1.2.

The hospitals continue to run manual (paper-based) systems as they migrate to e-health systems (Acquah-Swanzy, 2015; Gyamfi, 2016). Consequently, the benefits of the newly introduced e-health systems have yet to be fully realised. This notwithstanding, there has been modest success in terms of extending care access to rural communities, and in the collection and management of health information (IICD, 2014). In some health facilities, improved patient information management has helped address the problem of missing patient data and ensure easy access to past medical records (e.g., Acquah-Swanzy, 2015; Gyamfi, 2016).

In recent years, the government has passed laws that grant individuals control over how their personal information, including health information, in any format is collected, used, and disclosed (Data Protection Act, 2012). However, there are no detailed privacy legislation/policies regarding health information exchange by healthcare providers, and the handling of health data even within an institution (e.g., what data must be stored and for how long) (Achampong, 2012). Thus, similar to the initial introduction of IT systems in the health sector of the developed world (see Rothstein, 2007), privacy regulation in Ghana is lagging behind health technology development effort. As e-health development continues, it is expected that privacy laws and policies will evolve to both safeguard the privacy of consumer health information and to ensure the sharing of this information by healthcare providers.

Given that existing EHR systems being used by healthcare providers in Ghana are stand-alone systems, this study's investigation of consumers' PHI disclosure intentions in a digitized healthcare environment was undertaken within the general context of stand-alone EHR systems, irrespective of a specific EHR system implementation by a particular healthcare provider which might influence perceptions about PHI privacy concerns and disclosure intentions. This approach is consistent with prior IS privacy research in the healthcare context (e.g., Anderson & Agarwal, 2011; Dinev et al., 2016). The sections that follow outline the

procedure used in identifying the sample (i.e., target respondents) for the survey, the respondent recruitment strategy, and the survey design.

4.3 Sampling Procedure

This study used the purposive sampling strategy. With this sampling technique, the researcher uses a set of criteria to identify study samples (Kemper, Stringfield, & Teddlie, 2003). The core objective of this study is to understand factors influencing individuals' PHI disclosure intentions in a digitized healthcare environment. The purposive sampling strategy was selected to ensure that individuals selected for the survey were diverse in terms of demographic characteristics and perceptions regarding PHI privacy concerns and disclosure intensions.

The criteria used in ensuring diversity among participants are age, education, health status, and computer experience. As discussed in Section 2.3.1, several studies show that age has a positive influence on PHI privacy concerns (Kenny & Connolly, 2016; Papoutsi et al., 2015). A few studies have also found that older individuals have less trust in technology than younger individuals (Dutta-Bergman, 2003; Li et al., 2008). Despite expressing high concerns about PHI privacy, the majority of studies indicate older individuals are more willing to disclose their PHI than younger individuals (Frost et al., 2014; Jena, 2015; Kordzadeh & Warren, 2017). These findings indicate that diverse age groups are required to capture varying levels of privacy and trust beliefs as well as PHI disclosure intentions.

The second criterion used concerns the educational level of the participants. PHI privacy concerns either decreases with higher levels of education (King et al., 2012; Vodicka et al., 2013) or increases with higher levels of education (Hwang et al., 2012; Papoutsi et al., 2015). Also, whereas some studies show that higher levels of education decrease willingness to share PHI (e.g., Anderson & Agarwal, 2011), other studies found no significant influence of education on PHI disclosure intentions (Esmaeilzadeh, 2018a; Jena, 2015). The existing studies thus indicate that privacy perceptions and PHI disclosure intentions may also vary based on the educational level of individuals and hence it was important to consider a sample of individuals with varying levels of education.

The third criterion used in identifying survey participants was health status. A number of studies have found that individuals with poor health express greater PHI privacy concerns (Flynn et al., 2003; Kordzadeh et al., 2016), whereas other studies show individuals with poor health have decreased concerns about PHI privacy (Esmaeilzadeh, 2018a; Lafky & Horan, 2011). Notwithstanding concerns about privacy, regarding intention to disclose PHI, the majority of studies show that individuals with poor health are more willing to disclose their PHI to seek needed help in order to improve their health condition (Anderson & Agarwal, 2011; Zhou, 2018). As individuals with varying health conditions are likely to express different privacy beliefs and PHI disclosure intentions, selecting individuals with varying health status is important.

The final criterion relates to computer experience. The influence of computer experience has received scant attention in the healthcare privacy literature. One study found that computer experience reduces PHI privacy concerns (Perera et al., 2011). Several studies, however, suggest that computer experience influence individuals' perceptions and beliefs regarding technology innovation (Davis, 1989; Im, Bayus, & Mason, 2003) including HITs (Rahman & Ko, 2012). Based on these studies, it is expected that privacy beliefs and PHI disclosure behaviour of individuals may vary based on their experience with using computers, especially in developing countries where digital divide and gender digital gap still exist (ITU, 2016, 2017; PRC, 2015). Thus, individuals with varying levels of computer experience must be selected.

The next section describes the process for recruiting survey participants for the study based on the above outlined criteria.

4.3.1 Recruitment of Survey Sample

The survey used in the study was paper-based and was conducted between November 2017 and February 2018. Ethical approval was sought from the University of Canterbury's Human Ethics Committee before conducting the survey (see Appendix C).

As discussed in the previous section, the researcher sought to recruit a survey sample that varied in age, education, health status, and computer experience. In line with this objective, samples were recruited from various sources including college campuses, hospitals, business/governmental organizations, and local neighbourhoods. A recent study by PRC (2015) found that in developing countries, Internet usage is more common among young people, the higher educated, and individuals with English language ability. Thus, it was reasoned that recruiting individuals from college campuses, local neighbourhoods, and business/governmental organizations would improve the sample variety in terms of age, education, and computer experience. Local neighbourhoods could also be a source of individuals with less or no education and computer experience. To include individuals with varying health status, the researcher recruited patients visiting or admitted at hospitals as it was reasoned that the health condition of these individuals might differ from individuals not seeking care at the time of the survey.

The researcher recruited survey assistants to help in the distribution and collection of surveys on college campuses and in local neighbourhoods. The purpose of the survey was explained to all survey assistants to ensure they have good background knowledge about the study. They were also taken through all the ethical issues concerning the survey as described in the consent form (see Appendix E). This was to ensure that the survey assistants treat participants with respect and dignity and that confidentiality of participants' information was maintained throughout the data collection process. The survey assistants were compensated for their help with data collection.

Similar to past studies (e.g., Dinev et al., 2016), to recruit survey participants from college campuses and local neighbourhoods, individuals were approached in person. The purpose of

the survey as well as ethical issues concerning the survey were explained to all potential participants and then they were asked if they would like to participate in the survey. Hardcopy questionnaires were distributed to all participants who volunteered to participate in the study and collected at a later date.

To recruit individuals working in different professions with varying educational levels, contacts were made with employees known to the researcher working in various business and governmental organizations who distributed and collected surveys from the staff of their organizations. As regards recruiting patients visiting or admitted at hospitals, for hospitals where permission to conduct the survey was granted, the researcher arranged with a member of staff to distribute and collect the surveys completed by the patients. An example of the invitation letter sent to hospitals is provided in Appendix D.

As an expression of the researcher's appreciation for the time and effort spent in completing the survey, a nominal reward of three Ghana cedis (GH¢3.00) worth of mobile credits equivalent to NZD1.00 was given to every volunteered survey participant.

4.4 Survey

This section details the design of the survey that was used to collect data for and test the hypothesized relationships in the proposed research model.

4.4.1 Survey Procedure and Pilot Testing

The survey study was cross-sectional in nature and hence all the variables of interest to the research were measured at a single point in time using a single set of respondents (see survey instrument in Appendix E). At the beginning of the survey, participants were asked to read the consent form which explains the purpose of the study and ethical considerations including voluntary participation in the survey. The introductory pages of the survey defined the key term, personal health information (PHI), and explained the technological context of the study, i.e., stand-alone EHR system. "EHR system" was replaced with the term "computer health system" since it was reasoned that the target group might not be familiar with the term, EHR. However, the description of a "computer health system" was consistent with that of a stand-alone or simple EHR system implementation by a healthcare provider. To infuse realism, the description included a typical scenario of how an individual's interaction with the various units/departments in a hospital with a functional EHR system would look like. The explanation of an EHR system was provided to ensure participants answered the survey with a common understanding of the technological context of the study. This approach is consistent with recent studies examining consumers' attitudes toward and adoption of EHR systems (Angst & Agarwal, 2009; Dinev et al., 2016).

The main questions related to the constructs in the proposed research model are presented after the description of the technological context of the study. Regarding perceived negative

consequences of PHI disclosure, a scenario-based approach was used to explore the influence of the three negative consequences considered in the study (i.e., perceived inferiority, employment discrimination, and family rejection) on individuals' PHI disclosure decisions. First, a question was posed asking participants to imagine they have HIV/AIDS. Next, on a Likert-type scale with an anchor as 1 for "Not at all sensitive" and 7 for "Extremely sensitive", participants were asked to indicate the extent to which they would consider their HIV positive status as sensitive information (i.e., information they want to keep private). The participants then answered questions regarding the negative consequences (i.e., perceived inferiority, employment discrimination, and family rejection) they might face should there be an exposure of their HIV positive status. Hypothetical scenarios have been used in recent years in examining individuals' adoption of technologies (Miltgen et al., 2013) and their willingness to disclose PHI (Anderson & Agarwal, 2011). This approach was considered appropriate for this study.

Also, to explore the influence of the effectiveness of government regulation in the proposed model, a brief summary of the existing regulations in Ghana aimed at protecting personal information in general and health information specifically was provided. Survey participants were required to read the summarized regulations before answering questions which measured their perceptions of the effectiveness of the regulations in protecting the privacy of their PHI. This approach is consistent with the measurement of government regulation by Xu et al. (2009) in the context of location-based services.

As with all cross-sectional design, the study was subject to common method bias. In the survey design, several procedural remedies recommended by Podsakoff, MacKenzie, Lee, and Podsakoff (2003) were implemented to reduce the negative effect of common method bias. These include assuring anonymity of respondents, encouraging respondents to provide honest responses by informing them that there were no right or wrong answers, and psychological separation of independent and dependent variables. Also as described above, contextual information was provided, and key terms and technologies were defined to reduce ambiguity. The statistical analysis performed to explore the presence of common method bias are discussed in the next chapter.

The survey was pretested with a convenience sample of 24 individuals from Ghana. The sample was diverse in terms of age, gender, and health concern (i.e., the extent to which an individual is concerned or worried about his/her health). The majority of the participants had secondary education or above and some computer experience; however, this is not representative of the wider population.

The purpose of the pretest study was to ensure the survey instructions were adequate and that the technological context was well understood. Minor amendments were made based on feedback from the respondents. For instance, examples were provided to make the description of the technological context easy to understand. The researcher reviewed the revised survey with the survey assistants (recruited to help in the distribution of surveys) to ensure all instructions and definitions were clearly understood prior to the actual survey.

4.4.2 Operationalization of Variables

The measurement items for the constructs in the research model were derived from existing validated measures and adapted to the context of this study. The four rules developed by Jarvis, MacKenzie, and Podsakoff (2003) for identifying a construct as formative or reflective were applied in determining whether a construct in the proposed model was measured formatively or reflectively. According to the first rule, for formative measures, the direction of causality is from items to construct, whereas in the case of reflective measures the direction of causality is from construct to items. The second rule states that items should be interchangeable for reflective measures but not for formative measures. The third rule maintains that covariation among items is not necessary for formative measures but is necessary for reflective measures. According to the fourth and final rule, reflective measures are required to have the same antecedents and consequences, but this is not a necessary condition for formative measures.

To measure PHI privacy concerns, the Concern for Information Privacy (CFIP) instrument (Smith et al., 1996), which is commonly used to measure information privacy concerns (Bélanger & Crossler, 2011; Yun et al., 2019), was used. CFIP consists of four dimensions: collection, errors, secondary use, and unauthorised access. In an empirical study to determine the factor structure of the CFIP, Stewart and Segars (2002) found that CFIP is better represented as a reflective second-order construct with reflective first-order constructs comprising of the four CFIP dimensions. Thus, individuals' privacy concerns includes both the concerns related to each dimension of CFIP as well as concerns shared across the four dimensions.

As discussed in Chapter 2, the common theme in IS privacy literature is that individuals' concerns about privacy stem from their lack of control over their personal information. In line with this notion, Stewart and Segars (2002) suggest that concern about control over one's personal information may explain privacy concerns related to each of the dimensions of CFIP and the interdependencies among the dimensions. In support of this suggestion, Xu, Teo, Tan, and Agarwal (2012) found that individuals' perceived control over their personal information significantly reduces privacy concerns related to each dimension of CFIP as well as the overall concerns shared across the four dimensions.

In addition to Stewart and Segars (2002), strong support has been found for a reflective second-order model of CFIP in a number of studies including studies in the healthcare context (e.g., Esmaeilzadeh, 2018a; Korzaan & Boswell, 2008). These studies show that in addition to the measures/items of the respective dimensions of CFIP, the dimensions of collection, errors, secondary use, and unauthorised access which are collectively used to measure CFIP also meet the four conditions for reflective measures identified by Jarvis et al. (2003). Accordingly, PHI privacy concerns was operationalized in this study as a reflective second-order construct with reflective first-order construct measures of collection, errors, secondary use, and unauthorised access.

To assess individuals' trusting beliefs in healthcare providers, the three dimensions of trusting beliefs namely benevolence, competence (or ability), and integrity identified by McKnight et al. (2002) were used. The measures of the three dimensions fulfil the four rules for reflective measures and therefore these dimensions are measured reflectively in most IS studies (see Söllner & Leimeister, 2013). However, trusting beliefs is considered a theoretical construct (Mayer et al., 1995; McKnight et al., 2002) which is formed by the three dimensions of benevolence, competence, and integrity (Klein & Rai, 2009; Petter, Straub, & Rai, 2007). Thus, the three dimensions of benevolence, competence, and integrity used to measure trusting beliefs meet the four conditions of formative measures noted above. Studies examining conceptualizations of trusting beliefs have found strong support for a formative second-order conceptualization with reflective first-order factors comprising of the benevolence, competence, and integrity dimensions (Klein & Rai, 2009; Petter et al., 2007; Serva, Benamati, & Fuller, 2005). Following these studies, trust in healthcare providers was operationalized as a second-order formative construct with first-order reflective construct measures of benevolence, competence, and integrity.

Aside from the operationalization of PHI privacy concerns and trust in healthcare providers discussed above, all other remaining constructs were measured as first-order constructs. The measures of these constructs meet the four rules for reflective measures and hence the constructs were measured reflectively. The definition of all the constructs and the literature support for the measurement items used in the study are provided in Table 4.1. The actual measurement items used in the study are provided in Appendix E. 7-point Likert-type scales were used to measure all items.

Table 4.1 Construct Definition and Source of Items

Categories	Construct	Definition	Source of Items
Main Dependent Variable	Willingness to disclose PHI	Willingness to provide personal health information (PHI) to receive care where the disclosed PHI is digitized.	Malhotra et al. (2004); Anderson and Agarwal (2011)
Drivers of PHI Disclosure	Convenience	Individuals' perception of the time and effort that will be spent in receiving care in a digitized healthcare environment.	Berry, Seiders, and Grewal (2002); Seiders et al. (2007)
	Trust in Healthcare Providers	Trusting belief in healthcare providers' benevolence, competence, and integrity.	McKnight et al. (2002)
	Trust in Health Information Technology (HIT)	Trusting beliefs reflecting the confidence that PHI submitted for electronic storage will be handled competently, reliably, and safely.	Dinev and Hart (2006);
Inhibitors of PHI Disclosure	PHI Privacy Concerns	Concerns about healthcare providers' practices related to the collection, storage, and use of PHI through HITs.	Smith et al. (1996)
	Privacy Risk	Beliefs that a high potential for loss is associated with disclosing PHI for electronic storage.	Xu, Dinev, Smith, and Hart (2011)

Categories	Construct	Definition	Source of Items
	Perceived Inferiority	Beliefs about the potential negative evaluation of the self by others that can result from the exposure of one's PHI.	Goss et al. (1994)
	Employment Discrimination	Beliefs about the potential for impaired employment opportunities that can result from the exposure of an individual's PHI.	Ulasi et al. (2009)
	Family Rejection	Beliefs about the potential for neglect by one's family that can result from exposure of an individual's PHI.	Genberg et al. (2008)
Antecedents to Trust & Concerns	Perceived Attitude of Health Workers	The extent to which individuals believe that health workers treat them with dignity, politeness, and respect throughout the process of receiving care.	Sumaedi et al. (2016)
	Perceived effectiveness of government regulation	The extent to which individuals believe that government regulation is able to provide effective and reliable protection against privacy breaches on their PHI.	Dinev et al. (2016)
Control Variables	Privacy Orientation	The extent to which one wants to guard and limit access to his personal information.	Taylor et al. (2015)
	Privacy experience	Experience of personal information abuse in the past and awareness of media coverage of such abuses.	Smith et al. (1996); Xu et al. (2005)
	Computer Experience	Number of years an individual has used a computer for any task.	
	Health Status	One's perception of his/her overall health condition.	Angst and Agarwal (2006)
	Health Concern	The extent to which an individual is concerned or worried about his/her health.	Angst and Agarwal (2006)
	Gender	Coded as 0 for Females, 1 for Males.	
	Education	The level of education of an individual.	
	Age		

4.5 Data Analysis

To test the proposed research model, the structural equation modelling (SEM) technique was used. SEM is a second-generation multivariate data analysis technique. SEM overcomes the weaknesses of first-generation statistical methods/techniques (e.g., regression, factor analysis, and analysis of variance) as it helps to incorporate unobserved (latent) variables and account for measurement error in observed variables (Hair, Hult, Ringle, & Sarstedt, 2016).

There are two approaches to SEM: covariance-based SEM (CB-SEM) and partial least squares SEM (PLS-SEM). The primary use of CB-SEM is to confirm or reject theories whereas PLS-

SEM is primarily used in exploratory research to develop theories, i.e., predicting key target constructs (Hair et al., 2016). Given that this study is an early attempt at developing a theoretical model to explore the factors driving the intention to disclose PHI in a digitized healthcare environment among individuals in developing countries, PLS-SEM was considered to be more suitable for this study than CB-SEM.

There are other characteristics of PLS-SEM which makes it suitable for this study. First, PLS-SEM helps to analyse measurement and structural models with multi-item constructs that include direct, indirect, and interaction effects (Kim, Chan, & Kankanhalli, 2012; Wasko & Faraj, 2005). Unlike CB-SEM, PLS-SEM can handle complex structural models and easily incorporates reflective and formative measurement models. Second, PLS-SEM makes no assumptions about the distribution of data and can generate robust model estimations with data that have normal as well as extremely non-normal distributional properties (Hair et al., 2016). Third, PLS-SEM is not as restrictive on the sample size like CB-SEM methods that require relatively large sample sizes (Kim et al., 2012).

Due to the above features of PLS-SEM, the use of PLS-SEM in testing the research model of the study is considered appropriate (Marcoulides, Chin, & Saunders, 2009; Ringle, Sarstedt, & Straub, 2012).

4.6 Chapter Summary

This chapter discussed the research philosophy and methodology underlying the study. This study is positivist and the quantitative research methodology was used in testing the proposed research model. A cross-sectional survey design was used in collecting data to test the model. PLS-SEM, the statistical technique for analysing the survey data was briefly introduced. The following chapter discusses in detail the use of the PLS-SEM technique in validating the survey data and in testing the research model.

CHAPTER FIVE: DATA ANALYSIS

This chapter details the analysis and results of the survey conducted to test the research model proposed in this study. First, the sample response, data preparation process carried out and the sample characteristics are described. Next, the statistical tests performed to address common method bias issues are presented. The constructs in the proposed research model are then evaluated to assess their reliability and validity. This is followed by a test of the hypothesized relationships in the model. The chapter concludes by highlighting the results from the test of the key hypotheses.

5.1 Sample Response

As noted in the previous chapter, the samples of the study were recruited from various settings in Ghana including college campuses, hospitals, business/governmental organizations, and local neighbourhoods. An estimated total of 450 surveys were distributed in these settings. Out of this total, 302 questionnaires were returned. Each questionnaire was manually examined by the researcher to identify any problematic surveys (e.g., uncompleted surveys or straight-lining response patterns). Through this process, 15 surveys were identified which were partially completed. Following recommendations in Hair et al. (2010), since each of these surveys had over 50% missing data, they were excluded from the data analysis. Also, 11 surveys were answered by various health professionals (e.g., doctors, nurse). The survey includes questions which assess individuals' perceptions of the attitude of health workers and their trust in healthcare providers. Due to potential bias (e.g., leniency bias (Podsakoff et al., 2003)) in the health professionals' responses to these questions, these surveys were also excluded. Thus, a total of 276 usable surveys were returned. This equates to a usable response rate of 61.33%

5.2 Data Preparation

The 276 completed surveys were further screened to identify, and address issues related to missing data and outliers. None of the items/variables has missing values of 5% or more with the overall extent of missing data across all cases was less than 1%. Similarly, there were some missing data in 65 cases, but each case was missing below 10% of data. Given the low extent of missing data, missing data is not likely to pose a problem in the analysis (Hair et al., 2010), and any imputation method could be used with limited effect on the analysis results (Hair et al., 2016). As mean replacement is a commonly used imputation method, missing values for an item were replaced by the item's mean value.

After addressing missing values, the data was explored for the presence of univariate outliers using boxplots. All cases with extremely high or low values (i.e., outliers) for a particular item were examined to see if the values were outside the 7 Likert type scales used in measuring variables. None of the cases had values outside the 7-point scales used. The answers for the identified cases across all variables were also assessed. None of the cases had an unusually low or high standard deviation in their answers across all variables. Therefore, it was decided to

retain cases with extreme responses as these responses fall within the populations studied and thus could be theoretically justified. For example, it is possible that individuals with no computer usage experience may express high PHI privacy concerns due to anxiety about computers or the Internet. It is also possible that they may not be aware of the threats to the privacy of digitized information and therefore be less concerned about the privacy of digitized PHI.

5.3 Sample Profile

The sample profile of the completed 276 responses is provided in Table 5.1. Health status was measured with 7-point scales anchored with *"Very poor"* and *"Very good"*. Responses corresponding to the lower end (i.e., 1-3), mid-point (i.e., 4), and higher end (i.e., 5-7) of the scale were considered as representing individuals with *poor health*, *fair health*, and *good health*, respectively. Similarly, health concern was measured with 7-point scales anchored with *"Not at all worried"* and *"Extremely worried"*. Responses corresponding to the lower end, mid-point, and higher end of the scale were considered as representing individuals who are *less worried*, *somewhat worried*, and *extremely worried* about their health, respectively.

Table 5.1 Profile of Survey Participants

Demographic	**Category**	**Frequency (%)**
Gender	Female	128 (46.4%)
	Male	148 (53.6%)
Age	18-24 years	63 (22.8%)
(Prefer not to say: 2)	25-34 years	91 (33.0%)
	35-44 years	58 (21.0%)
	45 years and over	62 (22.5%)
Education	Junior High School or below	56 (20.3%)
(Missing, n=2)	Senior High School	47 (17.0%)
(Prefer not to say: 6)	Some Undergraduate study	62 (22.5%)
	Bachelor or above	103 (37.3%)
Health Status	Very poor	18 (6.5%)
(Missing, n=2)	Fair	20 (7.2%)
(Prefer not to say: 6)	Very good	230 (83.3%)
Health Concern	Less worried	113 (40.9%)
(Missing, n=3)	Somewhat worried	37 (13.4%)
(Prefer not to say: 9)	Extremely worried	114 (41.3%)
Computer Experience	No usage experience	59 (21.4%)
(Missing, n=1)	Below 3 years of experience	60 (21.7%)
	3 to 7 years of experience	50 (18.1%)
	Over 7 years of experience	106 (38.4%)

In general, there was much variation in the sample in terms of gender, age, education, and computer experience. The sample did not vary in terms of health status as the majority of the respondents (83.3%) rated the state of their health as very good. However, the sample was split regarding the extent to which individuals are worried about their health; 40.9% of the

respondents were less worried about their health, whereas 41.3% were extremely worried. There were 37 (13.4%) respondents who were somewhat worried.

As indicated in Table 5.1, there were some respondents who preferred not to respond to questions regarding their age, educational level, health status or degree of worry about their health. Since these respondents were quite small for each of the variables, their responses were treated as missing values in the analysis of the survey data.

The last population census in Ghana (GSS, 2012) showed that the country has a young population with 15.1% between ages 25 and 34, 13.8% between 18 and 24 years, 10.6% between 35 and 44 years, and 15.8% 45 years and older. The total population of Ghana then was a little over 24 million. Out of this 51% were females, whereas 49% were males. The sample of the study thus fairly reflect the age demographics of the Ghanaian population.

5.4 Testing for Common Method Bias

Common method bias occurs when the method of measurement introduces systematic variance into the measures or items of constructs (Doty & Glick, 1998). An example is when survey instructions influence the responses of participants in the same direction, causing the survey items to share a certain amount of common variation (Kock, 2015). Common method bias can cause the observed relationships among constructs to be different from the true relationships (Doty & Glick, 1998) and thus threatens the validity of conclusions about the relationships among the constructs (Podsakoff et al., 2003). It is thus important that appropriate measures are taken to control method biases.

In the previous chapter, it was noted that a number of survey design recommendations (e.g., assuring anonymity of respondents) were followed to reduce the negative effect of common method bias. Additionally, two statistical tests were performed to assess whether common method bias represented a serious problem in the data. First, the Harman's Single Factor test suggested by Podsakoff et al. (2003) was conducted using the statistical package for the social sciences (SPSS[2]). After performing an unrotated principal component factor analysis of all constructs, more than one factor emerged with the first (largest) factor accounting for only 19.1% of the variance in the model.

Second, the full collinearity test recommended by Kock and Lynn (2012) which can simultaneously assess both vertical collinearity and lateral collinearity was performed using both multiple regression analysis in SPSS and PLS-SEM. Regarding the test using PLS-SEM, following the suggestion in Kock and Lynn (2012), all constructs were modelled as predictors with a dummy variable used as the dependent variable. Then after running the PLS-SEM algorithm, the variance inflation factor values for the inner model was examined for collinearity problems. Similarly, multiple regression analysis was performed with latent scores of all constructs (obtained from the PLS-SEM analysis) as predictors and a dummy variable as the

[2] IBM Corp. Released 2017. IBM SPSS Statistics for Windows, Version 25.0. Armonk, NY: IBM Corp.

dependent variable. The results of the PLS-SEM estimation and multiple regression analysis showed that the variance inflation factor values ranged from 1 to 2 which is below the threshold value of 3.3 for variance-base structural equation modelling (Kock & Lynn, 2012). In both tests, education and computer experience had the highest variance inflation factor values ranging from 2.0 to 2.1.

From the results of the Harman's Single Factor test and the full collinearity test, it is concluded that common method bias is not a problem in the data. Thus, the data analysis can proceed with the evaluation of the measurement models and the structural relationships in the research model.

5.5 Analysis Strategy

This section provides details of the statistical analysis of the survey data in testing the research model proposed in this study. The main statistical technique used for data analysis is briefly introduced. Then, the various analyses performed are discussed in detail in the sub-sections of this section.

The partial least square structural equation modelling (PLS-SEM), a second-generation statistical technique, was used in the analysis of the survey data to evaluate the proposed research model. The SmartPLS 3.2.8 software package (Ringle et al., 2015) was used. As noted in Section 4.5 in Chapter 4, PLS-SEM was used in this study as it helps to analyse measurement and structural models with multi-item constructs that include direct, indirect, and interaction effects (Kim et al., 2012). Also, since the research model includes both reflective and formative constructs, PLS-SEM was deemed appropriate as it easily incorporates these constructs compared to covariance-based structural equation modelling (CB-SEM) methods (Hair et al., 2016). More importantly, PLS-SEM is generally considered more appropriate in early stages of theory development (Hair et al., 2016; Xu et al., 2009). As this study is an early attempt at developing a theoretical model to explore the factors driving the intention to disclose PHI in a digitized healthcare environment among individuals in developing countries, PLS-SEM was considered to be more suitable for this study than other methods.

As mentioned above, PLS-SEM is used to assess the measurement model (i.e., the relationship between items and constructs) as well as estimate the relationships in the structural model (i.e., the relationship among constructs). The rest of this section focuses on the evaluation of the reliability and validity of the measurement model, and the assessment of the structural model.

5.5.1 Evaluation of the Measurement Model

This section focuses on examining the reliability and validity of the measurement models in the proposed research model. The measurement model describes the relationship between latent variables or constructs and their measures or items (Hair et al., 2016). The relationship

between items and constructs can be either reflective (when the items are a reflection of the construct) or formative (when the items define the construct) (Petter et al., 2007).

As noted in the previous chapter, with the exception of trust in healthcare providers, all constructs in the proposed research model are measured reflectively. Trust in healthcare providers is conceptualized and measured as a formative second-order construct with reflective first-order constructs comprising of the three trusting beliefs identified by McKnight et al. (2002): benevolence, competence, and integrity. All the other remaining constructs are reflective first-order constructs except PHI privacy concerns for which a second-order factor structure is considered. The four dimensions of privacy concerns (i.e., collection, errors, secondary use, and unauthorised access) proposed by Smith et al. (1996) are treated as reflective first-order constructs which load onto a reflective second-order construct representing overall PHI privacy concerns.

Given that the proposed research model includes second-order constructs (which PLS-SEM does not directly support), the assessment of measurement model involved two stages following past studies (e.g., Agarwal & Karahanna, 2000; Hair et al., 2016). First, the psychometric properties of all first-order constructs were examined. Here, the second-order constructs were represented by all the items of their first-order constructs in the PLS-SEM path model. Second, the measurement models of both first-order and second-order constructs were examined. In this stage, the second-order constructs namely PHI privacy concerns and trust in healthcare providers were represented by the factor scores of their associated first-order constructs obtained from the path model analysis in the first stage. Below, the two stages of measurement model evaluation are discussed in detail.

5.5.1.1 Assessing Measurement Models of First-Order Constructs

Depending on the type of measurement model (reflective or formative), different evaluation criteria are used (Hair et al., 2016). All first-order constructs in the proposed model were measured reflectively. Consequently, the criteria recommended by Hair et al. (2016) for evaluating reflective measurement models were followed; they include convergent validity, internal consistency, and discriminant validity.

Convergent validity reflects the positive correlation of measures of the same construct (Hair et al., 2010). Convergent validity is evaluated by the outer loadings of items and the average variance extracted (AVE) (Hair et al., 2016). A common rule of thumb is that outer loadings should be 0.70 or higher and AVE should be 0.50 or higher for convergent validity to be considered acceptable (Hair et al., 2016).

From an initial estimation of a path model based on the proposed research model by running the PLS-SEM algorithm, the outer loadings of all items were equal to or above the threshold value of 0.70 with the exception of the third item of privacy experience (P_EXP3) and the first two items of employment discrimination (EMPD1 and EMPD2). P_EXP3 had a loading of

0.105 and the outer loadings of EMPD1 and EMPD2 were 0.332 and 0.237, respectively. Following the recommendations in Hair et al. (2016), P_EXP3 and EMPD2 were dropped due to their low loadings and as they contributed to low AVE values for the privacy experience (0.494) and employment discrimination (0.446) constructs, respectively. After dropping EMPD2, the outer loading of EMPD1 improved from 0.332 to 0.529. However, since its cross-loading with the construct, perceived inferiority, was higher (i.e., 0.586) and dropping it significantly improved the AVE of employment discrimination, EMPD1 was also dropped.

As indicated in Table 5.2, after dropping the above problematic items, the outer loadings and AVE values of almost all constructs' items are well above the threshold value of 0.70 for outer loadings and 0.50 for AVE. Only two items of secondary use (SU1 and SU4) had loadings equal to the critical value of 0.70. The outer loadings of items and the AVE values thus demonstrate adequate convergent validity. This suggests that both the researcher (i.e., the questionnaire designer) and the survey respondents agree on the set of items that measure (or belong to) each construct (Kock & Lynn, 2012).

Table 5.2 Construct Descriptives

Construct	**Items**	**Loadings**	**Mean (SD)**	**CR**	**CA**	**AVE**
Collection (COL) (Mean=3.36, SD=1.66)	COL1	0.87	3.12 (1.86)	0.91	0.87	0.71
	COL2	0.77	3.69 (2.01)			
	COL3	0.90	3.21 (1.94)			
	COL4	0.82	3.41 (2.01)			
Errors (ERR) (Mean=6.28, SD=0.84)	ERR1	0.81	6.19 (1.06)	0.93	0.90	0.76
	ERR2	0.88	6.28 (0.97)			
	ERR3	0.91	6.27 (0.95)			
	ERR4	0.89	6.38 (0.88)			
Secondary Use (SU) (Mean=6.01, SD=1.03)	SU1	0.70	5.47 (1.84)	0.81	0.70	0.52
	SU2	0.74	5.84 (1.61)			
	SU3	0.74	5.93 (1.57)			
	SU4	0.70	6.35 (1.12)			
Unauthorised Access (UA) (Mean=6.37, SD=0.83)	UA1	0.91	6.44 (0.88)	0.92	0.87	0.79
	UA2	0.87	6.24 (1.07)			
	UA3	0.89	6.42 (0.87)			
Benevolence (BEN) (Mean=5.16, SD=1.27	BEN1	0.86	5.23 (1.48)	0.91	0.86	0.78
	BEN2	0.91	4.93 (1.44)			
	BEN3	0.88	5.31 (1.39)			
Integrity (INTEG) (Mean=4.84, SD=1.46)	INTEG1	0.92	4.94 (1.58)	0.96	0.94	0.89
	INTEG2	0.96	4.82 (1.55)			
	INTEG3	0.94	4.77 (1.53)			
	COMP1	0.88	5.13 (1.42)	0.93	0.89	0.76

Construct	Items	Loadings	Mean (SD)	CR	CA	AVE
Competence (COMP) (Mean=5.21, SD=1.21)	COMP2	0.88	5.0 (1.41)			
	COMP3	0.90	5.19 (1.38)			
	COMP4	0.83	5.54 (1.31)			
Convenience (CONV) (Mean=5.59, SD=1.17)	CONV1	0.87	5.64 (1.37)	0.90	0.85	0.69
	CONV2	0.87	5.60 (1.41)			
	CONV3	0.82	5.57 (1.40)			
	CONV4	0.77	5.50 (1.43)			
Willingness to Disclose PHI (WILL) (Mean=5.06, SD=1.52)	WILL1	0.96	5.07 (1.59)	0.98	0.97	0.92
	WILL2	0.98	5.05 (1.58)			
	WILL3	0.97	5.07 (1.58)			
	WILL4	0.94	5.05 (1.56)			
Perceived Attitude of Health Workers (HW_ATT) (Mean=4.24, SD=1.55)	HW_ATT1	0.93	4.25 (1.69)	0.96	0.95	0.87
	HW_ATT2	0.93	3.96 (1.64)			
	HW_ATT3	0.95	4.35 (1.65)			
	HW_ATT4	0.92	4.37 (1.66)			
Perceived Effectiveness of Government Regulation (REGUL) (Mean=5.25, SD=1.45)	REGUL1	0.92	5.30 (1.60)	0.95	0.94	0.84
	REGUL2	0.90	5.28 (1.60)			
	REGUL3	0.93	5.20 (1.64)			
	REGUL4	0.92	5.23 (1.52)			
Trust in Health Information Technology (HIT) (T_HIT) (Mean=5.37, SD=1.34)	T_HIT1	0.85	5.33 (1.65)	0.90	0.84	0.76
	T_HIT2	0.88	5.38 (1.48)			
	T_HIT3	0.88	5.39 (1.51)			
Privacy Risk (RISK) (Mean=3.68, SD=1.68)	RISK1	0.88	3.42 (1.94)	0.91	0.87	0.71
	RISK2	0.86	3.86 (1.95)			
	RISK3	0.84	3.76 (2.00)			
	RISK4	0.79	3.76 (2.01)			
Employment Discrimination (EMPD) (Mean=4.71, SD=1.89)	EMPD3	0.96	4.63 (1.96)	0.95	0.90	0.91
	EMPD4	0.95	4.80 (2.00)			
Family Rejection (FAMR) (Mean=3.81, SD=1.97)	FAMR1	0.98	3.66 (2.11)	0.88	0.79	0.79
	FAMR2	0.79	4.30 (2.08)			
Perceived Inferiority (INFE) (Mean=5.43, SD=1.38)	INFE1	0.73	5.59 (1.53)	0.92	0.89	0.69
	INFE2	0.85	5.73 (1.46)			
	INFE3	0.88	5.61 (1.60)			
	INFE4	0.84	4.95 (1.86)			
	INFE5	0.83	5.29 (1.75)			
	ORIENT1	0.92	5.89 (1.38)	0.95	0.93	0.83

Construct	Items	Loadings	Mean (SD)	CR	CA	AVE
Privacy Orientation (ORIENT) (Mean=5.94, SD=1.22)	ORIENT2	0.93	5.94 (1.32)			
	ORIENT3	0.94	5.95 (1.32)			
	ORIENT4	0.83	5.97 (1.35)			
Privacy Experience (P_EXP) (Mean=2.61, SD=1.51)	P_EXP1	0.88	2.93 (1.76)	0.90	0.78	0.82
	P_EXP2	0.92	2.37 (1.61)			

***Key: SD**: Standard Deviation; **CR**: Composite Reliability; **CA**: Cronbach's Alpha; **AVE**: Average Variance Extracted*

The next criterion for assessing the measurement model is internal consistency reliability. For acceptable internal consistency reliability, a set of items must represent the same underlying construct. Internal consistency reliability is measured by composite reliability (CR) and Cronbach's alpha (CA). The coefficients of both CR and CA should be 0.70 or higher for internal consistency reliability to be considered acceptable. The results in Table 5.2 show high internal consistency reliability for the measurement items of all constructs with most CR and CA values considerably above 0.70. This indicates that the survey respondents agree on the meaning of each set of items belonging to each construct (Kock & Lynn, 2012).

The last criterion for assessing a reflective measurement model is discriminant validity. Discriminant validity reflects the extent to which a given construct is different from other constructs (Hair, Black, Babin, & Anderson, 2010; Hair et al., 2016). Discriminant validity is achieved when the items associated with a particular construct and are not associated with other constructs (Kock & Lynn, 2012). The dominant approaches for assessing discriminant validity have been the examination of cross-loadings and the Fornell-Larcker criterion (Hair et al., 2016; Henseler, Ringle, & Sarstedt, 2015). The cross-loadings criterion states that loadings of items on their respective constructs should be higher than their loadings on any other constructs (Chin, 1998). The items loadings and cross-loadings provided in Table 5.3 provide initial support for discriminant validity as items loaded high on their constructs than their cross-loadings with other constructs.

According to the Fornell-Larcker criterion, the square roots of average variances extracted (AVE) for any construct must be greater than the correlations shared between the construct and other constructs (Barclay, Higgins, & Thompson, 1995; Fornell & Larcker, 1981). This criterion is fulfilled as in Table 5.4, the diagonal values representing the square roots of the AVE of constructs are greater than the off-diagonal elements in the corresponding rows and columns which represent the correlations shared between constructs.

Recently, Henseler et al. (2015) examining the performance of cross-loadings and the Fornell-Larcker criterion found that neither approach is reliable in detecting discriminant validity problems. Specifically, the authors observed that when there is a perfect correlation between two constructs, cross-loadings fail to detect lack of discriminant validity. Similarly, when there are small variations in the item loadings of constructs, the Fornell-Larcker criterion performs poorly in detecting discriminant validity. To address the limitations of the traditional approaches, several researchers have recommended examining the heterotrait-monotrait ratio

(HTMT) of the correlations as a new approach for assessing discriminant validity in variance-based SEM (e.g., Hair et al., 2016; Henseler et al., 2015).

HTMT is an "estimate of what the true correlation between constructs would be if they were perfectly measured" (Hair et al., 2016). If the true correlation between two constructs is close to 1 there is lack of discriminant validity between the constructs. However, when constructs are conceptually similar, a threshold value of 0.90 has been suggested and when constructs are conceptually more distinct, a lower and more conservative threshold value of 0.85 is suggested (Hair et al., 2016; Henseler et al., 2015). Table 5.5 shows the HTMT values for all pairs of constructs. As evident, all HTMT values are lower than the conservative threshold value of 0.85. Only the HTMT value for the errors and unauthorised access dimensions of PHI privacy concerns (i.e., 0.834) was close to the threshold value of 0.85. The high HTMT value, however, is not surprising as the four dimensions of privacy concerns (collection, errors, secondary use, and unauthorised access) are interrelated with individuals' concerns about lack of control over their personal information being suggested as explaining the interrelationship between the dimensions (Stewart & Segars, 2002). In general, the HTMT values of the constructs further provide strong evidence of discriminant validity.

In addition to examining the HTMT ratios, Hair et al. (2016) have recommended testing whether the HTMT values are significantly different from 1 by computing bootstrap confidence intervals. If the HTMT confidence interval does not include 1 then discriminant validity is established (Hair et al., 2016). After running the bootstrapping procedure in SmartPLS, the lower and upper bounds of the confidence intervals of HTMT for the relationship between the constructs did not include the value of 1, an indication of discriminant validity of the reflective constructs.

Summing up, all the criteria for assessing a reflective measurement model were adequately met which demonstrates the reliability and validity of the measures of the reflective first-order constructs. Specifically, the constructs' items had high outer loadings (>= 0.70) and average variances extracted (AVE) values (>= 0.50) fulfilling the requirements for convergent validity. Internal consistency reliability was also achieved as the composite reliability (CR) and Cronbach's alpha (CA) values for all constructs were well above the threshold of 0.70 with the exception of secondary use, which had CA value of 0.70. Lastly, discriminant validity was observed as: (1) items loaded more strongly on their respective constructs than on other constructs (Cross-Loadings approach), and (2) all constructs shared more variance with their items than with other constructs (Fornell-Larcker criterion). In addition to the traditional approaches to assessing discriminant validity, the recently proposed HTMT approach similarly confirmed that the reflective constructs discriminate well; HTMT values were below the threshold value of 0.85 and HTMT confidence interval did not include the value of 1.

The next section continues the measurement model evaluation with a particular focus on second-order constructs which will be represented by the factor scores of their associated first-order constructs obtained from the above assessment of measurement models of first-order constructs.

Table 5.3 Loadings and Cross-Loadings: First-Order Constructs

	BEN	COL	COMP	CONV	EMPD	ERR	FAMR	HW_ATT	INFE	INTEG	ORIENT	P_EXP	REGUL	RISK	SU	T_HIT	UA	WILL
BEN1	**0.86**	-0.07	0.51	0.24	0.08	0.21	-0.04	0.43	0.02	0.51	0.04	-0.07	0.19	0.02	0.20	0.19	0.20	0.08
BEN2	**0.91**	-0.04	0.54	0.20	0.07	0.14	-0.08	0.44	0.00	0.59	0.06	0.00	0.22	0.09	0.11	0.27	0.10	0.17
BEN3	**0.88**	-0.06	0.62	0.28	0.02	0.27	-0.15	0.50	-0.05	0.58	0.19	-0.09	0.34	-0.01	0.17	0.32	0.22	0.22
COL1	-0.07	**0.87**	-0.16	-0.06	0.09	-0.17	0.15	-0.13	0.08	-0.05	-0.09	0.38	-0.11	0.26	-0.03	-0.16	-0.15	-0.42
COL2	-0.08	**0.77**	-0.15	-0.05	-0.02	-0.06	0.06	-0.10	0.04	-0.06	-0.04	0.28	-0.09	0.29	0.09	-0.16	-0.02	-0.34
COL3	-0.04	**0.90**	-0.17	-0.09	0.09	-0.19	0.15	-0.10	0.08	-0.06	-0.07	0.36	-0.05	0.25	0.01	-0.15	-0.15	-0.35
COL4	-0.04	**0.82**	-0.12	0.02	0.11	-0.17	0.20	-0.06	0.17	-0.03	-0.01	0.34	-0.02	0.13	0.02	-0.11	-0.11	-0.33
COMP1	0.62	-0.17	**0.88**	0.25	-0.05	0.22	-0.09	0.49	-0.06	0.60	0.15	-0.13	0.25	-0.05	0.09	0.29	0.18	0.30
COMP2	0.60	-0.13	**0.88**	0.23	-0.04	0.20	-0.04	0.48	-0.02	0.56	0.08	-0.09	0.23	-0.09	0.12	0.24	0.14	0.18
COMP3	0.53	-0.16	**0.90**	0.20	-0.07	0.20	-0.11	0.43	-0.01	0.49	0.15	-0.09	0.24	-0.07	0.08	0.24	0.13	0.18
COMP4	0.44	-0.18	**0.83**	0.24	-0.04	0.35	-0.14	0.39	0.02	0.41	0.30	-0.18	0.27	-0.13	0.12	0.35	0.27	0.24
CONV1	0.15	-0.07	0.21	**0.87**	-0.07	0.23	-0.09	0.13	0.07	0.14	0.37	-0.16	0.24	-0.19	0.21	0.39	0.25	0.36
CONV2	0.26	-0.06	0.25	**0.87**	0.00	0.22	-0.04	0.16	0.14	0.23	0.35	-0.10	0.31	-0.16	0.17	0.41	0.25	0.30
CONV3	0.29	-0.03	0.25	**0.82**	-0.03	0.28	-0.09	0.22	0.11	0.26	0.27	-0.12	0.30	-0.14	0.23	0.37	0.30	0.28
CONV4	0.23	-0.01	0.15	**0.77**	0.02	0.24	0.04	0.16	0.09	0.20	0.25	-0.10	0.17	-0.13	0.18	0.29	0.29	0.25
EMPD3	0.07	0.09	-0.06	-0.02	**0.96**	0.02	0.43	-0.04	0.47	0.07	-0.10	0.12	0.00	0.16	0.07	-0.03	0.09	-0.09
EMPD4	0.05	0.09	-0.05	-0.04	**0.95**	0.02	0.44	-0.07	0.47	0.11	-0.14	0.13	-0.04	0.21	0.07	-0.10	0.06	-0.09
ERR1	0.20	-0.12	0.24	0.22	0.02	**0.81**	-0.17	0.19	0.17	0.16	0.32	-0.21	0.16	-0.09	0.43	0.25	0.59	0.15
ERR2	0.25	-0.20	0.23	0.22	0.04	**0.88**	-0.24	0.17	0.14	0.17	0.32	-0.22	0.18	-0.15	0.44	0.28	0.67	0.19
ERR3	0.15	-0.17	0.24	0.30	0.02	**0.91**	-0.19	0.09	0.17	0.13	0.37	-0.26	0.21	-0.11	0.45	0.27	0.65	0.21
ERR4	0.23	-0.16	0.25	0.26	-0.01	**0.89**	-0.21	0.14	0.13	0.14	0.36	-0.20	0.20	-0.12	0.36	0.34	0.66	0.24
FAMR1	-0.10	0.20	-0.13	-0.06	0.45	-0.24	**0.98**	-0.18	0.38	-0.05	-0.26	0.26	-0.11	0.12	-0.04	-0.22	-0.21	-0.16
FAMR2	-0.07	0.05	-0.01	-0.03	0.37	-0.12	**0.79**	-0.12	0.47	-0.05	-0.10	0.14	-0.01	0.05	-0.09	-0.07	-0.08	-0.05
HW_ATT1	0.46	-0.11	0.48	0.20	-0.05	0.16	-0.16	**0.93**	-0.10	0.42	0.12	-0.07	0.22	-0.05	0.11	0.25	0.21	0.16
HW_ATT2	0.43	-0.13	0.45	0.16	-0.09	0.12	-0.15	**0.93**	-0.15	0.42	0.06	-0.12	0.13	-0.05	0.09	0.20	0.16	0.18
HW_ATT3	0.51	-0.11	0.48	0.17	-0.06	0.16	-0.18	**0.95**	-0.17	0.44	0.10	-0.09	0.18	0.01	0.07	0.24	0.18	0.19

	BEN	COL	COMP	CONV	EMPD	ERR	FAMR	HW_ATT	INFE	INTEG	ORIENT	P_EXP	REGUL	RISK	SU	T_HIT	UA	WILL
HW_ATT4	0.51	-0.08	0.50	0.20	-0.01	0.18	-0.17	**0.92**	-0.15	0.50	0.10	-0.10	0.20	0.00	0.10	0.26	0.18	0.21
INFE1	-0.04	0.06	0.01	0.07	0.32	0.15	0.22	-0.11	**0.73**	0.01	0.08	0.01	0.01	-0.03	0.17	0.08	0.18	-0.02
INFE2	-0.01	0.13	0.01	0.11	0.35	0.15	0.23	-0.12	**0.85**	-0.02	0.10	0.07	0.02	0.01	0.18	0.03	0.21	-0.11
INFE3	-0.07	0.06	-0.09	0.10	0.42	0.18	0.32	-0.14	**0.88**	-0.03	0.10	0.06	0.03	0.01	0.19	0.05	0.17	-0.07
INFE4	-0.01	0.12	-0.04	0.10	0.48	0.10	0.48	-0.16	**0.84**	0.04	-0.03	0.10	-0.01	0.02	0.16	-0.06	0.08	-0.11
INFE5	0.08	0.04	0.06	0.11	0.45	0.17	0.46	-0.10	**0.83**	0.06	0.04	0.05	0.07	0.00	0.15	0.01	0.11	-0.07
INTEG1	0.62	-0.05	0.55	0.23	0.10	0.12	-0.05	0.44	0.01	**0.92**	0.06	-0.06	0.22	-0.01	0.18	0.26	0.15	0.17
INTEG2	0.59	-0.06	0.56	0.24	0.07	0.20	-0.06	0.45	0.01	**0.96**	0.06	-0.01	0.19	-0.02	0.16	0.27	0.20	0.18
INTEG3	0.58	-0.04	0.58	0.22	0.08	0.17	-0.04	0.47	0.01	**0.94**	0.04	-0.02	0.22	-0.03	0.17	0.26	0.17	0.16
ORIENT1	0.13	-0.07	0.17	0.43	-0.14	0.38	-0.21	0.09	0.03	0.07	**0.92**	-0.07	0.36	-0.21	0.16	0.29	0.31	0.23
ORIENT2	0.10	-0.03	0.19	0.36	-0.10	0.33	-0.22	0.10	0.09	0.06	**0.93**	0.00	0.35	-0.22	0.10	0.34	0.27	0.23
ORIENT3	0.12	-0.08	0.18	0.37	-0.15	0.40	-0.25	0.08	0.04	0.03	**0.94**	-0.11	0.35	-0.20	0.16	0.28	0.32	0.25
ORIENT4	0.05	-0.06	0.14	0.20	-0.05	0.32	-0.18	0.10	0.07	0.05	**0.83**	0.00	0.31	-0.12	0.09	0.21	0.20	0.19
P_EXP1	-0.06	0.40	-0.10	-0.13	0.12	-0.15	0.18	-0.11	0.08	-0.04	0.02	**0.88**	-0.04	0.21	-0.15	-0.12	-0.15	-0.13
P_EXP2	-0.05	0.34	-0.15	-0.14	0.12	-0.29	0.26	-0.08	0.07	-0.02	-0.10	**0.92**	-0.06	0.19	-0.22	-0.15	-0.29	-0.16
REGUL1	0.27	-0.05	0.24	0.28	0.01	0.24	-0.06	0.15	0.06	0.19	0.35	-0.06	**0.92**	-0.10	0.13	0.32	0.24	0.20
REGUL2	0.26	-0.05	0.26	0.27	0.02	0.17	-0.07	0.21	0.04	0.24	0.36	-0.02	**0.90**	-0.08	0.09	0.27	0.21	0.20
REGUL3	0.26	-0.08	0.27	0.29	-0.07	0.18	-0.10	0.19	0.01	0.20	0.34	-0.07	**0.93**	-0.10	0.12	0.24	0.21	0.26
REGUL4	0.26	-0.12	0.28	0.29	-0.04	0.18	-0.10	0.18	-0.02	0.19	0.33	-0.06	**0.92**	-0.10	0.09	0.26	0.21	0.25
RISK1	0.06	0.26	-0.08	-0.18	0.21	-0.13	0.15	0.00	0.01	0.01	-0.20	0.22	-0.06	**0.88**	0.00	-0.42	-0.09	-0.22
RISK2	0.05	0.22	-0.06	-0.11	0.16	-0.08	0.07	-0.02	0.03	0.01	-0.15	0.21	-0.08	**0.86**	-0.06	-0.36	-0.08	-0.19
RISK3	-0.01	0.21	-0.14	-0.18	0.11	-0.14	0.09	-0.05	-0.04	-0.09	-0.19	0.19	-0.16	**0.84**	-0.01	-0.34	-0.10	-0.15
RISK4	0.02	0.21	-0.03	-0.17	0.15	-0.09	0.05	-0.01	0.03	-0.01	-0.16	0.10	-0.06	**0.79**	0.01	-0.27	-0.06	-0.12
SU1	0.09	0.14	0.00	0.07	0.17	0.22	0.02	0.04	0.11	0.10	-0.02	-0.11	0.00	0.06	**0.70**	-0.03	0.26	0.11
SU2	0.11	-0.02	0.08	0.15	0.01	0.32	-0.10	0.08	0.16	0.09	0.08	-0.15	-0.03	-0.05	**0.74**	0.09	0.33	0.19
SU3	0.03	0.05	0.02	0.09	0.04	0.28	0.03	-0.05	0.15	0.02	0.04	-0.15	0.06	0.03	**0.74**	0.11	0.27	0.13
SU4	0.24	-0.07	0.18	0.31	0.02	0.48	-0.07	0.17	0.15	0.25	0.24	-0.16	0.24	-0.05	**0.70**	0.20	0.45	0.22
T_HIT1	0.21	-0.18	0.19	0.30	-0.08	0.31	-0.22	0.22	-0.04	0.14	0.26	-0.14	0.25	-0.41	0.08	**0.85**	0.24	0.41

	BEN	COL	COMP	CONV	EMPD	ERR	FAMR	HW_ATT	INFE	INTEG	ORIENT	P_EXP	REGUL	RISK	SU	T_HIT	UA	WILL
T_HIT2	0.29	-0.11	0.25	0.44	-0.04	0.29	-0.17	0.20	0.01	0.27	0.24	-0.14	0.19	-0.34	0.19	**0.88**	0.30	0.39
T_HIT3	0.29	-0.15	0.40	0.42	-0.05	0.26	-0.12	0.25	0.05	0.32	0.30	-0.12	0.35	-0.35	0.13	**0.88**	0.23	0.34
UA1	0.20	-0.12	0.17	0.31	0.10	0.66	-0.16	0.22	0.16	0.20	0.28	-0.24	0.21	-0.10	0.47	0.31	**0.91**	0.24
UA2	0.15	-0.12	0.18	0.25	0.04	0.63	-0.16	0.16	0.20	0.13	0.25	-0.19	0.19	-0.08	0.43	0.19	**0.87**	0.19
UA3	0.16	-0.14	0.19	0.30	0.07	0.68	-0.20	0.14	0.10	0.16	0.29	-0.23	0.25	-0.08	0.39	0.28	**0.89**	0.23
WILL1	0.17	-0.39	0.24	0.35	-0.10	0.20	-0.13	0.17	-0.12	0.19	0.21	-0.15	0.23	-0.14	0.24	0.38	0.21	**0.96**
WILL2	0.18	-0.42	0.27	0.36	-0.09	0.24	-0.15	0.22	-0.09	0.19	0.26	-0.17	0.25	-0.22	0.22	0.43	0.26	**0.98**
WILL3	0.17	-0.44	0.25	0.39	-0.10	0.23	-0.13	0.20	-0.11	0.17	0.23	-0.18	0.26	-0.25	0.22	0.46	0.23	**0.97**
WILL4	0.17	-0.38	0.23	0.30	-0.07	0.20	-0.13	0.17	-0.10	0.15	0.27	-0.13	0.20	-0.17	0.24	0.39	0.24	**0.94**

Key: *Benevolence (BEN); Collection (COL); Competence (COMP); Convenience (CONV); Employment Discrimination (EMPD); Errors (ERR); Family Rejection (FAMR); Perceived Attitude of Health Workers (HW_ATT); Perceived Inferiority (INFE); Integrity (INTEG); Privacy Orientation (ORIENT); Privacy Experience (P_EXP); Perceived Effectiveness of Government Regulation (REGUL); Privacy Risk (RISK); Secondary Use (SU); Trust in Health Information Technology (T_HIT); Unauthorised Access (UA); Willingness to Disclose PHI (WILL).*

Note: Regarding control variables, only multi-item constructs, ORIENT (privacy orientation) and P_EXP (privacy experience), were included. The remaining control variables were excluded due to space limitations. The same applies to Tables 5.4 and 5.5.

Table 5.4 Interconstruct Correlations: First-order Constructs

	BEN	COL	COMP	CONV	EMPD	ERR	FAMR	HW_ATT	INFE	INTEG	ORIENT	P_EXP	REGUL	RISK	SU	T_HIT	UA	WILL
BEN	**0.88**																	
COL	-0.06	**0.84**																
COMP	0.64	-0.18	**0.87**															
CONV	0.27	-0.05	0.26	**0.83**														
EMPD	0.06	0.09	-0.06	-0.03	**0.96**													
ERR	0.24	-0.19	0.27	0.29	0.02	**0.87**												
FAMR	-0.10	0.18	-0.11	-0.06	0.46	-0.23	**0.89**											
HW_ATT	0.52	-0.11	0.51	0.20	-0.06	0.17	-0.18	**0.93**										
INFE	-0.01	0.11	-0.02	0.12	0.50	0.17	0.43	-0.15	**0.83**									
INTEG	0.63	-0.06	0.60	0.25	0.09	0.17	-0.05	0.48	0.01	**0.94**								
ORIENT	0.11	-0.07	0.19	0.38	-0.12	0.39	-0.24	0.10	0.06	0.06	**0.91**							
P_EXP	-0.06	0.41	-0.14	-0.15	0.13	-0.25	0.25	-0.10	0.08	-0.03	-0.05	**0.90**						
REGUL	0.29	-0.08	0.28	0.31	-0.02	0.21	-0.09	0.20	0.03	0.22	0.38	-0.06	**0.92**					
RISK	0.04	0.26	-0.09	-0.19	0.19	-0.13	0.11	-0.02	0.01	-0.02	-0.21	0.22	-0.10	**0.85**				
SU	0.18	0.01	0.12	0.24	0.07	0.48	-0.05	0.10	0.20	0.18	0.14	-0.21	0.12	-0.02	**0.72**			
T_HIT	0.30	-0.17	0.32	0.44	-0.06	0.33	-0.19	0.26	0.01	0.28	0.31	-0.15	0.30	-0.42	0.15	**0.87**		
UA	0.19	-0.14	0.20	0.32	0.08	0.74	-0.19	0.20	0.17	0.19	0.31	-0.25	0.24	-0.10	0.48	0.29	**0.89**	
WILL	0.18	-0.43	0.26	0.36	-0.10	0.23	-0.14	0.20	-0.11	0.18	0.25	-0.16	0.25	-0.21	0.24	0.44	0.24	**0.96**

Key: *Benevolence (BEN); Collection (COL); Competence (COMP); Convenience (CONV); Employment Discrimination (EMPD); Errors (ERR); Family Rejection (FAMR); Perceived Attitude of Health Workers (HW_ATT); Perceived Inferiority (INFE); Integrity (INTEG); Privacy Orientation (ORIENT); Privacy Experience (P_EXP); Perceived Effectiveness of Government Regulation (REGUL); Privacy Risk (RISK); Secondary Use (SU); Trust in Health Information Technology (T_HIT); Unauthorised Access (UA); Willingness to Disclose PHI (WILL).*

Note: *Diagonal elements are the square root of Average Variance Extracted (AVE)*

Table 5.5 Heterotrait-Monotrait Ratio (HTMT): First-Order Constructs

	BEN	COL	COMP	CONV	EMPD	ERR	FAMR	HW_ATT	INFE	INTEG	ORIENT	P_EXP	REGUL	RISK	SU	T_HIT	UA	WILL
BEN																		
COL	0.078																	
COMP	0.717	0.205																
CONV	0.327	0.074	0.301															
EMPD	0.073	0.106	0.063	0.046														
ERR	0.270	0.197	0.314	0.333	0.026													
FAMR	0.115	0.161	0.101	0.086	0.528	0.238												
HW_ATT	0.569	0.126	0.555	0.223	0.065	0.180	0.189											
INFE	0.072	0.110	0.079	0.143	0.542	0.205	0.535	0.161										
INTEG	0.704	0.063	0.650	0.283	0.100	0.188	0.062	0.509	0.041									
ORIENT	0.122	0.078	0.213	0.414	0.131	0.431	0.233	0.108	0.094	0.062								
P_EXP	0.085	0.495	0.168	0.180	0.156	0.296	0.275	0.121	0.090	0.042	0.093							
REGUL	0.315	0.093	0.312	0.345	0.046	0.233	0.081	0.209	0.046	0.239	0.405	0.069						
RISK	0.065	0.313	0.113	0.219	0.213	0.148	0.108	0.048	0.057	0.049	0.230	0.259	0.116					
SU	0.216	0.144	0.132	0.277	0.116	0.570	0.119	0.144	0.254	0.198	0.165	0.266	0.151	0.097				
T_HIT	0.351	0.201	0.372	0.518	0.074	0.378	0.196	0.285	0.069	0.317	0.348	0.188	0.335	0.481	0.208			
UA	0.223	0.147	0.233	0.380	0.086	0.834	0.192	0.215	0.201	0.204	0.336	0.292	0.264	0.111	0.587	0.341		
WILL	0.194	0.464	0.278	0.393	0.101	0.245	0.129	0.206	0.097	0.191	0.265	0.184	0.257	0.219	0.279	0.480	0.264	

Key: *Benevolence (BEN); Collection (COL); Competence (COMP); Convenience (CONV); Employment Discrimination (EMPD); Errors (ERR); Family Rejection (FAMR); Perceived Attitude of Health Workers (HW_ATT); Perceived Inferiority (INFE); Integrity (INTEG); Privacy Orientation (ORIENT); Privacy Experience (P_EXP); Perceived Effectiveness of Government Regulation (REGUL); Privacy Risk (RISK); Secondary Use (SU); Trust in Health Information Technology (T_HIT); Unauthorised Access (UA); Willingness to Disclose PHI (WILL).*

5.5.1.2 Assessing Measurement Models of First- and Second-order Constructs

As noted earlier in the introduction of Section 5.5.1, the research model proposed in this study includes two multi-dimensional constructs namely PHI privacy concerns and trust in healthcare providers which are operationalized as second-order constructs. PHI privacy concerns is conceptualized and measured as a reflective second-order construct with reflective first-order constructs comprising of the four dimensions of privacy concerns: collection, errors, secondary use, and unauthorised access. On the other hand, trust in healthcare providers is a formative second-order construct with reflective first-order constructs comprising of the benevolence, competency, and integrity trusting beliefs.

Following recommendations in existing studies (e.g., Agarwal & Karahanna, 2000; Hair et al., 2016), a two-stage approach was followed in the PLS-SEM path model analysis. The previous section discussed the first stage of the analysis which focused on the assessment of the measurement models of first-order constructs. In this stage, the second-order constructs were represented by all the items of their first-order constructs and hence were not examined for their reliability and validity.

In the second stage of the analysis, second-order constructs were represented by the factor scores of their associated first-order constructs obtained from the path model analysis in the first stage. Specifically, the four dimensions of privacy concerns (collection, errors, secondary use, and unauthorised access) represented by their factor scores were modelled as reflective items of PHI privacy concerns, whereas the trusting beliefs of benevolence, competence, and integrity were modelled as formative items of trust in healthcare providers. Thus, a reduced path model was considered in the second stage of analysis as the measurement models of the first-order constructs associated with the second-order constructs (i.e., PHI privacy concerns and trust in healthcare providers) were excluded from the path model.

According to Hair et al. (2016), the addition or elimination of certain items or constructs impact on path model estimates. In particular, the assessment of cross-loadings and the Fornell-Larcker criterion can be different when additional constructs are added to or eliminated from a model (Hair et al., 2016). Since a reduced path model was considered in the second stage of the PLS-SEM path model analysis, this section reassesses the measurement models of the constructs in the path model prior to evaluating the structural model. As different criteria are applied in evaluating reflective and formative measurement models, the evaluation of the reflective and formative measurement models is discussed separately.

Reflective Measurement Model Evaluation

The criteria for evaluating reflective measurement models were discussed in the earlier assessment of measurement models of first-order constructs. They include convergent validity, internal consistency reliability, and discriminant validity.

The estimation of the reduced path model using the PLS-SEM algorithm found that the measures of convergent validity (i.e., outer loadings and average variances extracted (AVE) values) for all first-order constructs were the same as reported in Table 5.2. Similarly, the internal consistency reliability measures of composite reliability (CR) and Cronbach's alpha (CA) for the first-order constructs were the same as reported in Table 5.2. Thus, the measurement models of the first-order constructs in the reduced path model fulfilled the criteria for convergent validity and internal consistency reliability.

Table 5.6 provides the descriptive statistics of the second-order construct, PHI privacy concerns. As evident, the collection dimension loaded negatively, whereas the other three dimensions (errors, secondary use, and unauthorised access) had positive loadings on PHI privacy concerns. The AVE value was 0.506, marginally above the critical value of 0.50. The requirements for convergent validity was thus not adequately fulfilled. Similarly, internal consistency reliability was not achieved as the CR and CA values of the four dimensions were below the critical value of 0.70.

Table 5.6 PHI Privacy Concerns - Descriptives

Construct	**Dimensions/Items**	**Outer Loadings**	**CR**	**CA**	**AVE**
PHI Privacy Concerns	Collection (COL)	-0.57	0.586	0.545	0.506
	Errors (ERR)	0.83			
	Secondary Use (SU)	0.60			
	Unauthorised Access (UA)	0.81			

The loadings and cross-loadings of all constructs are provided in Table 5.7. All measurement items fulfilled the cross-loadings requirement for discriminant validity except the collection (COL) dimension of PHI privacy concerns which loaded more strongly on other constructs (e.g., privacy risk) than on its construct. However, all constructs shared more variance with their items than with other constructs fulfilling the Fornell-Larcker criterion (see Table 5.8). Similarly, as indicated in Table 5.9, the heterotrait-monotrait ratio (HTMT) values for all pairs of constructs are lower than the threshold value of 0.85 indicating further the discriminant validity of the constructs.

In general, the second-order construct, PHI privacy concerns, did not adequately meet the convergent validity and internal consistency reliability criteria for evaluating reflective measurement models due to the negative loading of the collection dimension. When collection is dropped, the outer loadings of the remaining dimensions are above the threshold of 0.70. Similarly, the values of CR, CA, and AVE significantly improve to 0.88, 0.80, and 0.713, respectively. However, the outer loading of the collection dimension is statistically highly significant at 0.1% level; this indicates that the collection dimension makes absolute contribution to the PHI privacy concerns construct (Hair et al., 2016). Further, collection is a necessary antecedent to the other three dimensions namely errors, secondary use, and unauthorised access (Hong & Thong, 2013), and in some studies, it is considered as one of the most important dimensions of information privacy (e.g., Hann et al., 2007). Therefore, since

dropping the collection dimension affects the content validity of the PHI privacy concerns construct, to obtain a broader domain of the construct collection was maintained.

Formative Measurement Model Evaluation

This section examines the measurement model of the formative second-order construct, trust in healthcare providers, which has benevolence, competence, and integrity as first-order constructs. Two criteria suggested by Hair et al. (2016) were used to assess the formative model of trust in healthcare providers: collinearity assessment and outer weights significance testing.

Collinearity (or multicollinearity) refers to high correlations between two formative items (Hair et al., 2016). Whereas high correlations between items are required in reflective measurement models, they are not expected in formative measurement models (Petter et al., 2007). According to Hair et al. (2016), high levels of collinearity between formative items can increase standard errors and thereby reduce the ability to detect the significance of outer weights of items. Additionally, it can result in wrong estimations of weights and the reversal of their signs. It is thus important to assess and address collinearity issues in formative measurement models.

An important measure of collinearity is the variance inflation factor (VIF). In the context of PLS-SEM, a VIF value of 5 or higher is an indication of collinearity problem (Hair et al., 2016). As evident in Table 5.10, the VIF values of the dimensions of trust in healthcare providers are considerably lower than the threshold of 5 demonstrating that no collinearity exists between the dimensions.

In addition to collinearity assessment, the significance of outer weights of formative items must be analysed. The outer weight of an item reflects the item's relative contribution to the construct it is associated with. If the outer weight is significantly different from zero, it means that the formative item truly contributes to forming the construct (Hair et al., 2016). The outer weights of the dimensions of trust in healthcare providers obtained by running the bootstrapping procedure in SmartPLS 3.2.8 are provided in Table 5.10. Only the weight of the integrity dimension was not significant at $p \leq 0.05$ (but was significant at $p \leq 0.10$).

According to Hair et al. (2016), when the weight of a formative item is insignificant, the item's absolute contribution to (or absolute importance for) its construct must be considered. The absolute contribution of an item is the information the item provides in forming its construct without considering any other items of the construct. An item's absolute contribution depends on the value of its outer loading. Hair et al. (2016) maintain that when an item's weight is insignificant, but its outer loading is high (i.e., above 0.50), the item should be retained as it is absolutely important. The results in Table 5.10 show that the integrity dimension is absolutely important whereas benevolence and competence are both relatively and absolutely important. The above assessment thus demonstrates good formative measurement model quality.

Table 5.7 Loadings and Cross-Loadings: First- and Second-order Constructs

	AGE	COMP-_EXP	*PHIPC*	CONV	EMPD	EDUC	FAMR	GEN-DER	HW-_ATT	HCONC	INFE	ORIENT	P_EXP	REGUL	RISK	T_HIT	*T_PROV*	WILL
AGE	**1.00**	-0.26	0.09	-0.04	-0.12	-0.12	-0.13	0.02	0.05	0.16	-0.03	0.00	-0.04	0.02	0.11	-0.05	0.16	0.04
COMP_EXP	-0.26	**1.00**	0.04	0.04	-0.04	0.66	-0.17	0.17	0.03	0.00	-0.11	0.29	0.04	0.18	-0.16	0.25	-0.09	0.23
COL	-0.13	0.01	**-0.57**	-0.05	0.09	-0.03	0.18	0.14	-0.11	0.07	0.11	-0.07	0.41	-0.08	0.26	-0.17	-0.14	-0.43
ERR	0.01	0.08	**0.83**	0.29	0.02	0.06	-0.23	-0.01	0.17	0.09	0.17	0.39	-0.25	0.21	-0.13	0.33	0.28	0.23
SU	0.10	-0.07	**0.60**	0.24	0.07	-0.02	-0.05	0.05	0.10	0.17	0.20	0.14	-0.21	0.12	-0.02	0.15	0.17	0.24
UA	0.00	0.10	**0.81**	0.32	0.08	0.09	-0.19	0.02	0.20	0.13	0.17	0.31	-0.25	0.24	-0.10	0.29	0.22	0.24
CONV1	-0.02	0.06	0.26	**0.87**	-0.07	0.08	-0.09	0.06	0.13	0.04	0.07	0.37	-0.16	0.24	-0.19	0.39	0.20	0.36
CONV2	0.00	0.05	0.24	**0.87**	0.00	0.14	-0.04	0.13	0.16	0.08	0.14	0.35	-0.10	0.31	-0.16	0.41	0.29	0.30
CONV3	-0.05	0.03	0.28	**0.82**	-0.03	0.13	-0.09	-0.05	0.22	0.08	0.11	0.27	-0.12	0.30	-0.14	0.37	0.30	0.28
CONV4	-0.06	-0.02	0.24	**0.77**	0.02	0.04	0.04	-0.07	0.16	0.12	0.09	0.25	-0.10	0.17	-0.13	0.29	0.21	0.25
EMPD3	-0.13	0.02	0.02	-0.02	**0.96**	0.01	0.43	-0.01	-0.04	-0.14	0.47	-0.10	0.12	0.00	0.16	-0.03	0.00	-0.09
EMPD4	-0.11	-0.10	0.00	-0.04	**0.95**	-0.09	0.44	0.00	-0.07	-0.13	0.47	-0.14	0.13	-0.04	0.21	-0.10	0.02	-0.09
EDUC	-0.12	0.66	0.06	0.12	-0.04	**1.00**	-0.16	0.15	0.06	0.00	-0.12	0.26	0.07	0.16	-0.16	0.22	-0.05	0.21
FAMR1	-0.14	-0.17	-0.26	-0.06	0.45	-0.15	**0.98**	-0.08	-0.18	-0.13	0.38	-0.26	0.26	-0.11	0.12	-0.22	-0.12	-0.16
FAMR2	-0.05	-0.11	-0.12	-0.03	0.37	-0.12	**0.79**	-0.11	-0.12	-0.05	0.47	-0.10	0.14	-0.01	0.05	-0.07	-0.04	-0.05
GENDER	0.02	0.17	-0.05	0.03	-0.01	0.15	-0.09	**1.00**	-0.04	0.02	0.03	0.05	0.05	0.07	-0.07	0.07	0.00	-0.05
HW_ATT1	0.06	0.04	0.21	0.20	-0.05	0.10	-0.16	-0.01	**0.93**	0.18	-0.10	0.12	-0.07	0.22	-0.05	0.25	0.53	0.16
HW_ATT2	0.08	-0.03	0.18	0.16	-0.09	-0.02	-0.15	-0.04	**0.93**	0.18	-0.15	0.06	-0.12	0.13	-0.05	0.20	0.50	0.18
HW_ATT3	0.04	0.07	0.19	0.17	-0.06	0.07	-0.18	-0.09	**0.95**	0.18	-0.17	0.10	-0.09	0.18	0.01	0.24	0.56	0.19
HW_ATT4	0.02	0.04	0.19	0.20	-0.01	0.07	-0.17	-0.02	**0.92**	0.15	-0.15	0.10	-0.10	0.20	0.00	0.26	0.58	0.21
HCONC	0.16	0.00	0.09	0.09	-0.14	0.00	-0.12	0.02	0.19	**1.00**	-0.03	0.13	-0.03	0.03	0.05	0.13	0.11	0.08
INFE1	0.01	-0.06	0.14	0.07	0.32	-0.07	0.22	0.06	-0.11	-0.10	**0.73**	0.08	0.01	0.01	-0.03	0.08	-0.01	-0.02
INFE2	0.00	-0.07	0.12	0.11	0.35	-0.06	0.23	0.10	-0.12	0.02	**0.85**	0.10	0.07	0.02	0.01	0.03	0.00	-0.11
INFE3	0.03	-0.10	0.15	0.10	0.42	-0.10	0.32	0.03	-0.14	-0.05	**0.88**	0.10	0.06	0.03	0.02	0.05	-0.08	-0.07
INFE4	-0.06	-0.13	0.05	0.10	0.48	-0.15	0.48	-0.03	-0.16	-0.04	**0.84**	-0.03	0.10	-0.01	0.02	-0.06	-0.02	-0.11
INFE5	-0.05	-0.07	0.12	0.11	0.45	-0.09	0.46	-0.04	-0.10	-0.03	**0.83**	0.04	0.05	0.07	0.00	0.01	0.08	-0.07

	AGE	COMP-_EXP	*PHIPC*	CONV	EMPD	EDUC	FAMR	GEN-DER	HW-_ATT	HCONC	INFE	ORIENT	P_EXP	REGUL	RISK	T_HIT	*T_PROV*	WILL
ORIENT1	-0.01	0.27	0.31	0.43	-0.14	0.23	-0.21	0.03	0.09	0.10	0.03	**0.92**	-0.07	0.36	-0.21	0.29	0.16	0.23
ORIENT2	0.00	0.29	0.25	0.36	-0.10	0.27	-0.22	0.06	0.10	0.13	0.09	**0.93**	0.00	0.35	-0.22	0.34	0.16	0.23
ORIENT3	-0.02	0.29	0.33	0.37	-0.15	0.23	-0.25	0.00	0.08	0.13	0.04	**0.94**	-0.11	0.35	-0.20	0.28	0.15	0.25
ORIENT4	0.06	0.18	0.24	0.20	-0.05	0.19	-0.18	0.10	0.10	0.13	0.07	**0.83**	0.00	0.31	-0.12	0.21	0.11	0.19
P_EXP1	-0.04	0.06	-0.33	-0.13	0.12	0.06	0.18	0.01	-0.11	0.05	0.08	0.02	**0.88**	-0.04	0.21	-0.12	-0.08	-0.13
P_EXP2	-0.03	0.02	-0.42	-0.14	0.12	0.07	0.26	0.06	-0.08	-0.08	0.07	-0.10	**0.92**	-0.06	0.18	-0.15	-0.11	-0.16
REGUL1	0.04	0.16	0.23	0.28	0.01	0.16	-0.06	0.10	0.15	-0.01	0.06	0.35	-0.06	**0.92**	-0.10	0.32	0.27	0.20
REGUL2	0.02	0.16	0.18	0.27	0.02	0.11	-0.07	0.08	0.21	0.07	0.04	0.36	-0.02	**0.90**	-0.08	0.27	0.29	0.20
REGUL3	0.01	0.16	0.21	0.29	-0.07	0.14	-0.10	0.02	0.19	0.02	0.01	0.34	-0.07	**0.93**	-0.10	0.24	0.29	0.26
REGUL4	0.00	0.20	0.22	0.29	-0.04	0.18	-0.10	0.05	0.18	0.04	-0.02	0.33	-0.06	**0.92**	-0.10	0.26	0.29	0.25
RISK1	0.09	-0.15	-0.20	-0.18	0.21	-0.16	0.15	-0.06	0.00	0.01	0.01	-0.20	0.22	-0.06	**0.88**	-0.42	-0.02	-0.22
RISK2	0.11	-0.16	-0.17	-0.11	0.16	-0.11	0.07	-0.05	-0.02	-0.01	0.03	-0.15	0.21	-0.08	**0.86**	-0.36	-0.01	-0.19
RISK3	0.10	-0.10	-0.18	-0.18	0.11	-0.11	0.09	-0.06	-0.05	0.12	-0.04	-0.19	0.19	-0.16	**0.84**	-0.34	-0.10	-0.15
RISK4	0.05	-0.14	-0.14	-0.17	0.15	-0.17	0.05	-0.08	-0.01	0.05	0.03	-0.16	0.10	-0.06	**0.79**	-0.27	-0.01	-0.12
T_HIT1	-0.08	0.31	0.30	0.30	-0.08	0.23	-0.22	0.09	0.22	0.16	-0.04	0.26	-0.14	0.25	-0.40	**0.85**	0.21	0.41
T_HIT2	-0.09	0.20	0.31	0.44	-0.04	0.20	-0.17	0.07	0.20	0.09	0.01	0.24	-0.14	0.19	-0.34	**0.88**	0.31	0.39
T_HIT3	0.03	0.14	0.27	0.42	-0.05	0.15	-0.12	0.03	0.25	0.08	0.05	0.30	-0.12	0.35	-0.35	**0.88**	0.40	0.34
BEN	0.13	-0.10	0.23	0.27	0.06	-0.05	-0.10	0.04	0.52	0.07	-0.01	0.11	-0.06	0.29	0.04	0.30	**0.86**	0.18
COMP	0.16	-0.04	0.28	0.26	-0.06	-0.03	-0.11	-0.03	0.51	0.12	-0.02	0.19	-0.14	0.28	-0.09	0.32	**0.92**	0.26
INTEG	0.09	-0.11	0.20	0.25	0.09	-0.07	-0.05	0.03	0.48	0.08	0.01	0.06	-0.03	0.22	-0.02	0.28	**0.79**	0.18
WILL1	0.06	0.20	0.38	0.35	-0.10	0.19	-0.13	-0.06	0.17	0.06	-0.12	0.21	-0.15	0.23	-0.14	0.38	0.24	**0.96**
WILL2	0.03	0.23	0.43	0.36	-0.09	0.20	-0.15	-0.06	0.22	0.08	-0.09	0.26	-0.17	0.25	-0.22	0.43	0.26	**0.98**
WILL3	0.04	0.21	0.42	0.39	-0.10	0.22	-0.13	-0.05	0.20	0.07	-0.11	0.23	-0.18	0.26	-0.25	0.46	0.24	**0.97**
WILL4	0.02	0.23	0.39	0.30	-0.07	0.20	-0.13	-0.04	0.17	0.09	-0.10	0.27	-0.13	0.20	-0.17	0.39	0.22	**0.94**

Key: *Computer Experience (COMP_EXP);* ***PHI Privacy Concerns (PHIPC)*** *[Collection (COL); Errors (ERR); Secondary Use (SU); Unauthorised Access (UA)]; Convenience (CONV); Employment Discrimination (EMPD); Family Rejection (FAMR); Perceived Attitude of Health Workers (HW_ATT); Health Concern (HCONC); Perceived Inferiority (INFE); Privacy Orientation (ORIENT); Privacy Experience (P_EXP); Perceived Effectiveness of Government Regulation (REGUL); Privacy Risk (RISK); Trust in Health*

Information Technology (T_HIT); ***Trust in Healthcare Providers (T_PROV)*** *[Benevolence (BEN); Competence (COMP); Integrity (INTEG)]; Willingness to Disclose PHI (WILL).*

Table 5.8 Interconstruct Correlations: First- and Second-order Constructs

	AGE	COMP-_EXP	PHIPC	CONV	EMPD	EDUC	FAMR	GEN-DER	HW-_ATT	HCONC	INFE	ORIENT	P_EXP	REGUL	RISK	T_HIT	T_PROV	WILL
AGE	**1.00**																	
COMP_EXP	-0.26	**1.00**																
PHIPC	0.09	0.04	**0.71**															
CONV	-0.04	0.04	0.31	**0.83**														
EMPD	-0.12	-0.04	0.01	-0.03	**0.96**													
EDUC	-0.12	0.66	0.06	0.12	-0.04	**1.00**												
FAMR	-0.13	-0.17	-0.24	-0.06	0.46	-0.16	**0.89**											
GENDER	0.02	0.17	-0.05	0.03	-0.01	0.15	-0.09	**1.00**										
HW_ATT	0.05	0.03	0.21	0.20	-0.06	0.06	-0.18	-0.04	**0.93**									
HCONC	0.16	0.00	0.09	0.09	-0.14	0.00	-0.12	0.02	0.19	**1.00**								
INFE	-0.03	-0.11	0.12	0.12	0.50	-0.12	0.43	0.03	-0.15	-0.03	**0.83**							
ORIENT	0.00	0.29	0.32	0.38	-0.12	0.26	-0.24	0.05	0.10	0.13	0.06	**0.91**						
P_EXP	-0.04	0.04	-0.42	-0.15	0.13	0.07	0.25	0.05	-0.10	-0.03	0.08	-0.05	**0.90**					
REGUL	0.02	0.18	0.23	0.31	-0.02	0.16	-0.09	0.07	0.20	0.03	0.02	0.38	-0.06	**0.92**				
RISK	0.11	-0.16	-0.21	-0.19	0.19	-0.16	0.11	-0.07	-0.02	0.05	0.01	-0.21	0.22	-0.10	**0.85**			
T_HIT	-0.05	0.25	0.34	0.44	-0.06	0.22	-0.20	0.07	0.26	0.13	0.01	0.31	-0.15	0.30	-0.42	**0.87**		
T_PROV	0.16	-0.09	0.28	0.30	0.01	-0.05	-0.11	0.00	0.58	0.11	-0.01	0.16	-0.11	0.31	-0.04	0.35		
WILL	0.04	0.23	0.43	0.36	-0.10	0.21	-0.14	-0.05	0.20	0.08	-0.11	0.25	-0.16	0.25	-0.21	0.44	0.25	**0.96**

Key: *Computer Experience (COMP_EXP);* ***PHI Privacy Concerns (PHIPC)*** *[Collection (COL); Errors (ERR); Secondary Use (SU); Unauthorised Access (UA)]; Convenience (CONV); Employment Discrimination (EMPD); Family Rejection (FAMR); Perceived Attitude of Health Workers (HW_ATT); Health Concern (HCONC); Perceived Inferiority (INFE); Privacy Orientation (ORIENT); Privacy Experience (P_EXP); Perceived Effectiveness of Government Regulation (REGUL); Privacy Risk (RISK); Trust in Health Information Technology (T_HIT);* ***Trust in Healthcare Providers (T_PROV)*** *[Benevolence (BEN); Competence (COMP); Integrity (INTEG)]; Willingness to Disclose PHI (WILL).*

Note: *Diagonal elements are the square root of Average Variance Extracted (AVE).*

Table 5.9 Heterotrait-Monotrait Ratio (HTMT): First- and Second-order Constructs

	AGE	COMP-_EXP	PHIPC	CONV	EMPD	EDUC	FAMR	GENDER	HW_ATT	HCONC	INFE	ORIENT	P_EXP	REGUL	RISK	T_HIT	WILL
AGE																	
COMP_EXP	0.257																
PHIPC	0.105	0.112															
CONV	0.042	0.051	0.423														
EMPD	0.130	0.067	0.119	0.046													
EDUC	0.120	0.660	0.089	0.129	0.058												
FAMR	0.118	0.172	0.274	0.086	0.528	0.168											
GENDER	0.019	0.169	0.093	0.100	0.010	0.152	0.113										
HW_ATT	0.055	0.049	0.253	0.223	0.065	0.070	0.189	0.045									
HCONC	0.156	0.005	0.193	0.106	0.150	0.002	0.112	0.025	0.192								
INFE	0.039	0.107	0.301	0.143	0.542	0.118	0.535	0.067	0.161	0.065							
ORIENT	0.026	0.293	0.401	0.414	0.131	0.264	0.233	0.055	0.108	0.140	0.094						
P_EXP	0.041	0.047	0.535	0.180	0.156	0.080	0.275	0.048	0.121	0.083	0.090	0.093					
REGUL	0.019	0.191	0.289	0.345	0.046	0.166	0.081	0.070	0.209	0.038	0.046	0.405	0.069				
RISK	0.112	0.172	0.237	0.219	0.213	0.174	0.108	0.078	0.048	0.064	0.057	0.230	0.259	0.116			
T_HIT	0.084	0.271	0.440	0.518	0.074	0.244	0.196	0.081	0.285	0.137	0.069	0.348	0.188	0.335	0.481		
WILL	0.041	0.231	0.496	0.393	0.101	0.215	0.129	0.055	0.206	0.078	0.097	0.265	0.184	0.257	0.219	0.480	

Key: *Computer Experience (COMP_EXP);* ***PHI Privacy Concerns (PHIPC)*** *[Collection (COL); Errors (ERR); Secondary Use (SU); Unauthorised Access (UA)]; Convenience (CONV); Employment Discrimination (EMPD); Family Rejection (FAMR); Perceived Attitude of Health Workers (HW_ATT); Health Concern (HCONC); Perceived Inferiority (INFE); Privacy Orientation (ORIENT); Privacy Experience (P_EXP); Perceived Effectiveness of Government Regulation (REGUL); Privacy Risk (RISK); Trust in Health Information Technology (T_HIT);* ***Trust in Healthcare Providers (T_PROV)*** *[Benevolence (BEN); Competence (COMP); Integrity (INTEG)]; Willingness to Disclose PHI (WILL).*

Table 5.10 Trust in Healthcare Providers - Descriptives

Construct	Dimensions/Items	Outer Loadings	Variance Inflation Factor (VIF)	Outer Weights	*t* Value	*p* Value	Significance ($p < 0.05$)?
Trust in Healthcare Providers	Benevolence (BEN)	0.86	2.01	0.36	3.017	0.003	Yes
	Competence (COMP)	0.92	1.88	0.56	4.968	0.000	Yes
	Integrity (INTEG)	0.79	1.87	0.22	1.710	0.087	No

In summary, confirmatory factor analysis was conducted using PLS-SEM to test the factor structure of the research model proposed in the study. The evaluation of the reflective and formative measurement models in the research model has shown that all reflective and formative constructs exhibit satisfactory levels of quality. The Harman's Single Factor test and the full collinearity test also revealed that common method bias does not pose a problem in the data. The research model thus can be considered appropriate for use in further analysis. The next section focuses on evaluating the hypothesized relationships in the research model.

5.5.2 Evaluation of the Structural Model

When the reliability and validity of constructs' measures (or measurement models) are confirmed, the next stage in the PLS-SEM path model analysis is to evaluate the structural model. Structural model refers to the hypothesized relationship between independent and dependent constructs.

The evaluation of the structural model involves examining the model's predictive power and the relationships between constructs (Hair et al., 2016). The measure of a model's predictive power is the coefficient of determination (R^2 value), which represents the amount of explained variance in the dependent constructs by all of the independent constructs linked to it (Hair et al., 2016). On the other hand, the hypothesized relationships among constructs are represented by the path coefficient (i.e., *beta value*) which measures the strength of an effect from independent constructs to dependent constructs.

The explanatory power of the structural model was assessed by considering the R^2 values on the dependent constructs obtained by running the PLS-SEM algorithm. The statistical significance of the path coefficients was assessed using *t* values and *p* values obtained by means of bootstrapping. Following the recommendation in Hair et al. (2016), a total of 5000 bootstrapping samples were utilized. All hypotheses were examined based on a two-tailed test with a significance level of 0.05. The results of the main hypotheses are presented first and then the mediating effects in the research model are explored.

5.5.2.1 Hypothesis Testing - Results

Figure 5.1 presents the results of the structural model with R^2 values, path coefficients and significant levels indicated. Chin (1998) considers R^2 values of 0.67, 0.33, or 0.19 for

dependent variables as, respectively, substantial, moderate, or weak. The R^2 value of the main dependent variable, willingness to disclose PHI (WILL), is 0.37, which can be considered moderate. Thus, the structural model explained 0.37 of the variance in individuals' willingness to disclose their PHI. The R^2 values for the other dependent variables trust in healthcare providers (0.38), trust in HIT (0.32), and PHI privacy concerns (0.14) can be considered as moderate, very close to moderate, and weak, respectively.

The results provided support for the proposed research model with the majority of constructs found to be significant, albeit a few of them not in hypothesized directions. The findings for the proposed antecedents to trust in HIT (T_HIT) are first presented. It was proposed that perceived attitude of health workers (HW_ATT) and perceived effectiveness of government regulation (REGUL) will each have a positive influence on trust in healthcare providers (T_PROV) which in turn is hypothesized to have positive influence on T_HIT. In support of H1a, HW_ATT was found to have a pronounced positive effect on T_PROV (β=0.54, p=0.000). Similarly, the data found evidence for the positive influence of REGUL on T_PROV (β=0.21, p=0.001), supporting H2a. T_PROV was also found to have a positive effect on T_HIT (β=0.24, p=0.003), offering support for H4b. The path analysis further revealed a direct positive influence of REGUL on T_HIT (β=0.17, p=0.009) in support of H2b. However, the hypothesized direct positive influence of HW_ATT on T_HIT in H1b was not supported (β=0.08, p=0.260). Lastly, H7b asserted that privacy risk (RISK) will negatively influence T_HIT. The path analysis revealed that RISK had a strong negative, significant effect on T_HIT (β=-0.39, p=0.000), supporting H7b.

The above explored antecedents to trust in HIT (T_HIT) were also examined as antecedents to PHI privacy concerns (PHIPC). Surprisingly, all the antecedents (significant and insignificant) influenced PHIPC contrary to hypothesized expectations. H1c proposed a negative relationship between perceived attitude of health workers (HW_ATT) and PHIPC. H1c was not supported as a weak and insignificant positive relationship was found between HW_ATT and PHIPC (β=0.06). It was hypothesized in H2c that perceived effectiveness of government regulation (REGUL) will negatively influence PHIPC. The relationship was, however, positive and significant (β=0.14, p=0.042) indicating lack of support for H2c. Similarly, trust in healthcare providers (T_PROV) had a significant positive effect on PHIPC (β=0.20, p=0.009) contrary to the hypothesized negative relationship between these constructs leading to the rejection of H4c. Lastly, whereas H7a proposed a positive influence of privacy risk (RISK) on PHIPC, a significant negative relationship was observed in the data (β=-0.18, p=0.004). Thus, H7a was not supported. These contrary findings are explored further in a series of post hoc analyses in Section 5.5.3.

The roles of convenience (CONV), trust in healthcare providers (T_PROV), and trust in HIT (T_HIT) in driving individuals' willingness to disclose PHI (WILL) in digitized healthcare environments were respectively explored in H3, H4a, and H5. First, the data provided evidence for the hypothesized positive relationship between CONV and WILL (β=0.19, p=0.005) supporting H3. Similarly, the path analysis revealed that T_HIT has a positive influence on WILL (β=0.21, p=0.002), offering support for H5. However, T_PROV was found to have a weak and insignificant effect on WILL (β=0.05). Thus, H4a was not supported.

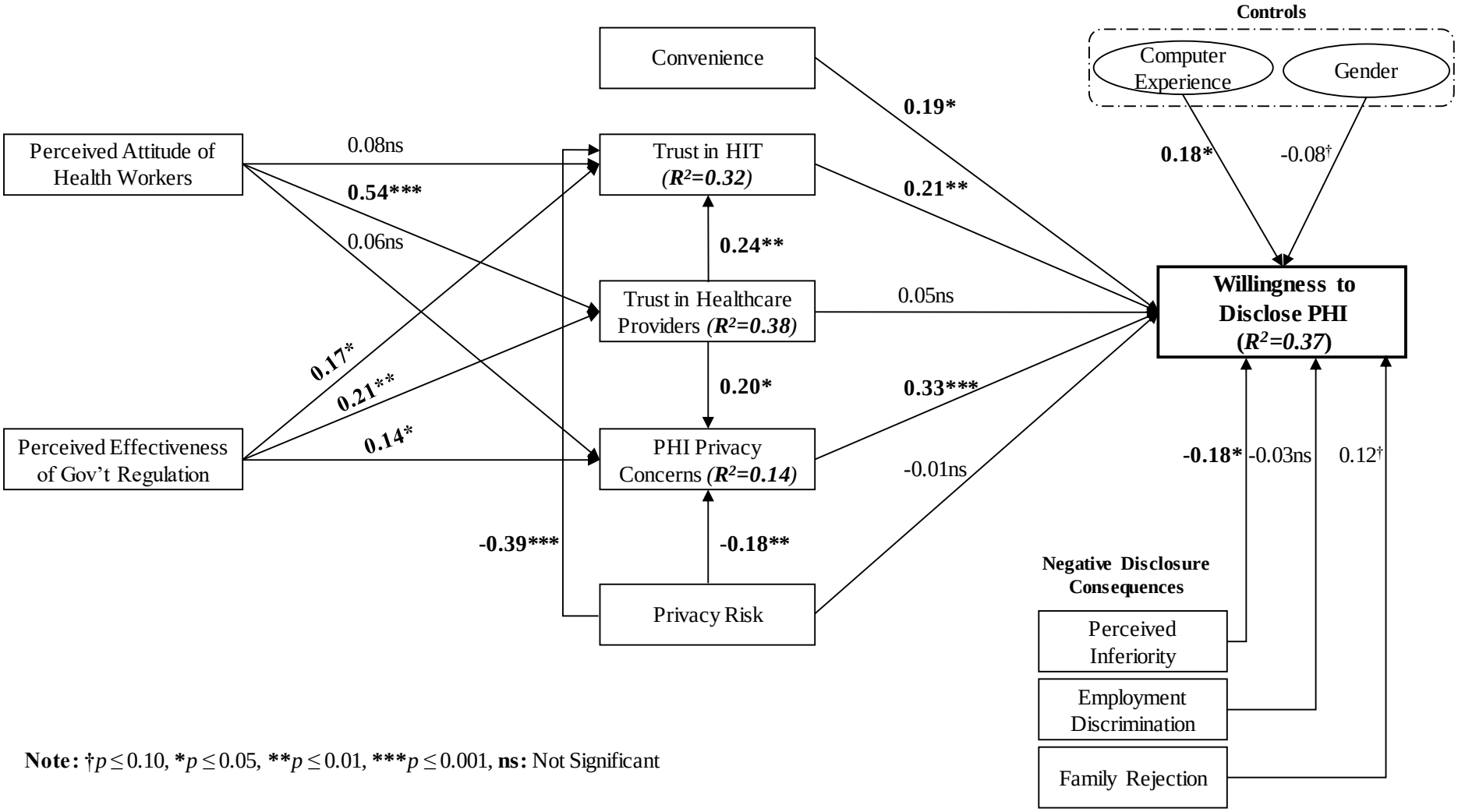


Figure 5.1 Structural Model of Proposed Research Model

In addition to the factors that drive individuals' willingness to disclose PHI, factors that inhibit individuals' PHI disclosure were also explored. First, it was proposed in H6 that PHI privacy concerns (PHIPC) will negatively influence willingness to disclose PHI (WILL). Surprisingly, contrary to expectations, a strong positive relationship was observed between PHIPC and WILL (β=0.33, $p<0.000$). Thus, H6 was not supported.

Table 5.11 Summary of Findings

Hypotheses	**Path Coefficients**	***t* Values**	***p* Values**	**Supported**
H1a(+): Perceived attitude of health workers → Trust in healthcare providers	0.54	11.180	0.000	✓
H1b(+): Perceived attitude of health workers → Trust in HIT	0.08	1.126	0.260	**X**
H1c(-): Perceived attitude of health workers → PHI privacy concerns	0.06	0.775	0.438	**X**
H2a(+): Perceived effectiveness of government regulation → Trust in healthcare providers	0.21	3.366	0.001	✓
H2b(+): Perceived effectiveness of government regulation → Trust in HIT	0.17	2.627	0.009	✓
H2c(-): Perceived effectiveness of government regulation → PHI privacy concerns	0.14	2.038	0.042	**X***
H3(+): Convenience → Willingness to disclose PHI	0.19	2.827	0.005	✓
H4a(+): Trust in healthcare providers → Willingness to disclose PHI	0.05	0.647	0.518	**X**
H4b(+): Trust in healthcare providers → Trust in HIT	0.24	2.997	0.003	✓
H4c(-): Trust in healthcare providers → PHI privacy concerns	0.20	2.601	0.009	**X***
H5(+): Trust in HIT → Willingness to disclose PHI	0.21	3.062	0.002	✓
H6(-): PHI privacy concerns → Willingness to disclose PHI	0.33	4.351	0.000	**X***
H7a(+): Privacy risk → PHI privacy concerns	-0.18	2.919	0.004	**X***
H7b(-): Privacy risk → Trust in HIT	-0.39	7.588	0.000	✓
H7c(-): Privacy risk → Willingness to disclose PHI	-0.01	0.166	0.868	**X**
H8(-): Perceived Inferiority → Willingness to disclose PHI	-0.18	2.593	0.010	✓
H9(-): Employment discrimination → Willingness to disclose PHI	-0.03	0.413	0.680	**X**
H10(-): Family Rejection → Willingness to disclose PHI	0.12	1.665	0.096	**X**

X Not supported, **X*** Significant but not in the hypothesized direction, ✓ Supported

The path analysis revealed that privacy risk (RISK) has a weak negative and insignificant effect on WILL (β=-0.01), indicating lack of support for H7c. H8-H10 investigated the impact of the negative consequences individuals may perceive to occur from the disclosure of their PHI (i.e., perceived inferiority, employment discrimination, and family rejection) on their willingness to disclose their PHI. Of these, only perceived inferiority (INFE) was found to be a significant predictor of willingness to disclose PHI (WILL). In support of H8, the data revealed a significant negative relationship between INFE and WILL (β=-0.18, p=0.010). Employment discrimination (EMPD) had a weak negative and insignificant effect on WILL (β=-0.03). Thus, H9 was not supported. In contrast to the negative relationship proposed between family

rejection (FAMR) and WILL in H10, the data revealed an insignificant positive relationship the two constructs (β=0.12, p=0.096) leading to the rejection of H10.

Of the control variables examined in the research model, computer experience had a significant positive influence on willingness to disclose PHI (β=0.18, p=0.020). Gender was found to have a negative influence on willingness to disclose PHI and this effect was marginally significant at 0.10 level (β=-0.08, p=0.092). Thus, males expressed less willingness to disclose their PHI. None of the remaining control variables (i.e., age, education, health concern, privacy experience, and privacy orientation) was significant. A summary of the main findings is provided in Table 5.11. Findings related to the mediation effects in the research model are explored next.

5.5.2.2 Testing Mediation Effects

The previous section presented the results of hypotheses related to the direct effects in the research model of the study. As noted in the introduction of Section 5.5, an important advantage of PLS-SEM is that it enables the analysis of indirect effects. This section presents the results regarding the mediation (or indirect) effects in the research model.

The mediation analysis procedure recommended by Hair et al. (2016) was followed in testing the mediation effects. The first step is to test the significance of the indirect effect. For example, as noted in the preceding section, it was proposed that perceived attitude of health workers (HW_ATT) will have a direct influence on trust in HIT (T_HIT) and indirect influence through trust in healthcare providers (T_PROV). The indirect effect from HW_ATT via T_PROV to T_HIT is the product of the *beta* values (i.e., path coefficients) from HW_ATT to T_PROV and from T_PROV to T_HIT. Using the above example, the next step in the mediation analysis is to examine the significance of the direct effect from HW_ATT to T_HIT. There is partial mediation when both the direct and indirect effects are significant and there is a full mediation when only the indirect effect is significant.

The results of the mediation effects obtained by running the bootstrapping procedure in SmartPLS 3.2.8 are provided in Table 5.12. For easy reference, the direct effects related to the mediation analysis which are presented in Table 5.11 have been repeated in Table 5.12. Regarding the above example, the results indicate that T_PROV fully mediates the HW_ATT to T_HIT relationship as the direct effect from HW_ATT is insignificant, whereas the indirect effect is highly significant. It was similarly proposed that T_PROV will mediate the influence of perceived effectiveness of government regulation (REGUL) on T_HIT. As evident in Table 5.12, both the direct and indirect effects from REGUL to T_HIT are significant indicating that T_PROV partially mediates this relationship.

The mediating influence of trust in healthcare providers (T_PROV) on the relationship from perceived attitude of health workers (HW_ATT) to PHI privacy concerns (PHIPC) and perceived effectiveness of government regulation (REGUL) to PHIPC was also explored. A

full mediation of T_PROV on the HW_ATT → PHIPC relationship was observed as the HW_ATT → PHIPC direct effect is weak and insignificant, whereas the indirect effect via T_PROV is significant. On the other hand, the direct effect from REGUL to PHIPC was found to be significant. The indirect effect via T_PROV is also marginally significant at the 0.05 level. Thus, it can be concluded that T_PROV partially mediates the REGUL → PHIPC relationship.

Trust in HIT (T_HIT) and PHI privacy concerns (PHIPC) were both proposed as mediators of the relationship from trust in healthcare providers (T_PROV) to willingness to disclose PHI (WILL) and privacy risk (RISK) to WILL. As the results in Table 5.12 indicate, the direct effect from T_PROV to WILL is insignificant. However, T_PROV had a significant indirect influence on WILL via T_HIT, and also via PHIPC. Thus, it can be concluded that either T_HIT or PHIPC fully mediates the T_PROV to WILL relationship. Similarly, T_HIT and PHIPC were each found to fully mediate the RISK → WILL relationship as the direct effect from RISK to WILL was weak and insignificant, whereas the indirect effects via T_HIT and also via PHIPC were significant.

Table 5.12 Findings – Mediation Effects

Relationship	**Direct/Indirect Effects**	***t* Values**	***p* Values**	**Significance ($p \leq 0.05$)**	**Mediation Type**
H1b(+): Perceived attitude of health workers → Trust in HIT	0.08	1.126	0.260	No	Full
Perceived attitude of health workers → Trust in healthcare providers → Trust in HIT	0.13	2.842	0.005	Yes	
H2b(+): Perceived effectiveness of government regulation → Trust in HIT	0.17	2.627	0.009	Yes	Partial
Perceived effectiveness of government regulation → Trust in healthcare providers → Trust in HIT	0.05	2.267	0.023	Yes	
H1c(-): Perceived attitude of health workers → PHI privacy concerns	0.06	0.775	0.438	No	Full
Perceived attitude of health workers → Trust in healthcare providers → PHI privacy concerns	0.11	2.483	0.013	Yes	
H2c(-): Perceived effectiveness of government regulation → PHI privacy concerns	0.14	2.038	0.042	Yes	Partial
Perceived effectiveness of government regulation → Trust in healthcare providers → PHI privacy concerns	0.04	1.944	0.052	Yes	
H4a(+): Trust in healthcare providers → Willingness to disclose PHI	0.05	0.647	0.518	No	Full
Trust in healthcare providers → Trust in HIT → Willingness to disclose PHI	0.05	2.024	0.043	Yes	
Trust in healthcare providers → PHI privacy concerns → Willingness to disclose PHI	0.07	2.389	0.017	Yes	
H7c(-): Privacy risk → Willingness to disclose PHI	-0.01	0.166	0.868	No	Full
Privacy risk → Trust in HIT → Willingness to disclose PHI	-0.08	3.057	0.002	Yes	

Privacy risk → PHI privacy concerns → Willingness to disclose PHI	-0.06	2.631	0.009	Yes	

The results of the mediation analysis and hypothesis testing presented in the previous section are explored further in a series of post hoc analyses in the immediately following section.

5.5.3 *Post Hoc* Analysis

To check the robustness of some of the study results discussed in Section 5.5.2 and to obtain further insight into the findings, especially those that were contrary to hypothesized expectations, a series of *post hoc* analyses were conducted. First, the contrary findings observed in connection with hypotheses related to PHI privacy concerns are explored by re-conceptualizing PHI privacy concerns. Second, the findings related to the antecedents of trust in HIT and PHI privacy concerns were validated by accounting for the influence of several control variables.

5.5.3.1 Exploring Unexpected Findings

In Section 5.5.2.1, the test of the structural model reveals unexpected results regarding hypotheses related to PHI privacy. PHI privacy concerns was operationalized as a reflective second-order construct with reflective first-order constructs comprising of the four dimensions of concern for information privacy (CFIP) (Smith et al., 1996): collection, errors, secondary use, and unauthorised access. The evaluation of the factor structure of PHI privacy concerns revealed that it reflects negatively on the collection dimension, whereas it reflects positively on each of the other dimensions (see Table 5.6). Given these unexpected results, we conducted a post hoc analysis of the PHI privacy concerns construct to probe further the results related to the antecedents and consequence of PHI privacy concerns.

The descriptive statistics in Table 5.2 showed that collection has a considerably lower mean (3.36) than the other three dimensions which ranged from 6.01 to 6.37. The correlations among constructs provided in Table 5.4 also show that collection is negatively correlated with errors and unauthorised access and positively but marginally correlated with secondary use. Prior research in the healthcare context has similarly found collection to have a lower mean than the other three dimensions (Hwang et al., 2012) or not converge well with these dimensions (Angst & Agarwal, 2009). In their review of the broader IS privacy literature, Hong and Thong (2013) also observed that the collection dimension has a lower mean and average correlation than the other three CFIP dimensions. This suggests that individuals' concerns about the collection of their personal information may be different from their concerns after the information is collected and is in the custody of organizations (i.e., concerns related to errors, secondary use, and unauthorised access).

In exploring the factor structure of CFIP, Stewart and Segars (2002) proposed alternative models as plausible representations of CFIP. One of the models hypothesizes that the combined

15 items of the four CFIP dimensions (collection, errors, secondary use, and unauthorised access) form into two factors: individuals' concerns about collection and their concerns about management of personal information once it is in the custody of organizations. Stewart and Segars (2002) found support for this model in a pretest among university students with the collection dimension loading on a single factor, whereas the items measuring the dimensions of errors, secondary use, and unauthorised access converged onto a single factor.

The two-factor model of CFIP suggested by Stewart and Segars (2002) fits the factor structure of PHI privacy concerns supported by the data in this study as the collection dimension did not converge well with the other three dimensions. Thus, to probe into the study's contrary findings, PHI privacy concerns was remodelled as comprising of two key factors: (i) concerns about the *collection* of PHI by healthcare providers (i.e., PHI collection concerns), and (ii) concerns regarding the management and protection of the collected and electronically stored PHI (i.e., PHI management concerns), where the latter comprises concerns related to errors, secondary use, and unauthorised access. The evaluation of the measurement model of PHI privacy concerns in Section 5.5.1.2 revealed support for a second-order factor structure with first-order dimensions of errors, secondary use, and unauthorised access. Consequently, PHI management concerns was operationalized as a second-order construct.

A revised PLS-SEM path model of the proposed research model was examined where the two proposed factors, PHI collection concerns and PHI management concerns, replaced PHI privacy concerns in the path model. The measurement models of all constructs in the revised model demonstrated acceptable levels of quality. Confirming the second-order factor structure proposed for PHI management concerns, the loadings of the first-order dimensions of errors, secondary use, and unauthorised access were each above the critical value of 0.70. The results of the structural relationships in the revised model are provided in Figure 5.2. The model explained more of the variance in willingness to disclose PHI (0.43) than the original model in Figure 5.1, which explained 0.37 of the variance in willingness to disclose PHI.

The two proposed dimensions of PHI privacy concerns (PHIPC), PHI collection concerns (PHI_COLC) and PHI management concerns (PHI_MgtC), were significant predictors of willingness to disclose PHI (WILL) with PHI_COLC exerting a pronounced negative effect (β=-0.40, p=0.000), whereas PHI_MgtC had a positive effect on WILL (β=0.14, p=0.031). Thus, hypothesis H6 which predicted a negative effect of PHIPC on WILL is supported regarding PHI_COLC. The other significant predictors of WILL in the test of the original research model (convenience, trust in HIT, perceived inferiority, and computer experience) were similarly found to significantly predict WILL in the revised model. However, gender and family rejection which were marginally significant in the original model became insignificant in the revised model.

For ease of comparison, the results regarding the influence of the antecedent factors on the overall PHI privacy concerns (PHIPC) and on each of the two proposed dimensions of PHIPC, PHI management concerns (PHI_MgtC) and PHI collection concerns (PHI_COLC), are summarized in Table 5.13. In general, the antecedent factors exert similar influences on overall

PHIPC and PHI_MgtC. This is not surprising as the three dimensions of PHI_MgtC (errors, secondary use, and unauthorised access) had loaded positively, on the underlying construct, PHIPC. Regarding PHI_COLC, there were significant differences. In contrast to the overall PHIPC and PHI_MgtC, the results indicated that perceived attitude of health workers (HW_ATT), perceived effectiveness of government regulation (REGUL), and trust in healthcare providers (T_PROV) had insignificant effects on PHI_COLC. Privacy risk (RISK), on the other hand, had a significant positive effect on PHI_COLC (β=0.27, p=0.000) contrary to its negative effect on both the overall PHIPC and PHI_MgtC. The hypothesized positive effect of RISK on PHIPC was thus supported regarding PHI_COLC.

Regarding mediation effects, trust in healthcare providers (T_PROV) partially mediated the indirect effect (0.040) from perceived effectiveness of government regulation (REGUL) to PHI management concerns (PHI_MgtC) (t=1.884, p=0.060) but it did not mediate the REGUL to PHI collection concerns (PHI_COLC) relationship (-0.018, t=0.881, p=0.379). Similarly, T_PROV fully mediated the indirect effect (0.104) from perceived attitude of health workers (HW_ATT) to PHI_MgtC (t=2.300, p=0.021) but its mediation role on the HW_ATT to PHI_COLC relationship was insignificant (-0.048, t=1.017, p=0.309). In the original model (Figure 5.1), the overall PHI privacy concerns (PHIPC) fully mediated the influence of T_PROV on willingness to disclose PHI (WILL). However, in the revised model none of the two dimensions of PHIPC, i.e., PHI_COLC (0.035, t=1.034, p=0.296) and PHI_MgtC (0.027, t=1.418, p=0.139), was found to mediate the relationship between T_PROV and WILL. On the other hand, PHI_COLC fully mediated the relationship between privacy risk (RISK) and WILL (-0.108, t=3.644, p=0.000) but PHI_MgtC did not mediate this relationship (-0.011, t= 1.228, p= 0.219).

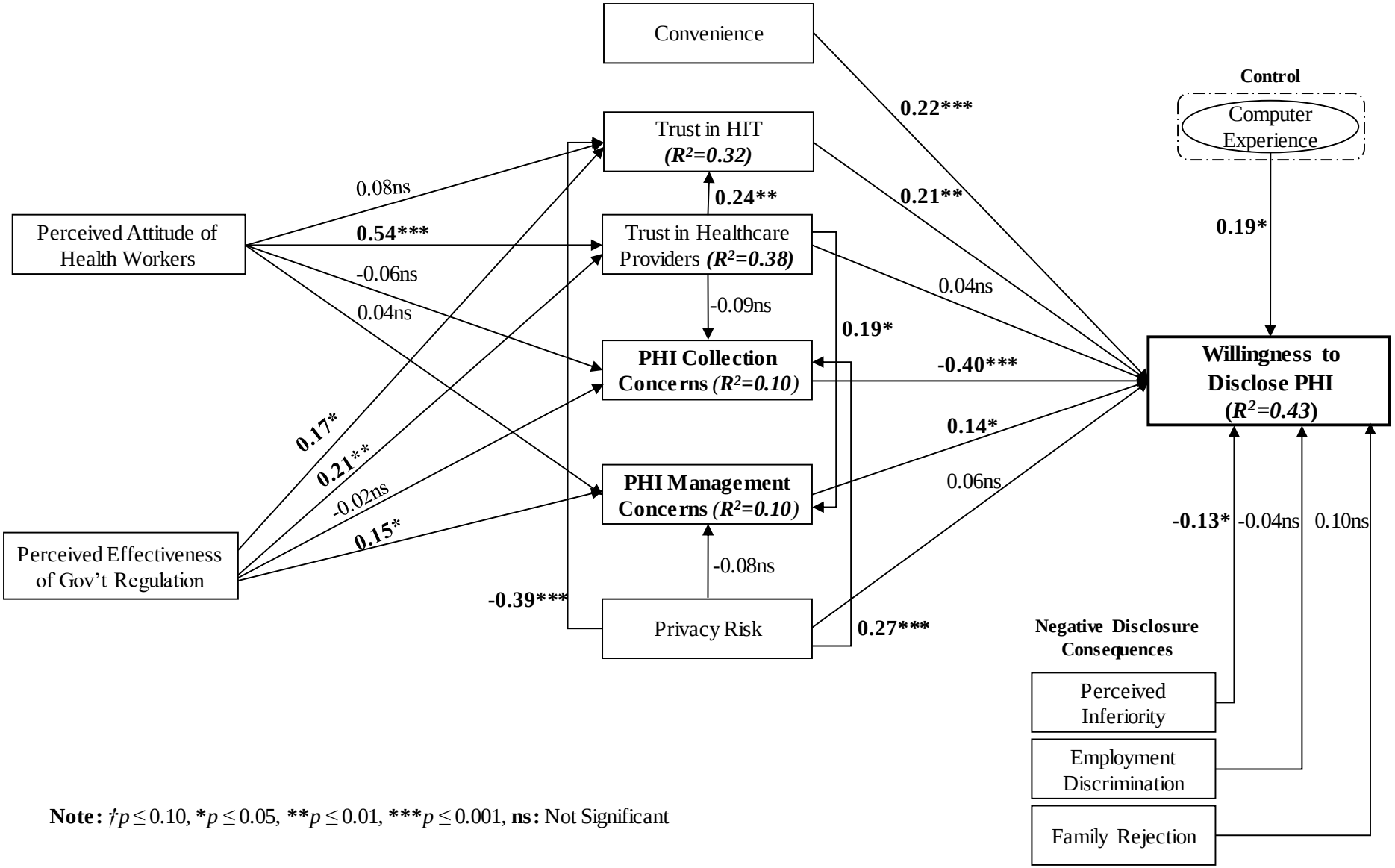
Similar to the results in the original model (Figure 5.1), trust in HIT (T_HIT) fully mediated the T_PROV to WILL relationship (0.051, t=2.063, p=0.039) and the RISK to WILL relationship (-0.083, t=3.169, p=0.002). Similarly, T_PROV partially mediated the relationship between REGUL and T_HIT (0.048, t=2.171, p=0.030) and fully mediated the relationship between HW_ATT and T_HIT (128, t=2.718, p=0.007).

Table 5.13 Summary of Results – Antecedents to PHIPC

Antecedent	**PHI Privacy Concerns (R^2=0.14)**	**PHI Management Concerns (R^2=0.10)**	**PHI Collection Concerns (R^2=0.10)**
	Path Coefficients		
Perceived Attitude of Health workers (HW_ATT)	0.06	0.04	-0.06
Perceived Effectiveness of Government Regulation (REGUL)	0.14*	0.15*	-0.02
Trust in Healthcare Providers (T_PROV)	0.20*	0.19*	-0.09
Privacy Risk (RISK)	-0.18*	-0.08	0.27***

**p ≤ 0.05, **p ≤ 0.01, ***p ≤ 0.001*

Summing up, lending support to a two-factor structure of PHI privacy concerns (PHIPC), the results of the revised model suggest that individuals divide their PHI privacy concerns into two main areas: PHI collection concerns (PHI_COLC) and PHI management concerns (PHI_MgtC). The influence of the antecedent factors on PHI_MgtC was significantly different from their influence on PHI_COLC. Similarly, PHI_MgtC and PHI_COLC had differential impacts on willingness to disclose PHI (WILL) with PHI_MgtC positively associated with WILL, whereas PHI_COLC strongly decreases WILL. Possible explanations for these findings will be explored in the next chapter drawing on prior research. The next section validates the findings regarding the influence of the antecedent factors on the two dimensions of PHIPC by accounting for the influence of control variables.



Note: †$p \leq 0.10$, *$p \leq 0.05$, **$p \leq 0.01$, ***$p \leq 0.001$, **ns:** Not Significant

Figure 5.2 Post Hoc Analysis – 2-Factor Model of PHIPC

5.5.3.2 Antecedents to PHI Privacy Concerns – Validating Findings

In Section 2.3.2 of Chapter 2, it was discussed that individual characteristics including age, gender, education, and health status have been found to influence PHI privacy concerns (PHIPC) in a number of studies (e.g., Laric et al., 2009; Papoutsi et al., 2015; Wilkowska & Ziefle, 2012). A few studies have also found that experience-related factors such as computer experience and past experience of privacy violation (i.e., privacy experience) influence PHIPC (e.g., Bansal et al., 2010; Perera et al., 2011). Privacy orientation (one's desire for privacy of his personal information) has also been found to increase privacy concerns in other IS contexts (Taylor et al., 2015; Yao et al., 2007). The influence of the individual characteristics and experience factors on each of the two dimensions of PHIPC (i.e., PHI collection concerns and PHI management concerns) was examined to account for any variance they might explain in each dimension. The objective was to confirm the findings in the study regarding the four proposed antecedents to PHIPC: perceived attitude of health workers (HW_ATT), perceived effectiveness of government regulation (REGUL), trust in healthcare providers (T_PROV), and privacy risk (RISK).

Regarding PHI collection concerns (PHI_COLC), out of the four antecedents, RISK was the only significant predictor (see Figure 5.3). The remaining antecedents HW_ATT, REGUL, and T_PROV were each negatively but weakly related to PHI_COCL. These findings thus confirm the results from the test of the revised model in Figure 5.2.

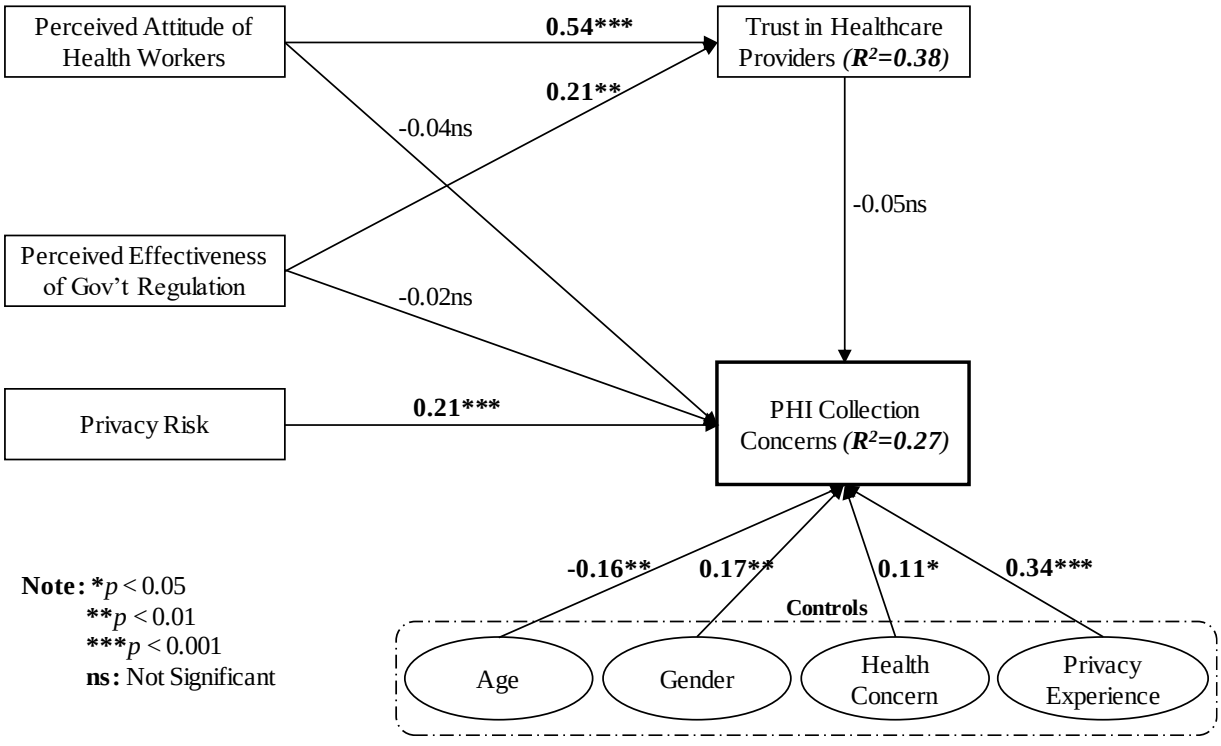


Figure 5.3 Post Hoc Analysis – Antecedents to PHI Collection Concerns

Interestingly, a number of the control variables were found to be significant predictors of PHI_COCL. Contradicting most findings in prior research (e.g., Esmaeilzadeh, 2018a; Kordzadeh & Warren, 2014; Laric et al., 2009), males and younger individuals were found to

be more concerned about the collection of their PHI than females and older individuals, respectively. Not surprisingly, however, health concern and privacy experience each had a significant positive influence on PHI_COLC. The other control variables education (β=-0.034), privacy orientation (β=0.005), and computer experience (β=-0.030) were all insignificant.

Following Angst and Agarwal (2006), health concern (i.e., the extent to which one is concerned about his/her health) was included in the study as an alternative measure of one's health condition in addition to health status (see Table 4.1). Health status was initially tested as a control variable but was insignificant (β=-0.093, p=0.153). Consequently, health concern was tested in place of health status and it was found to be significant as reported Figure 5.3.

The structural model results regarding the influence of the antecedent factors on PHI management concerns (PHI_MgtC) are provided in Figure 5.4. Partially confirming the revised model results in Figure 5.2, trust in healthcare providers (T_PROV) remained a significant predictor of PHI_MgtC, whereas perceived effectiveness of government regulation (REGUL) became insignificant after controlling for the influence of individual characteristics and experience factors. However, the indirect effect (0.038) from REGUL to PHI_MgtC was significant (t=1.970, p=0.049). Thus, with the addition of control variables, T_PROV fully mediated the REGUL to PHI_MgtC relationship as against the partial mediation in the revised model (Figure 5.2). Similarly, consistent with the results of the revised model, perceived attitude of health workers (HW_ATT) had a significant indirect influence (0.100) on PHI_MgtC via T_PROV (t=2.256, p=0.024) indicating the full mediation role of T_PROV on the HW_ATT to PHI_MgtC relationship. Among the control variables, computer experience, privacy experience, and privacy orientation significantly influenced PHI_MgtC. The remaining control variables (age, gender, education, and health status) were insignificant.

In summary, in the revised model (Figure 5.2), the four antecedent factors considered in the study explained 0.10 of the variance in both PHI collection concerns (PHI_COLC) and PHI management concerns (PHI_MgtC). The addition of several individual factors (e.g., age, gender, education, etc.) as control variables improved the variance explained in both PHI_COLC (R^2=0.27) and PHI_MgtC (R^2=0.25). However, the influence of the antecedent factors on both PHI_COLC and PHI_MgtC largely remained the same after controlling for the influence of control variables. The only exception is the relationship between perceived effectiveness of government regulation (REGUL) and PHI_MgtC which became insignificant with the addition of control variables. Privacy risk (RISK) and trust in healthcare providers (T_PROV) were confirmed as significant predictors of PHI_COLC and PHI_MgtC, respectively. Perceived attitude of health workers (HW_ATT) and REGUL indirectly influenced PHI_MgtC via T_PROV. Regarding the control variables, age, gender, and health concern significantly influenced PHI_COLC. On the other hand, computer experience and privacy orientation were significant predictors of PHI_MgtC. Privacy experience had significant effect on both PHI_COLC and PHI_MgtC, positively associated with the former but negatively related to the latter.

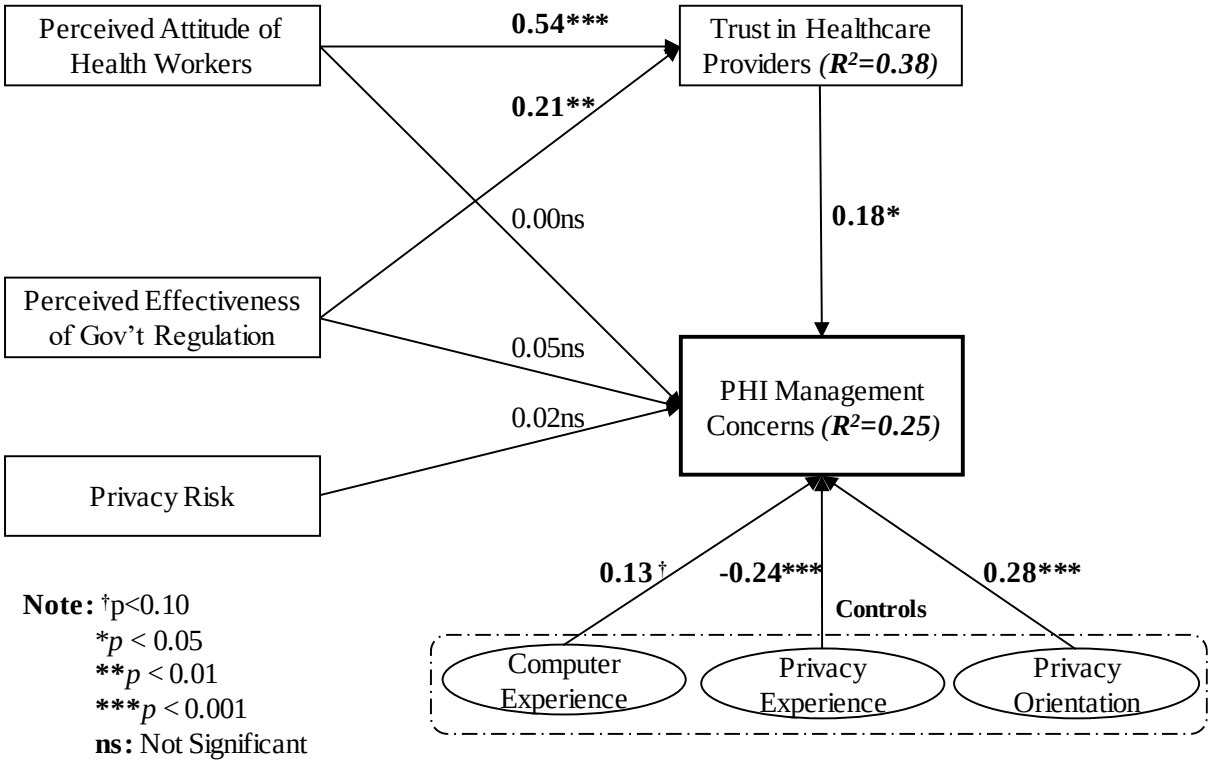


Figure 5.4 Post Hoc Analysis – Antecedents to PHI Management Concerns

5.5.3.3 Antecedents to Trust in HIT – Validating Findings

The antecedents to PHI privacy concerns were also examined as antecedents to trust in HIT (T_HIT) in the research model of the study. The results of the structural relationships in the research model (see Figure 5.1) found perceived effectiveness of government regulation (REGUL), trust in healthcare providers (T_PROV), and privacy risk (RISK) as significant predictors of T_HIT. Perceived attitude of health workers (HW_ATT) was also found to indirectly influence T_HIT via T_PROV.

As was noted in Section 2.3.4 of Chapter 2, demographic factors including gender, age, education, health status, and computer experience have been found to influence individuals' trust in a technological artefact including HIT (Bansal et al., 2010; Corbitt et al., 2003; Dickerson, 2003; Dutta-Bergman, 2003). Therefore, to validate the findings related to the antecedents to T_HIT, the influence of these variables on T_HIT was controlled for.

Figure 5.5 is the structural model results of the antecedents to T_HIT. Confirming the results of the main research model presented in Section 5.5.2.1, REGUL, RISK, and T_PROV each had a significant direct influence on T_HIT. The indirect effect (0.059) from REGUL to T_HIT was also significant (t=2.555, p=0.011) confirming the partial mediation of T_PROV on the REGUL to T_HIT relationship. Similarly, the full mediation of T_PROV on the HW_ATT to T_HIT relationship was confirmed as HW_ATT had a significant indirect influence (0.158) on T_HIT via T_PROV (t=3.510, p=0.000).

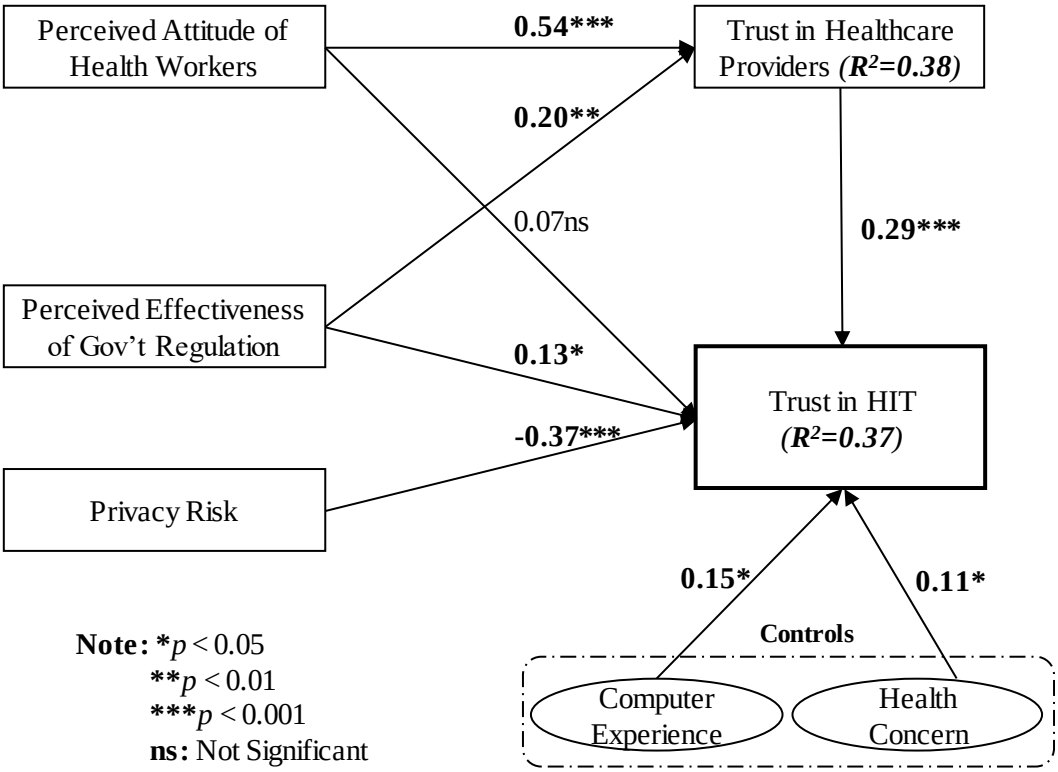


Figure 5.5 Post Hoc Analysis – Antecedents to Trust in HIT

In the main research model results (Figure 5.1), the four antecedent factors (HW_ATT, REGUL, T_PROV, and RISK) explained 0.32 of the variance in T_HIT. The addition of the control variables increased the variance explained in T_HIT to 0.37. Of the control variables examined, only computer experience and health concern were significant. Age, gender, and education were all insignificant. As noted earlier in Section 5.5.3.2, health concern (i.e., the extent to which one is concerned about his/her health) was included in the study as an alternative measure of one's health condition in addition to health status (see Table 4.1). Since health status had a weak, insignificant effect on T_HIT (β=0.066, p=0.330), health concern was also tested, and it was found to be significant (Figure 5.5)

In general, the findings demonstrate the importance of the four main antecedent factors considered in the study in predicting individuals' trust in HIT.

5.6 Summary of Findings

This chapter presented the quantitative analysis of the collected survey data in testing the structural relationships in the proposed research model. The hypothesis testing was followed by a series of supplementary analyses to validate some of the results and to gain insight into findings that were contrary to hypothesized expectations. The key findings from the various analyses are briefly outlined below.

The study proposed perceived attitude of health workers (HW_ATT), perceived effectiveness of government regulation (REGUL), trust in healthcare providers (T_PROV), and privacy risk (RISK) as antecedents to trust in HIT (T_HIT) and PHI privacy concerns (PHIPC). Regarding T_HIT, RISK was found to be the strongest predictor, with a negative effect. T_PROV was found to mediate the positive relationship from HW_ATT to T_HIT fully, and from REGUL to T_HIT partially.

In the case of PHI privacy concerns (PHIPC), unexpected results were observed for the antecedent factors. RISK had a significant negative influence on PHIPC despite the hypothesized positive effect. Similarly, T_PROV mediated the positive (despite the hypothesized negative) relationship from HW_ATT to PHIPC fully, and from REGUL to PHIPC partially. To gain insight into these contrary findings, based on the factor structure of PHIPC supported by the data, PHIPC was remodelled as consisting of two key dimensions: PHI collection concerns (PHI_COLC) and PHI management concerns (PHI_MgtC). A series of post hoc analyses revealed the effects of the antecedent factors on PHI_MgtC to be the same as their effects on the overall PHIPC. A minor exception is the negative influence of RISK on PHI_MgtC which was insignificant. However, RISK had a strong positive influence on PHI_COLC. The remaining three antecedents (HW_ATT, REGUL and T_PROV) had negative but marginal effects on PHI_COLC. Thus, the influence of the antecedent factors on PHI_COLC and on PHI_MgtC differed significantly.

The study also examined factors that influence individuals' willingness to disclose PHI in order to receive care from healthcare providers in a digitized healthcare setting. Convenience and trust in HIT were each found to have a significant positive influence on willingness to disclose PHI (WILL). Trust in HIT also fully mediated the trust in healthcare providers (T_PROV) → WILL relationship, as well as the privacy risk (RISK) → WILL relationship. Surprisingly, contradicting findings in prior research, PHI privacy concerns (PHIPC) had a strong positive influence on WILL. Further analysis revealed that this positive influence occurred through the PHI management concerns dimension of PHIPC. However, the PHI collection concerns dimension of PHIPC had a pronounced negative effect on WILL. PHI collection concerns was found to fully mediate the influence of privacy risk on WILL. Another important factor that was negatively associated with WILL was perceived inferiority (i.e., individuals' beliefs about the negative evaluation of the self by others resulting from the exposure of one's PHI).

Several individual characteristics and experience factors were controlled for in the study. Of these, computer experience was found to significantly influence trust in HIT, PHI management concerns (PHI_MgtC), and willingness to disclose PHI. Health concern also significantly influenced trust in HIT and PHI collection concerns (PHI_COLC). In contrast to prior research findings (e.g., Esmaeilzadeh, 2018a; Laric et al., 2009), males and younger individuals expressed greater PHI_COLC than females and older individuals, respectively. Further, privacy orientation was found to significantly increase PHI_MgtC, whereas privacy experience significantly influenced both PHI_COLC and PHI_MgtC. The above findings are discussed further in detail in the next chapter in relation to the existing IS privacy literature.

CHAPTER SIX: DISCUSSION

This study explores the factors that influence the willingness of individuals in developing countries to disclose their PHI in order to receive care from healthcare providers where the disclosed PHI is digitized. This chapter discusses how the findings presented in the previous chapter meet the core objectives of the study. The chapter begins by briefly outlining the study's objectives. The findings of the study are then reviewed in relation to these objectives and previous literature.

6.1 Research Objectives

The overarching aim of this study was to explore the factors that influence PHI disclosure intentions of individuals in digitized healthcare environments. The aim of the study was addressed using data collected from among the understudied population of individuals in a developing country. Specifically, samples were drawn from Ghana, a Sub-Saharan African country. The study was conducted with 3 broad objectives, namely: understanding (i) the drivers and inhibitors of PHI disclosure, (ii) the extent and antecedents of PHI privacy concerns, and (iii) the antecedents to trust in HIT. The details of these objectives are described next.

6.1.1 Drivers & Inhibitors of PHI Disclosure

The first objective was to explore the factors that drive or motivate individuals to disclose their PHI (which are called drivers) and those that inhibit or bar PHI disclosure by individuals (which are called inhibitors). Prior IS privacy research conducted in several contexts, often drawing on the privacy calculus theory, show trust and privacy concerns as the major driver and inhibitor of individuals' privacy disclosure, respectively (e.g., Anderson & Agarwal, 2011; Dinev & Hart, 2006; Malhotra et al., 2004). The target of trust often considered in prior studies, especially in the healthcare context, is the technology artefact through which online services are provided (e.g., Anderson & Agarwal, 2011; Dinev et al., 2016). In addition to trust in HIT, this study also examined the influence of trust in healthcare providers on individuals' willingness to disclose PHI. Also, following Dinev et al. (2016), convenience was examined as another driver of willingness to disclose PHI.

As highlighted earlier, privacy concerns is considered in prior research as a major inhibitor to personal information disclosure. Another important inhibitor often considered alongside privacy concerns is privacy risk (e.g., Dinev & Hart, 2006) which reflects individuals' beliefs that high potential for loss is associated with information disclosure especially in online settings (Malhotra et al., 2004). However, the impact of the negative consequences that individuals perceive may result from privacy loss on personal information disclosure have yet to be considered in privacy empirical models. A number of studies have suggested that the dread of the negative consequences that individuals perceive of a given disclosure may cause them to take preventive actions including refusing disclosure of their information (Goldman, 1998;

Karwatzki et al., 2017; Petronio, 2002). Individuals can suffer grave consequences (e.g., job or relationship loss) from the compromise of health information due to its highly sensitive nature. Consequently, in addition to PHI privacy concerns and privacy risk, this study explored the impact of the negative consequences of disclosure on individuals' PHI disclosure. Given that HIV/AIDS is a heavily stigmatized disease, especially in developing countries, the negative consequences associated with HIV/AIDS were considered. The influence of three negative consequences was examined: perceived inferiority, employment discrimination, and family rejection.

In summary, trust in HIT, trust in healthcare providers, and convenience were the drivers of PHI disclosure considered in this study. The inhibitors included PHI privacy concerns, privacy risk, and the three perceived negative consequences of PHI disclosure: perceived inferiority, employment discrimination, and family rejection. The privacy calculus theory was leveraged in examining the influence of the drivers and inhibitors on individuals' willingness to disclose PHI.

6.1.2 Extent and Antecedents of PHI Privacy Concerns

As noted in the preceding section, privacy concerns is considered as a major factor that prevents individuals from disclosing their personal information including PHI (Anderson & Agarwal, 2011; Dinev & Hart, 2006). The second objective of the study, therefore, was to explore the extent of individuals' concerns about PHI privacy and the salient factors driving these concerns.

There is a dearth of research examining individuals' PHI privacy concerns and the factors driving these concerns (Kenny, 2016; Yun et al., 2019). Moreover, a number of the existing studies did not use validated measures of privacy concerns often used in IS privacy literature, whereas other studies used a single item to measure privacy concerns (e.g., King et al., 2012; Papoutsi et al., 2015; Perera et al., 2011; Vodicka et al., 2013; Wilkowska & Ziefle, 2012). Compared to these studies, using the Concern for Information Privacy (CFIP) instrument (Smith et al., 1996), this study measured PHI privacy concerns as a multi-dimensional construct consisting of four dimensions: collection, errors, secondary use, and unauthorised access.

In recent years, a number of studies have explored antecedents to PHI privacy concerns drawing on the broader set of antecedents studied in other IS contexts. To date, individual characteristics including age, gender, education and health status have been the often-studied antecedents to PHI privacy concerns (e.g., Esmaeilzadeh, 2018a; Laric et al., 2009). Individual experience factors such as computer experience and privacy experience (i.e., past experience of privacy violation) have also been explored in a few studies (e.g., Bansal et al., 2010; Perera et al., 2011).

Taken into consideration the geographic context of this study, the study explored four antecedent factors which have yet to receive considerable attention in prior research: perceived

attitude of health workers, perceived effectiveness of government regulation, trust in healthcare providers, and privacy risk. To account for the variance in PHI privacy concerns that might be explained by other factors, the individual characteristics and individual experience factors considered in past studies were used as control variables. Additionally, the influence of privacy orientation (i.e., the extent to which one wants to guard and limit access to his personal information), which has been found in other IS contexts as a significant predictor of privacy concerns (e.g., Taylor et al., 2015; Yao et al., 2007) was also controlled.

6.1.3 Antecedents to Trust in HIT

The third objective of this study consisted of exploring factors that influence individuals' trust in HIT. As noted in Section 6.1.1, prior research shows trust in a technology facilitating the provision of online services as an important driver of online privacy disclosure (e.g., Dinev & Hart, 2006). However, research exploring the antecedents to online trust is scant and hence there have been calls for more studies, especially in the healthcare context (Beldad et al., 2010; Kim, 2016).

The few limited studies in the healthcare and e-commerce contexts indicate that demographic factors such as age, gender, education, health status, and computer experience influence trust in technology including HIT (Bansal et al., 2010; Corbitt et al., 2003; Dickerson, 2003; Dutta-Bergman, 2003). In this study, the four antecedents proposed as antecedents to PHI privacy concerns were also explored as antecedents to trust in HIT: perceived attitude of health workers, perceived effectiveness of government regulation, trust in healthcare providers, and privacy risk. The five demographic factors mentioned above were also used as control variables on trust in HIT.

In summary, this study was driven by three objectives pertinent to exploring PHI disclosure behaviour of individuals in developing countries. These objectives included (i) examining the drivers and inhibitors of individuals' willingness to disclose PHI, (ii) exploring the extent of PHI privacy concerns and the determinants of these concerns, and (iii) investigating the antecedents to trust in HIT. The study employed the privacy calculus theory to examine the simultaneous influence of drivers and inhibitors of individuals' willingness to disclose PHI. It draws on justice theory and prior privacy research to explore the antecedents to PHI privacy concerns and trust in HIT.

6.2 Research Findings

In this section, the key findings of the study are briefly reviewed in line with the research objectives. To help the flow of discussion, findings related to antecedents to trust in HIT are presented first. This will be followed by a review of findings regarding the extent of PHI privacy concerns and the antecedents to these concerns. Then, findings related to the drivers and inhibitors of individuals' willingness to disclose PHI are reviewed.

6.2.1 Antecedents to Trust in HIT

The study findings provided support for the influence of the antecedent factors considered in the study on trust in HIT. Trust in healthcare providers had a strong positive influence on trust in HIT. This indicates that the trusting beliefs (i.e., benevolence, competence, and integrity) individuals develop about healthcare providers over time through their offline encounters with the providers can influence them (individuals) to believe that HIT used by the providers is reliable, safe, and has the functionality to facilitate PHI-related transactions such as storing, updating, and sharing PHI. In the e-commerce context, Kuan and Bock (2007) similarly found that trust in an offline retailer significantly predicts trust in the retailer's website. Morosan and DeFranco (2015) also show that trust in a hotel has a strong positive influence on the mobile app developed by the hotel. This lends support to the notion in the trust transference literature that individuals transfer trust from a known or familiar entity to related entities (Belanche et al., 2014; Stewart, 2003). It also suggests that if individuals perceive organizations as trustworthy, they are likely to trust online services deployed by the organization.

The results did not provide support for the direct influence of perceived attitude of health workers on trust in HIT. However, perceived attitude of health workers had a strong positive influence on trust in healthcare providers and an indirect effect on trust in HIT via trust in healthcare providers. Perceived attitude of health workers was measured in terms of the quality or fairness of interpersonal treatment (i.e., being treated with dignity and respect) that individuals receive from health workers during a healthcare service encounter. Thus, individuals' beliefs that health workers treat them with dignity and respect engender their (individuals) trust in healthcare providers which the health workers represent, and this trust, as noted earlier, is transferred to the HITs used by the healthcare providers. The strong positive relationship between perceived attitude of health workers and trust in healthcare providers extends support to the justice literature which indicates that individuals' perception of the fairness of interpersonal treatment received from a transacting party increases their trust in the transacting party or an entity which the transacting party represents (e.g., Chiu et al., 2009; Kernan & Hanges, 2002; Tyler & Degoey, 1996).

Consistent with expectations, perceived effectiveness of government regulation had a direct positive influence on trust in HIT as well as an indirect positive influence via trust in healthcare providers. Government regulations meant to protect the privacy of PHI establish procedures for the collection, use, storage, and sharing of PHI by healthcare providers. They aim to deter non-compliance with these procedures through the threat of punishment including empowering individuals with the ability to seek redress in case of privacy breaches on their PHI. To avoid punishment and other negative consequences, individuals may believe that healthcare providers would collect and use PHI appropriately and that the providers will also introduce safe and reliable HITs that will ensure that individuals' PHI are protected. It is thus understandable that perceived effectiveness of government regulation has a positive direct effect on trust in HIT and an indirect effect via trust in healthcare providers. Dinev et al. (2016) similarly found that individuals' perception of the effectiveness of privacy enhancing regulatory mechanisms positively influences trust in EHR systems. This study extends support

for the positive influence of regulations on trust in a technological artefact by showing the partial mediating role of the organization deploying the technology on this relationship.

Privacy risk was found to exert a pronounced negative effect on trust in HIT. This is not surprising as the greater risk of PHI privacy loss that individuals perceive of the electronic storage of PHI the less trust they may have in the functionality, reliability, and safety of HITs for the management of their PHI. The result is consistent with findings in the general Internet context that perceived Internet privacy risk decreases trust in the Internet (Dinev & Hart, 2006).

Of the individual factors considered as antecedents, computer experience was positively related to trust in HIT. As individuals with greater computer experience are likely to be more knowledgeable about various computer technologies, it is reasonable that they may appreciate more the capacity of HITs for the reliable and safe storage, use, and communication of PHI. In a study in the e-commerce context, Corbitt et al. (2003) similarly found that individuals who had greater experience in using the Internet were more trusting of e-commerce websites.

Similar to computer experience, individuals who were more concerned about their health had increased trust in HIT. In a related study, however, Bansal et al. (2010) found that individuals who perceived their health to be poor had less trust in a health website. More studies are needed therefore to clarify the nature and direction of the influence of individuals' perception of their health condition on trust in HITs.

6.2.2 Understanding PHI Privacy Concerns

This section reviews the findings regarding the extent of PHI privacy concerns among individuals in developing countries and the factors influencing these concerns.

6.2.2.1 Extent of PHI Privacy Concerns

Using the Concern for Information Privacy (CFIP) instrument (Smith et al., 1996), PHI privacy concerns (PHIPC) was measured as a multi-dimensional construct consisting of four dimensions: collection, errors, secondary use, and unauthorised access. The construct statistics provided in Table 5.2 show that collection has a considerably lower mean (3.36) than the other dimensions which ranged from 6.01 to 6.37. This indicates that individuals are less concerned about the collection of their PHI by healthcare providers. However, they are highly concerned about what happens after their PHI has been collected and stored electronically, i.e., they are concerned about errors, the secondary use of, and unauthorised access to their PHI.

The study results regarding the CFIP dimensions are consistent with findings reported in some past studies. In examining privacy concerns regarding electronic medical records, Hwang et al. (2012) found that individuals' concerns about errors, secondary use, and unauthorised access were greater than their concerns regarding the collection of their health information by hospitals. Similarly, reviewing empirical studies in the broader IS privacy literature, Hong and

Thong (2013) observed that the collection dimension has a lower mean and average correlation than the other three CFIP dimensions. This is quite surprising given that collection is a necessary antecedent to the other three dimensions of CFIP (Hong & Thong, 2013), and that it is seen as one of the most important dimensions of information privacy (Hann et al., 2007).

The literature review in Chapter 2 shows the lack of control over one's personal information as the main source of privacy concerns (Stewart & Segars, 2002). Out of the four CFIP dimensions, individuals may have some degree of control over the collection of their personal information compared to the other three dimensions (i.e., errors, secondary use, and unauthorised access) where little or no control may exist once the data has been collected. For instance, in some healthcare contexts such as considered in this study, the collection of an individual's PHI may occur through the individual's honest disclosure during a consultation with health workers (e.g., doctors, nurses, etc.) or information generated through various medical tests which the individual submits to. Thus, the lower concerns regarding the collection dimension of CFIP compared to the other dimensions may be due to the degree of control individuals feel they have over the initial disclosure and therefore the collection of their PHI.

6.2.2.2 Antecedents to PHI Privacy Concerns

To explore the antecedents to PHI privacy concerns (PHIPC), following past studies (e.g., Esmaeilzadeh, 2018a; Stewart & Segars, 2002), PHIPC was modelled as a second-order construct comprising of the four dimensions of CFIP: collection, errors, secondary use, and unauthorised access. Three of the core antecedent factors considered in the study (i.e., perceived effectiveness of government regulation, trust in healthcare providers, and privacy risk) had significant but unexpected effects on PHIPC. Perceived attitude of health workers had an indirect effect on PHIPC via trust in healthcare providers.

Unexpectedly, the results further suggested that the second-order model of PHIPC was not well supported by the data as the collection dimension did not converge well with the other three CFIP dimensions (i.e., errors, secondary use, and unauthorised access) which may explain the divergent findings. Further analysis provided support for the two-factor structure of CFIP suggested in Stewart and Segars (2002): *PHI collection concerns* and *PHI management concerns*, where the latter reflects concerns regarding errors, secondary use, and unauthorised access. In general, the results of the PHI management concerns model were consistent with the overall PHIPC model with the only exception being the negative influence of privacy risk on PHI management concerns which was insignificant. The PHI collection concerns model, however, showed significant differences with privacy risk being the only significant predictor, while the other three core antecedents (perceived attitude of health workers, perceived effectiveness of government regulation, and trust in healthcare providers) were insignificant. Individual factors such as computer experience and privacy orientation were significant regarding PHI management concerns, whereas gender, age, and health concern significantly influenced PHI collection concerns. Privacy experience was significant in both models. These findings are discussed next.

In contrast to expectations, trust in healthcare providers was found to significantly increase PHIPC with further analysis showing that it increases PHI management concerns, whereas it had no significant impact on PHI collection concerns. Trust in healthcare providers was measured in terms of the trusting beliefs of benevolence, competence, and integrity. Individuals may trust the benevolence and integrity of healthcare providers as well as their competency in providing needed care services. However, they may not trust the ability of the providers to properly manage their digitized PHI. This probably explains why trust in healthcare providers is positively associated with PHI management concerns. Lending support to this speculation, in a recent study, Kenny and Connolly (2016) similarly found that individuals' trust in healthcare professionals' benevolence and integrity with individuals' health data does not decrease but rather increase health information privacy concerns. The insignificant effect of trust in healthcare providers on PHI collection concerns may be due to individuals' perceptions that they have control over what PHI they disclose to healthcare providers obviating the need for trust in the providers regarding the collection of their PHI. Future research should investigate the relationship between trust in healthcare providers and the two dimensions of PHIPC further as the relationship could be more nuanced than observed in this study.

Similar to the full mediating role of trust in healthcare providers on the relationship between perceived attitude of health workers and trust in HIT as discussed in Section 6.2.1, trust in healthcare providers was found to fully mediate the influence of perceived attitude of health workers on PHI management concerns. These results suggest that individuals' perceptions of the attitude of health workers, i.e., their beliefs about the quality of interpersonal treatment received from health workers, affects their trust perceptions regarding HIT and privacy perceptions through the trust that the perceptions of quality interpersonal treatment builds in the healthcare providers which the health workers represent. The direct positive relationship between perceived attitude of health workers and trust in healthcare providers extends support to the positive relationship between interactional justice (i.e., fairness/quality of interpersonal treatment) and trust in a transacting party or an entity which the transacting party represents(e.g., Chiu et al., 2009; Kernan & Hanges, 2002; Tyler & Degoey, 1996). More research is needed to shed light on the influence of individuals' perceptions regarding the attitude of health workers on their trust and privacy perceptions.

Trust in healthcare providers was also found to partially mediate the influence of perceived effectiveness of government regulation on PHI management concerns. However, when the influence of individual factors (e.g., computer experience, privacy orientation, and privacy experience) are controlled for, the direct effect from perceived effectiveness of government regulation to PHI management concerns becomes insignificant and trust in healthcare providers fully mediates this relationship. In the context of location-based services, Xu et al. (2012) similarly found a significant influence of government regulation on privacy concerns. In further analysis, the authors also found that the direct influence of government regulation on privacy concerns becomes insignificant in the presence of perceived control which has a strong negative influence on privacy concerns. This suggests that the influence of government regulation on privacy concerns may be mediated by other variables. This study provides some

insights showing that individuals' trust in the organization collecting and using their PHI, in this case, healthcare providers, mediates the effect of perceived effectiveness of government regulation on concerns regarding PHI management.

Consistent with the positive relationship between risk beliefs and privacy concerns often observed in past studies including in the healthcare context (Dinev & Hart, 2006; Kenny & Connolly, 2016; Xu et al., 2008), privacy risk had a strong positive influence on PHI collection concerns. That is the greater the risks individuals perceive of the electronic storage of PHI the more concerned they are about the collection of their PHI. However, RISK had no significant impact on concerns regarding PHI management (i.e., once the data is collected and stored electronically). These results highlight the importance of assuring individuals that their PHI if provided, would be protected and stored safely.

The study also found support for the influence of individuals' characteristics and experience-related factors on concerns about PHI privacy. In terms of individual experiences, computer experience was found to increase PHI management concerns. This contradicts a Canadian study which found that patients who were frequent computer users were less concerned about the privacy of computerized health information (Perera et al., 2011). This suggests that individuals' concerns about privacy may change over time with increased computer experience. As individuals become more knowledgeable about the capabilities of computer systems for managing personal information and the threats posed to the privacy of digitized information, their concerns regarding electronically stored information may be heightened. This suggests the need for healthcare providers to provide individuals with the assurance that their collected and electronically stored PHI will be kept safe.

Surprisingly, contradicting past studies (e.g., Bansal et al., 2010; Zviran, 2008), privacy experience (i.e., past experience of privacy invasion) was found to exert a pronounced negative effect on PHIPC. Further analysis found that privacy experience increased PHI collection concerns, which was expected. However, it had a significant negative influence on PHI management concerns. It is not clear what may account for the observed negative relationship between privacy experience and PHI management concerns. However, since PHI collection concerns was negatively correlated with PHI management concerns, the differential impacts of privacy experience on these sub-dimensions of PHIPC further suggest the need to explore the nuances of the relationship between PHIPC and its antecedents and consequences.

Regarding individual characteristics, age had a significant negative influence on PHI collection concerns, indicating that older individuals were less concerned than younger individuals about the collection of their PHI. However, age had no significant impact on PHI management concerns. This contradicts the findings in past studies that older individuals express greater concerns about PHI privacy (e.g., Ancker et al., 2013; Laric et al., 2009; Papoutsi et al., 2015). The result in this study could be due to older individuals being more susceptible to health problems and so more willing to share their health information with healthcare providers in order to receive needed care. In support of this speculation, some recent studies show that older individuals are more willing to share clinical information in online health communities for

various purposes including seeking feedback and advice on their specific conditions (Frost et al., 2014; Kordzadeh & Warren, 2017). It is, however, not clear why younger individuals may express greater concerns regarding the collection of their PHI. Thus, the relationship between age and concerns about PHI privacy needs to be examined further, especially in developing countries.

Similar to age, gender was not significant in relation to PHI management concerns. However, males were found to be more concerned about the collection of their PHI than females. This contrasts with past studies which have found that females express greater PHI privacy concerns (Laric et al., 2009; Perera et al., 2011; Vodicka et al., 2013). A possible explanation for this finding in this study may be the higher computer experience of males compared to females. Out of 59 (21.4%) individuals who have never used computers before, the majority were females (N=37, 62.7%). On the other hand, for the 106 (38.4%) individuals who have higher computer experience (over 7 years of experience), most of them were males (N=68, 64.2%). The chi-square test for independence confirmed the significant association between gender and computer experience: $X(3)=13.657$, $p=0.003$. The observed relationship between gender and computer experience is consistent with recent studies indicating that gender digital gap is wider in developing countries, especially Africa (ITU, 2016, 2017). Due to their higher computer experience, males may be more aware of the high risks associated with electronic information leading to their concerns about PHI collection for electronic storage. However, given this is speculative, further investigation of the relationship between gender and PHI privacy concerns is needed in the context of developing countries.

Individuals who were more concerned about their health expressed greater concerns about the collection of their PHI by healthcare providers. Some past studies have found individuals with sensitive health conditions such as mental illness to express higher concerns about PHI privacy (e.g., Flynn et al., 2003; Laric et al., 2009). In line with these past studies, the finding in this study may be due to the fact that individuals who express more concerns about their health have sensitive health conditions and therefore they are concerned about healthcare providers collecting information related to these conditions.

Consistent with past studies which show that individuals with greater dispositional desire for privacy express greater privacy concerns (Taylor et al., 2015; Yao et al., 2007), privacy orientation was found to increase PHI management concerns. Given the highly sensitive and personal nature of most health information, it is not surprising that individuals who desire to keep personal information confidential (i.e., people high in privacy orientation) will express greater concerns about the management of their electronically stored PHI. The results, however, showed that privacy orientation had no significant impact on concerns about PHI collection. This may be due to individuals' belief that they have greater degree of control over the collection of their PHI such that it does not have a significant impact on their privacy concerns.

6.2.3 Drivers & Inhibitors of PHI Disclosure

The study explored the influence of factors that drive or motivate individuals to disclose their PHI (i.e., drivers) and those that inhibit PHI disclosure by individuals (i.e., inhibitors). Convenience, trust in HIT, and trust in healthcare providers were the drivers of individuals' willingness to disclose PHI considered in the study. The set of inhibitors included PHI privacy concerns, privacy risk, and the three perceived negative consequences of PHI disclosure: perceived inferiority, employment discrimination, and family rejection.

The study found support for the positive influence of convenience on willingness to disclose PHI, indicating that the less effort and time individuals perceive they will spend in receiving care as a result of digitized healthcare, the greater their willingness to disclose their PHI to healthcare providers for digitization. This is consistent with past studies which show that the benefits individuals expect to receive from disclosing their PHI increase their PHI disclosure intentions in various digitized healthcare environments (Anderson & Agarwal, 2011; Ermakova et al., 2014; Esmaeilzadeh, 2018b; Kordzadeh & Warren, 2017).

The examination of the influence of trust on individuals' willingness to disclose PHI found that trust in HIT was a significant predictor, whereas trust in healthcare providers did not have a significant direct effect. However, trust in healthcare providers had an indirect effect on willingness to disclose PHI through trust in HIT. The majority of past studies have focused on the relationship between trust in technology including HIT and information disclosure and have found strong support for this relationship (Anderson & Agarwal, 2011; Bansal et al., 2016; Dinev & Hart, 2006; Jena, 2015). A few studies, especially in the e-commerce context, have also found support for the positive influence of trust in organization (e.g., online retailers) on willingness to provide information (Belanger et al., 2002) or willingness to transact online (Van Slyke et al., 2006). The results in this study, however, indicate that when trust in technology facilitating the provision of electronic services and trust in the organization (in this case healthcare providers) using the technology are examined together, trust in technology fully mediates the influence of trust in the organization on information disclosure. Clearly, more research is needed to elucidate further the relative influence of trust in organization and trust in technology on information disclosure.

In terms of inhibitors of PHI disclosure, surprisingly, contradicting past studies which show that PHI privacy concerns negatively influence individuals' PHI disclosure intentions (Anderson & Agarwal, 2011; Bansal et al., 2010; Kordzadeh & Warren, 2017), PHI privacy concerns was found to strongly increase willingness to disclose PHI. Further analysis, however, revealed that individuals' concerns about collection of their PHI (i.e. PHI collection concerns) strongly decreased willingness to disclose PHI, whereas their concerns regarding the management of their PHI once it has been collected and stored electronically (i.e., concerns related to errors, secondary use, and unauthorised access) increased their willingness to disclose PHI. These divergent findings may be due to individuals' perceptions of control over their PHI coupled with their need for care. Individuals may perceive they have control over the collection of their PHI which lowers their PHI collection concerns and increases their

willingness to disclose PHI to receive needed care. However, as control may be lost when PHI is disclosed, concerns about management of PHI increase and yet due to the need for care individuals may still disclose PHI. This lends support to the *"privacy paradox"* documented in some past studies: that despite the high level of concerns for personal information privacy, consumers disclose their sensitive information for various benefits including personalized shopping experience (Chellappa & Sin, 2005) and convenience or discounts (Spiekermann et al., 2001). Overall, the results of the study suggest that the relationships between the dimensions of PHI privacy concerns and PHI disclosure may be more complex and point to a need for more research to examine these relationships.

The study found no support for a significant direct effect of privacy risk on willingness to disclose PHI. However, privacy risk had an indirect effect on willingness to disclose PHI via PHI collection concerns and also through trust in HIT. In the Internet context, Dinev and Hart (2006) similarly found that Internet trust and Internet privacy concern each mediates the influence of perceived Internet privacy risk on consumers' willingness to disclose personal information to engage in transactions on the Internet. In addition, Dinev and Hart (2006) found a direct negative influence of perceived Internet privacy risk on willingness to disclose personal information. Malhotra et al. (2004) also found privacy risk to decrease intentions to disclose information to online firms through the Internet. It is not clear why the relationship between privacy risk and willingness to disclose PHI was not supported in this study, and thus further investigation of this relationship is needed.

The study also explored the influence of the negative consequences that individuals perceive may result from PHI privacy loss on their willingness to disclose PHI. Three negative consequences associated with HIV/AIDS were considered: perceived inferiority, employment discrimination, and family rejection. Perceived inferiority was found to significantly decrease willingness to disclose PHI. Thus, individuals' perceptions that they will be negatively evaluated by others (i.e., perceived inferiority) should their PHI be exposed, in this case, PHI indicating one has HIV/AIDS, decrease their willingness to disclose PHI. Surprisingly, however, neither employment discrimination nor family rejection had a significant impact on willingness to disclose PHI. Individuals, in general, are said to believe that they are less likely than others to experience negative events (i.e., optimistic bias) (Dinev et al., 2015; Taylor & Brown, 1988). This may be especially true if individuals have no prior experience of the negative events in question. The insignificant influence of employment discrimination and family rejection in the study may be due to individuals' discounting or underestimating the possibility that they will experience employment discrimination and family rejection should their sensitive PHI be exposed probably due to no prior experience of such consequences. Thus, future studies including individuals living with sensitive conditions such as HIV/AIDS or knowing of others with the conditions are required to explore further the influence of negative consequences of PHI disclosure on individuals PHI disclosure decisions.

Of the control variables considered, only computer experience significantly influenced willingness to disclose PHI. Specifically, individuals with higher computer experience were found to be more willing to disclose their PHI. This may be because individuals with greater

computer experience may be more knowledgeable about the capabilities of computer systems for managing PHI to support effective and quality healthcare delivery. They likely also appreciate the need to have their PHI digitized in order to benefit from digitized healthcare systems. It is thus reasonable that these individuals are more willing to disclose their PHI.

In summary, the findings of the study indicate that individuals' willingness to disclose PHI is influenced by both factors that motivate individuals to disclose PHI (drivers) and those that inhibit their PHI disclosure (inhibitors). The study thus provides support for the privacy calculus notion that antecedents influencing behavioural intention can be contrary, and that their relative influence must be considered in an effort to understand planned behaviour (Dinev & Hart, 2006).

6.3 Chapter Summary

This chapter discussed the finding of the quantitative results presented in the previous chapter. The findings were discussed in light of the study's objectives and prior research. The next chapter discusses the theoretical and practical implications of the findings.

CHAPTER SEVEN: CONTRIBUTIONS AND IMPLICATIONS

The previous chapter discussed the findings of the study. This chapter first discusses the contributions to theory and implications of the findings for practice. Next, the limitations of the study and directions for future research are presented. The chapter concludes with a summary of the study.

7.1 Contributions to Theory

This study explores PHI disclosure intentions of individuals in developing countries in digitized healthcare environments. More specifically, it seeks to understand (i) the factors that motivate or encourage individuals' willingness to disclose PHI (i.e., *drivers*) and those that discourage their PHI disclosure (i.e., *inhibitors*), (ii) the extent and antecedents of PHI privacy concerns, and (iii) the antecedents to trust in HIT. The study leverages privacy calculus theory to examine the simultaneous influence of contrary factors (i.e., drivers and inhibitors) on willingness to disclose PHI. It explores the antecedents to PHI privacy concerns and trust in HIT drawing on prior research and on the procedural and interactional dimensions of justice theory.

The study makes important contributions to IS privacy research in general and to the privacy research specifically related to the healthcare context. It extends the privacy calculus to incorporate several drivers and inhibitors of PHI disclosure thereby improving our understanding of the conflicting factors that influence individuals' personal information disclosure behaviours in the healthcare context. Also, it explores antecedents to trust (as a driver) and privacy concerns (as an inhibitor), which are two important factors considered to be the core relationships in the privacy calculus (Anderson & Agarwal, 2011). Lastly, the study contextualizes the privacy calculus to the healthcare and developing country context. These contributions are discussed next.

The study extends understanding of the drivers of personal information disclosure often considered in the privacy calculus. In line with suggestions in some prior research (e.g., Dinev & Hart, 2006; Yoo et al., 2013), this study considered convenience as a key benefit individuals expect to gain from disclosing PHI for digitization. Further, following recommendations in prior research (e.g., Beldad et al., 2010; Dinev et al., 2016), the study explored two aspects of trust as additional drivers of PHI disclosure: trust in a technology facilitating the provision of an online service (in this case HIT) and trust in the organization deploying the technology to provide the online service (in this case healthcare providers). Much of the prior studies using the privacy calculus has usually focused on the benefits individuals expect from disclosing their personal information as the only factor motivating their personal information disclosure or adoption of ITs (e.g., Kordzadeh & Warren, 2017; Xu et al., 2009). Other studies have considered trust as the main driver in the privacy calculus (e.g., Anderson & Agarwal, 2011) or explored trust as a driver in addition to the benefits individuals expect from disclosing personal information (e.g., Dinev & Hart, 2006). However, the existing studies that have considered trust have focused largely on one aspect of trust, i.e., trust in the technology, which

facilitates online service provision (e.g., Anderson & Agarwal, 2011; Dinev et al., 2016; Dinev & Hart, 2006). By considering a dyadic conceptualization of trust (i.e., trust in HIT and trust in healthcare providers) in addition to convenience as drivers of PHI disclosure, the study extends prior research by improving our understanding of the relative influence of these important drivers of PHI disclosure. Further, the study explored the relationship between the two trust dimensions as well as the antecedents to these dimensions. It has thus provided insights into the important factors forming individuals' trust beliefs and how trust ultimately influences willingness to disclose PHI.

Similar to the drivers of PHI disclosure, the study also examined a comprehensive model of the inhibitors to PHI disclosure, improving our understanding of the salient factors that discourage individuals' PHI disclosure. Aside from privacy risk and privacy concerns, the main inhibitors of personal information disclosure often considered in studies using the privacy calculus (e.g., Dinev & Hart, 2006, Kordzadeh & Warren, 2017), this study has explored and shown that the negative consequences individuals perceive may result from PHI privacy loss may further decrease their willingness to disclose PHI. This study thus contributes to IS privacy research by highlighting the need to go beyond conceptualizations of privacy risk that focus on the likelihood of losing ones' privacy associated with personal information disclosure (e.g., Malhotra et al., 2004), to consider also specific negative consequences that may arise from the privacy loss of personal information in an individual's risk calculus analysis.

Another extension to the privacy calculus of PHI disclosure relates to the conceptualization of PHI privacy concerns in this study. In contrast to most prior studies which conceptualized PHI privacy concerns as a unidimensional construct (e.g., King et al., 2012; Vodicka et al., 2013), this study examined PHI privacy concerns across four dimensions (Smith et al, 1996): collection, errors, secondary use, and authorised access. The results of the study suggest that while individuals have less concern about the collection of their PHI, they have greater concerns regarding errors, secondary use and unauthorised access. Recognizing these differences and extending prior research, this study further explored two underlying dimensions of PHI privacy concerns: i.e., concerns about PHI collection and concerns about PHI management (i.e., concerns related to errors, secondary use, and unauthorised access). The two sub-dimensions were related differently to the antecedent factors and outcome variable, i.e., willingness to disclose PHI, considered in the study. The examination of PHI privacy concerns in the study makes an important contribution to the existing literature, showing that the role of PHI privacy concerns may be more nuanced than how it has normally been represented in prior studies (e.g., Esmaeilzadeh, 2018a), and it may be better understood by looking closely at the aspects that make up overall PHI privacy concerns. The insights provided in the study confirm the need for a more comprehensive and granular examination of privacy concerns in the healthcare context (Kenny, 2016; Yun et al., 2019).

Finally, in recent years, there have been calls for the integration of context in theory development in IS research (Hong et al., 2014). Important contextual factors include the characteristics and usage contexts of an IT artefact and the characteristics of the users of the artefact (Hong et al., 2014). The healthcare context is considered unique compared to other IS

domains due to factors such as the sensitive nature of most PHI and severe consequences associated with their compromise, which can have implications for HIT adoption and use (Anderson & Agarwal, 2011; Dinev et al., 2016). Consequently, researchers have particularly emphasized the need to reshape existing IS constructs and theories to deal with the healthcare setting (Anderson & Agarwal, 2011; Chiasson & Davidson, 2004). Also, as argued in this study (e.g., Section 2.4.4), factors such as the digital divide in developing countries (ITU, 2016, 2017), and religion and morals, which play vital roles in the cultures of these countries (PEN, 2010), may cause privacy perceptions and its impacts to differ between individuals in developed and developing countries (Bélanger & Crossler, 2011). Therefore, it is equally important to consider the developing country context in building theoretical models especially aimed at explaining PHI disclosure behaviour.

Following recommendations for contextualizing theories in Hong et al. (2014), the research model of the study based on the privacy calculus adapted existing constructs (e.g., convenience, trust, privacy concerns) as well as introduced new constructs (e.g., negative consequences associated with PHI disclosure and perceived attitude of health workers), taking into consideration the healthcare and the developing country context. The resultant model provides valuable insights, which serve as actionable advice to practitioners. For example, the study shows that a major way in which healthcare providers can build individuals' trust in them and ultimately encourage their (individuals) PHI disclosure is by ensuring that individuals receive quality interpersonal treatment during a healthcare service encounter. According to Mathieson (1991), if a theoretical model does not provide valuable information to practitioners, it is of no use to practice regardless of how well it predicts. Thus, by contextualizing the privacy calculus to the healthcare and the developing country context and providing actionable insights as a result, this study has responded to the increasing calls for practical relevance in IS research (e.g., Benbasat & Zmud, 1999; Chiasson & Davidson, 2005). Further, by adapting existing constructs developed and used in various IS domains in the western contexts to the healthcare context of a developing country, the study contributes to both the construct validity and external validity of the measures of these constructs.

In general, the study has presented a comprehensive model, which has enhanced our understanding of the complex process that leads to individuals' decisions about disclosing PHI. Similar to prior studies using the lens of the privacy calculus theory, the study shows that individuals weigh contrary factors (i.e., drivers and inhibitors) where the strength of one factor may override the strength of another and ultimately influence the decision to disclose PHI. However, extending prior research most of which have focused on a few conflicting factors in the privacy calculus (e.g., Kordzadeh & Warren, 2017; Xu et al., 2009), this study has introduced new constructs (e.g., negative consequences associated with PHI disclosure), decomposed the core constructs usually considered in prior research (i.e., trust and privacy concerns) into specific relevant dimensions as well as explored relevant antecedents to these dimensions. By investigating such a more comprehensive model of the privacy calculus of PHI disclosure, the study has provided a more comprehensive understanding and in-depth insight into the relative importance of conflicting factors that influence PHI disclosure intentions and the important antecedents influencing some of these factors.

The sections that follow (Sections 7.1.1 to 7.1.4) further discuss in detail the theoretical contributions of the study across the study objectives outlined in the introduction of this section as well as additional contributions arising from the scope of the study.

7.1.1 Drivers and Inhibitors of PHI Disclosure

As discussed above in Section 7.1, drawing on the privacy calculus theory, this study examined the influence of contrary factors (i.e., drivers and inhibitors) on individuals' willingness to disclose PHI. The set of drivers considered were convenience and trust. On the other hand, PHI privacy concerns, privacy risk and negative consequences associated with PHI disclosure comprised the inhibitors. The study contributes to the existing IS privacy research in terms of the conceptualization of trust and PHI privacy concerns as well as the introduction of negative consequences associated with PHI disclosure as inhibitors in the privacy calculus. The contributions related to trust and negative consequences of PHI disclosure are discussed below, whereas the contribution regarding PHI privacy concerns is discussed in the next section.

This study explored a dyadic conceptualization of trust (i.e., trust in healthcare providers and trust in HIT) in the privacy calculus. Trust is an important construct in IS privacy research which has a strong impact on behaviour (Dinev & Hart, 2006; Miltgen et al., 2013). In the context of online or electronic transactions, the technology facilitating the transactions and the organization deploying the technology are considered as the proper objects of trust (Beldad et al., 2010; Dinev et al., 2016; Morosan & DeFranco, 2015; Tan & Thoen, 2000). However, the existing privacy studies, including in the healthcare context, have largely focused on either trust in technology (e.g., Dinev & Hart, 2006; Anderson & Agarwal, 2011) or trust in organization (e.g., Metzger, 2006; Klein, 2007). Confirming the salience of trust in privacy-related contexts, some of these studies show that trust in technology or trust in organization has a stronger impact on behaviour than privacy risk (Miltgen et al., 2013; Mou & Cohen, 2014) or privacy concerns (Bansal et al., 2010, 2016; Dinev & Hart, 2006; Jena, 2015; Van Slyke et al., 2006), the two commonly studied cost factors in the privacy calculus. Extending the prior research, this study examined together trust in HIT (i.e., technology trust) and trust in healthcare providers (i.e., organizational trust) and found that the influence of trust in healthcare providers on willingness to disclose PHI is fully mediated through trust in HIT. The conceptualization of trust in this study has thus helped to clarify the role of trust within IS privacy research, especially research in the healthcare context, showing the relative effects of the two trust dimensions on PHI disclosure.

As another contribution of this study, it extended the cost side of the privacy calculus to account for specific negative consequences associated with PHI disclosure. Privacy risk has been examined alongside privacy concerns as the main cost factors in the privacy calculus (Dinev & Hart, 2006). Privacy risk has often been defined as the expectation of negative consequences (or a high potential for loss) associated with personal information disclosure (Dinev et al., 2013; Malhotra et al., 2004). Negative consequences are often operationalized in a general

sense, referring to potential loss of control over personal information (e.g., Dinev & Hart, 2006; Xu et al., 2009). Therefore, it is not known what are the specific negative consequences that individuals may perceive to result from losing control over their personal information (Karwatzki, et al., 2017).

In addition to overall privacy risk, this study identified and explored the influence of specific negative consequences that individuals may perceive to result from PHI privacy loss on their PHI disclosure intentions. Drawing on the healthcare literature, the study considered three negative consequences related to a specific health condition , HIV/AIDs: perceived inferiority (an emotional consequence) (Goss et al., 1994), employment discrimination (an economic consequence) (Laric et al., 2009; Sprague et al., 2011), and family rejection (a social consequence) (Kwansa, 2013). The study found support for the negative association between perceived inferiority and willingness to disclose PHI, whereas no significant support was found for employment discrimination and family rejection. This lends support to the suggestions by some researchers (e.g., Karwatzki et al., 2017; Petronio, 2002) that the negative consequences individuals perceive to be associated with a given personal information disclosure may influence their behaviour (e.g., refusing information disclosure) even when the actual consequences have not occurred.

This study thus extends the operationalization of privacy risk in the existing literature by articulating specific negative consequences that impact individuals' PHI disclosure. It has highlighted the need to account for specific negative consequences associated with personal information disclosure in the calculus analysis of risks. For instance, future research can explore the relationship between individuals' expectations of losing control over their personal information (i.e., privacy risk) and the negative consequences they perceive may result from such loss. In general, by exploring specific negative consequences associated with PHI disclosure, this study responds to calls to examine diversity of privacy harms in IS privacy research (Kokolakis, 2015).

7.1.2 Understanding PHI Privacy Concerns

The study makes two contributions to the limited research examining privacy concerns in the healthcare context.

First, this study provides insights into the dimensions of PHI privacy concerns and their relative importance to individuals. Privacy concerns is considered a critical construct in IS privacy research which serves as a major deterrent to personal information disclosure (Smith et al., 2011). It is especially important in the healthcare context given the highly sensitive nature of health information (Gostin & Nass, 2009; Romanow et al., 2012). Despite its importance, however, there has been inadequate measurement of PHI privacy concerns in most studies. Validated measures of privacy concerns in IS privacy research are often not used and a good number of studies use a single item, examining PHI privacy concerns as a unidimensional

construct (e.g., King et al., 2012; Vodicka et al., 2013; Wilkowska & Ziefle, 2012). The existing studies, therefore, only capture individuals' overall concerns about PHI privacy.

Addressing the above limitations, this study, using the Concern for Information Privacy (CFIP) instrument (Smith et al., 1996), took a multi-dimensional approach and examined PHI privacy concerns across four dimensions: collection, errors, secondary use, and unauthorised access. The results of the study showed that individuals have less concern about the collection of their PHI, but greater concerns regarding errors, secondary use, and unauthorised access. The study has therefore provided insights into the dimensions of PHI privacy concerns and their relative importance to individuals, which would not otherwise have been obtained with unidimensional measurement of PHI privacy concerns.

Given the negative correlation between collection and the other three dimensions of PHI privacy concerns, having taken a multi-dimensional approach, this study further explored a two-dimensional structure of PHI privacy concerns: PHI collection concerns and PHI management concerns (i.e., concerns regarding errors, secondary use, and unauthorised access). The results of the study indicate that the two dimensions have differential impacts on PHI disclosure and that these dimensions are also differentially impacted by the same antecedent factors. As an example, whereas past experience of privacy violation increases PHI collection concerns, it decreases PHI management concerns. The study thus extends current understanding provided by the limited prior studies using the CFIP measure (e.g., Angst & Agarwal, 2009; Esmaeilzadeh, 2018a) by demonstrating that individuals distinguish between PHI collection concerns and PHI management concerns. It represents a call for future research to go beyond the treatment of PHI privacy concerns as a second-order construct (e.g., Esmaeilzadeh, 2018a) to consider alternative representations of the construct.

By exploring PHI privacy concerns as a multi-dimensional construct, this study responds to calls for a comprehensive examination of privacy concerns in the healthcare context to gain deeper insights into the facets of individuals' PHI privacy concerns (Kenny, 2016; Yun et al., 2019).

Second, the study has also provided insights into the salient factors that influence PHI privacy concerns by exploring a comprehensive set of factors as antecedents. Despite the importance of privacy concerns in the healthcare context, scant research has focused on the factors influencing individuals' PHI privacy concerns. Also, the existing studies have focused on a small number of antecedents which are largely related to individual characteristics such as age, gender, education, and health status (e.g., Papoutsi et al., 2015; Wilkows & Ziefle, 2012).

Extending the prior research, this study explored factors related to individual perceptions as antecedents controlling for the individual characteristics and experience-related factors studied in prior research. Empirical support was found for the influence of a number of the antecedents on the two dimensions of PHI privacy concerns identified in the study: PHI collection concerns and PHI management concerns. Age, gender, health concern, privacy experience, and privacy risk were found to influence PHI collection concerns. On the other hand, PHI management

concerns was shaped by computer experience, privacy experience, privacy orientation, and trust in healthcare providers. Perceived attitude of health workers and perceived effectiveness of government regulation indirectly influenced PHI management concerns through trust in healthcare providers.

In summary, this study extends the current understanding of the varying effects of the antecedent factors on PHI privacy concerns, showing that these differ at the sub-dimensional level. It also answers calls in recent studies to examine privacy concerns at a more granular level focusing on the antecedents to the dimensions of privacy concerns (Xu et al., 2012). In general, understanding the factors that influence individuals' PHI privacy concerns is critical to developing appropriate measures to address these concerns. In this regard, this study adds to the small number of studies that have examined antecedents to PHI privacy concerns.

7.1.3 Antecedents to Trust in HIT

This study has improved our understanding of the important antecedents to trust in HIT. As noted above in Section 7.1.1, trust in HIT has been found in a number of studies to more strongly influence PHI disclosure behaviour or adoption of HITs than PHI privacy concerns (Bansal et al., 2010; Jena, 2015) or risks (Miltgen et al., 2013). However, there is a lack of empirical studies on factors that form individuals' trust in HITs. Prior studies typically focused on one or two antecedents (e.g., age, gender, and education) and as such these antecedents have been studied once or a few times (e.g., Bansal et al., 2010; Dickerson, 2003; Dutta-Bergman, 2003; Li et al., 2008).

Due to the paucity of empirical studies, some researchers (e.g., Beldad et al., 2010; Kim, 2016) have called for more studies to examine the antecedents to trust in HITs. In response to this call, this study explored the influence of a number of factors related to individual characteristics, experiences, and perceptions. The results showed empirical support for the influence of computer experience, health concern, privacy risk and trust in healthcare providers with the latter two factors exerting the strongest influence on trust in HIT. Trust in healthcare providers also partially mediated the influence of perceived effectiveness of government regulation but fully mediated the influence of perceived attitude of health workers on trust in HIT.

In general, by exploring a comprehensive set of antecedent factors, this study has shed light on the salient factors that influence trust in HIT and the relative importance of these factors. These insights can be leveraged to build individuals' trust in HITs which is critical to individuals' PHI disclosure (Jena, 2015) and to their adoption of HITs (Miltgen et al., 2013). This study, therefore, makes an important contribution to the scant literature on trust in the healthcare context.

7.1.4 Additional Contributions

The preceding sections discussed theoretical contributions specifically related to each of the core objectives of this study. This section discusses additional contributions related to the scope of the study (as opposed to a specific objective).

First, the study explored the influence of perceived effectiveness of government regulation and perceived attitude of health workers on PHI privacy concerns and trust beliefs drawing on the procedural and interactional dimensions of justice theory. This study is one of the few studies (e.g., Culnan & Bies, 2003; Fang & Chiu, 2010) to explore individuals' formation of trust beliefs and privacy concerns using the justice theoretical framework. In this study, procedural justice and interactional justice were linked respectively with perceived effectiveness of government regulation and perceived attitude of health workers. The results of the study showed that trust in healthcare providers fully mediated the influence of individuals' perceptions of the effectiveness of government regulation and of the attitude of health workers on PHI management concerns (i.e., concerns regarding errors, secondary use, and unauthorised access). Trust in healthcare providers also partially mediated the influence of perceived effectiveness of government regulation but fully mediated the influence of perceived attitude of health workers on trust in HIT. These results suggest that, individuals' may evaluate the fairness of interpersonal treatment they receive (i.e., interactional justice) and the fairness of procedures for the handling their PHI (i.e., procedural justice) afforded by government regulations and this may directly influence their trust in the transacting party and indirectly influence their concerns about privacy through trust in the transacting party. Much of the justice literature has focused on examining the relationships between organizations and their employees (Culnan & Armstrong, 1999). This study thus contributes to the few studies that show that the justice theoretical framework can be used to evaluate consumers' formation of trust in an organization and of concerns about the organization's information practices (e.g., Culnan & Armstrong, 1999; Culnan & Bies, 2003; Fang & Chiu, 2010).

Second, this study improves our understanding of the influence of government regulation on privacy concerns and trust beliefs. Consumers' concerns about privacy are said to result from their lack of control over their personal information (Stewart & Segars, 2002). Government regulation can ensure that individuals' personal information are collected and used fairly and this can provide individuals with a sense of control over their information (Xu et al., 2009). Yet, the influence of regulations has received scant attention in empirical models examining privacy concerns and personal information disclosure (Miltgen & Smith, 2015; Yun et al., 2019). Two studies in healthcare show support for the direct effect of regulations on PHI privacy concerns (Ermakova et al., 2014) and on trust in HIT (Dinev et al., 2016). In the context of location-based services, Xu et al. (2012) similarly found a direct influence of government regulation on privacy concerns. However, further analysis by the authors revealed that the direct relationship between government regulation and privacy concerns becomes insignificant in the presence of perceived control which was found to exert a pronounced negative effect on privacy concerns. This suggests possible mediation of the influence of government regulation on privacy concerns by other variables. In support of this suggestion, this study found that trust

in healthcare providers fully mediates the influence of perceived effectiveness of government regulation on PHI management concerns and partially mediates its influence on trust in HIT. This study extends the existing literature by demonstrating that trust in the organization deploying technology to collect and use personal information (in this case healthcare providers) represents a mechanism explaining the role of government regulation in relation to privacy concerns and trust in a technological artefact.

Third, several researchers have acknowledged that privacy concerns may differ between individuals with computer or Internet experience and those without such experience (Anderson & Agarwal, 2011; Angst & Agarwal, 2009; Kenny, 2016; Li & Slee, 2014). However, the majority of studies, especially in the healthcare context, have failed to account for the influence of computer or Internet experience in examining privacy concerns and PHI disclosure. This is probably due to the fact that the existing studies have largely been conducted in developed countries where individuals with no computer or Internet experience may be considered a shrinking group (Kenny, 2016). Given the digital divide in developing countries (ITU, 2016, 2017; PRC, 2015), it was speculated that individuals' trust and privacy perceptions as well as information disclosure behaviours in online environments may differ based on computer experience (Sections 2.3.2 & 2.3.4). Consequently, computer experience was used as a control variable in the empirical models examined in this study. In support, computer experience was found to influence PHI management concerns, trust in HIT, and willingness to disclose PHI. This suggests that, in developing countries where there is still a digital divide, computer experience is a key factor to consider in empirical models examining trust perceptions regarding technologies or electronic servicers, privacy perceptions and personal information disclosure behaviours in online environments.

Finally, the IS privacy research in general, and studies specifically related to the healthcare context have largely focused on developed countries (Hong & Thong, 2013; Kenny, 2016). The majority of the studies have also relied on student and tech-savvy samples (e.g., Bansal et al., 2010) limiting the generalizability of the findings (Bélanger & Crossler, 2011). This study, in contrast, extends the literature by examining the factors influencing PHI privacy concerns, trust in HIT, and PHI disclosure among an understudied population - individuals in a developing country. Also, the sample for the study was diverse in terms of age, level of education, and computer experience. A diverse sample is required for understanding the various antecedents to PHI privacy concerns, trust in HIT, and PHI disclosure. The study, therefore, answers calls to extend the boundaries of IS privacy research by utilizing diverse samples and examining the developing country context (Bélanger & Crossler, 2011). In answering this call, the study makes a methodological contribution. The study adapted past research instruments developed and used in western contexts to examine privacy and trust perceptions and PHI disclosure intentions in a developing country. It thus contributes to the external validity of the past research instruments. It has also introduced instruments from the healthcare and the psychology literature which can be used by IS researchers and practitioners. Examples include instruments for perceived inferiority (Goss et al., 1994) and perceived attitude of health workers (Sumaedi et al., 2016).

7.2 Implications for Practice

This study explored the factors that both drive and inhibit PHI disclosure among individuals in developing countries in a digitized healthcare environment. The findings of the study provide insights that are of relevance for practice. First, practical contributions regarding the inhibitors of PHI disclosure considered in the study are discussed. This will be followed by the practical contributions related to the drivers of PHI disclosure.

7.2.1 Inhibitors of PHI Disclosure

The key inhibitors of PHI disclosure examined in this study were PHI privacy concerns, privacy risk and perceived negative consequences of PHI disclosure. PHI privacy concerns was explored as a multi-dimensional construct comprising of four dimensions (Smith et al., 1996): collection, errors, secondary use and unauthorised access. Concerns about the collection dimension were found to be lower compared to concerns regarding the other three dimensions. Consequently, two aspects of PHI privacy concerns were further explored: PHI collection concerns (i.e. concerns about collection of PHI) and PHI management concerns (i.e., concerns regarding errors, secondary use, and unauthorised access).

To briefly recap the core findings regarding the inhibitors, willingness to disclose PHI was found to be negatively influenced by PHI collection concerns and positively impacted by PHI management concerns. On the other hand, privacy risk had no direct influence on willingness to disclose PHI but had an indirect influence via PHI collection concerns. In addition to PHI privacy concerns and privacy risk, this study also explored the influence of the negative consequences that individuals perceive may result from PHI privacy loss on their PHI disclosure intentions. Individuals' perceptions that others will evaluate them negatively (i.e., perceived inferiority) should their PHI be exposed (in this case PHI indicating one has HIV/AIDS), decrease their willingness to disclose PHI. The study also showed a number of factors related to individual characteristics, experiences, and perceptions influence the two aspects of PHI privacy concerns. The practical implications of these findings are discussed next.

The results of the study show that individuals have greater concerns about the management of their PHI after it has been collected and stored electronically (i.e., concerns regarding errors, secondary use, and unauthorised access). Despite these concerns, however, individuals are still willing to disclose their PHI. This unexpected finding notwithstanding, it is important to address individuals' PHI management concerns given that it is strongly influenced by individuals' desire to limit and guard access to their personal information, which in turn is an indication that individuals, in general, have a strong desire for privacy. This has implications for the stakeholders involved in developing e-health systems in developing countries (e.g., developers, healthcare providers, policy makers, etc.). A review of e-health projects in these countries found that there is often a lack of consideration of PHI privacy in the development of e-health systems as the relevant stakeholders assume that individuals may not care much about privacy of their PHI (PEN, 2010). The results of this study contradict this assumption

and suggest that individuals do care about their privacy and that healthcare stakeholders need to pay attention to protecting PHI privacy when developing e-health systems. In particular, data integrity standards should be implemented to protect against and correct errors in the collected data and ensure that accurate and consistent patient data are maintained. Also, adequate technical measures should be put in place to prevent unauthorised access and/or use of patient data. For instance, audit trails can be implemented to track, inhibit and address any access to electronically stored PHI.

Though, individuals trust healthcare providers (in terms of benevolence, competence and integrity) in providing needed care services, their trust in the providers is associated also with increased rather than decreased privacy concerns centered on the management of their PHI. Healthcare providers can address these concerns by educating individuals about the technical measures put in place to protect the privacy of patient data (e.g., audit trails, encryption, etc.). They should also inform individuals of any secondary uses of their data and seek consent prior to such uses. Such transparency efforts coupled with the awareness of PHI privacy-protective measures may go a long way to build individuals' trust in the benevolence, integrity and competency of healthcare providers in managing electronically stored PHI. This can decrease concerns regarding PHI management.

Though not as high compared to PHI management concerns, individuals also have concerns about the collection of their PHI which significantly decrease their willingness to disclose PHI. Collection is considered to be one of the important dimensions of information privacy (Hann et al., 2007; Westin, 1967). It is especially important in the healthcare context as without the availability of complete and accurate information about patients, wrong diagnoses or prescriptions can occur which can lead to fatal outcomes. It is thus important to address any concerns regarding PHI collection. The results of the study show that PHI collection concerns is strongly impacted by individuals' perceptions about the risks of storing their PHI electronically and past experience of privacy breaches. In recent years, there has been an increase in cybercrimes and abuse of digitized information/systems (e.g., sextortion, leakage of medical records, etc.) in Africa (Debrah, 2019; Serianu, 2016; Technomag, 2018). The media attention (e.g., Darko, 2015; Kyei-Boateng, 2018) regarding these incidences is likely to increase individuals' risk perceptions regarding digitized information. Following earlier suggestions, healthcare providers can help to mitigate individuals' concerns by educating them regarding implemented PHI privacy-protective measures; their transparency in the handling of PHI may also assure individuals, especially victims of privacy violations, that their PHI, when collected, will be protected and stored safely. Males, younger individuals and those who are more concerned about their health, in particular, have higher concerns about PHI collection. Providers can further explore the concerns of these groups and tailor educational and privacy assurance programs to address their concerns.

The results of the study further suggest that for individuals with stigmatized diseases such as HIV/AIDS, fear of negative consequences, such as negative evaluation by others, should their disclosed PHI be exposed may lead to less willingness to disclose their PHI in seeking needed care. Healthcare providers can enhance the privacy protection of highly sensitive PHI by using

measures such as encryption or coding (e.g., using numeric code to represent health conditions) and educating people about these measures. This may encourage individuals to disclose and allow electronic storage of their sensitive PHI being assured that their PHI will be protected against any public exposure. The results also signal a bigger need (that goes beyond the scope of this study) to intensify public education and awareness to address erroneous perceptions associated with certain diseases which lead to the stigmatization of individuals affected by those diseases. This will help bolster the confidence of these individuals in disclosing their infection to seek needed care.

7.2.2 Drivers of PHI Disclosure

Convenience and trust are the drivers of PHI disclosure considered in this study. Two aspects of trust were explored: trust in healthcare providers and trust in HIT. Convenience and trust in HIT directly influence individuals' willingness to disclose PHI whereas trust in healthcare has an indirect effect on willingness to disclose PHI through its impact on trust in HIT. Trust in HIT is strongly influenced by trust in healthcare providers and privacy risk. On the other hand, perceived attitude of health workers and perceived effectiveness of government regulation strongly shape trust in healthcare providers. The practical implications of findings related to the drivers of PHI disclosure and their antecedent factors are discussed next.

Convenience plays an important role in influencing individuals' PHI disclosure. This indicates that if individuals perceive they will spend less time and effort in receiving care in a digitized healthcare environment, they are more likely to disclose their PHI for digitization. Therefore, to encourage PHI disclosure, healthcare providers can introduce HITs that provide observable benefits to individuals such as convenience. For instance, an EHR system that enables the cumulative storage of patient data and ensures its authorised access in the various units/ departments that patients visit during a healthcare service encounter can help patients receive safe treatments that are timely and less effortful. These benefits may influence individuals' perception of convenience and encourage their acceptance of the system.

The study shows that even if individuals view healthcare providers as trustworthy (i.e., the providers have the favourable attributes of benevolence, competence, and integrity), this does not directly influence their PHI disclosure. However, if individuals view healthcare providers as trustworthy, they are likely to trust the HIT introduced by the providers as well, which in turn, encourages their PHI disclosure. This suggests that healthcare providers should pay attention to the trust individuals place in them and, those providing HITs should pay even more attention to building trust in the HITs they deploy as trust in HIT directly influences PHI disclosure.

The study provides some insights regarding ways to build trust in healthcare providers. A major way in which healthcare providers can build individuals' trust in them is to ensure that individuals receive quality interpersonal treatment during the healthcare service encounter. Specifically, healthcare providers must ensure that health workers treat patients with kindness,

courtesy/respect, and care, and show a genuine desire to help the patients. This is especially important in Africa where studies have reported on the abuse of patient rights including mistreatments of various kinds (e.g., verbal abuse, abandonment, slapping, etc.) (Maya et al., 2018) and breach of confidentiality of sensitive PHI such as HIV status (Dapaah & Senah, 2016). The results also show that individuals' perceptions that government regulations are effective in providing protection against PHI privacy violations increase trust in healthcare providers. This suggests individuals' belief that if privacy regulations are there healthcare providers will comply with them. Governments, therefore, can contribute to building trust in healthcare providers by enacting regulations that govern the collection, use, sharing and protection of PHI. The regulations must also provide individuals with the opportunities to seek redress if there are violations in the handling of their PHI.

As indicated earlier, in as much as it is important for healthcare providers to build individuals' trust in them, they must also pay greater attention to building individuals' trust in the HITs they use as trust in HIT directly facilitates PHI disclosure. HIT providers can build trust in HITs by incorporating functionalities into the technologies which can signal to individuals that their PHI stored using these technologies will be protected and kept safe. For example, a patient portal can be added to an EHR system and through this portal individuals can control the use of their PHI by controlling the access levels of various stakeholders involved in their care. This, in addition to other technical measures that HIT providers put in place to protect PHI privacy, can alleviate individuals' risk perceptions regarding electronic storage of PHI which was found in this study to strongly decrease trust in HIT. Since individuals' perceptions of the effectiveness of government regulation increase trust in HIT, governments can also contribute to building trust in HITs by enacting regulations that ensure that HITs deployed by healthcare providers meet certain standards regarding privacy protection of digitized PHI. Such regulations must address issues related to access, security, and exchange of digitized PHI (IICD, 2014).

In conclusion, the success of IT innovations, in general, depends largely on individuals' acceptance of the innovation regardless of its beneficial features (Carter & Bélanger, 2005). This is especially true in the healthcare context where individuals' willingness to disclose and allow digitization of their PHI is critical to the successful leveraging of IT innovations in the provision of healthcare services (Angst & Agarwal, 2009). Due to the sensitive nature of PHI with its concomitant concerns about privacy, individuals may reject HITs (Dinev et al., 2016). Thus, healthcare stakeholders need to understand the important factors influencing individuals' PHI disclosure behaviours. This study contributes to addressing this gap by providing actionable insights and suggestions regarding the drivers and inhibitors of PHI disclosure, the specific concerns of individuals regarding PHI privacy and the determinants of these concerns, as well as the factors influencing individuals' trust in an HIT. Healthcare stakeholders, especially in developing countries, can leverage these insights to address individuals' PHI privacy concerns, build their trust in HITs, and ultimately encourage their PHI disclosure for digitization.

7.3 Limitations and Future Research

This study makes several contributions to research and practice. Nonetheless, there are some limitations which in turn may guide future research, as well as other opportunities for future research that arise directly from the contributions of this study.

First, this study extended the boundaries of IS privacy research by examining the developing country context, with the sample drawn from one country, Ghana, a Sub-Saharan African nation. As Bélanger and Crossler (2011) have noted, differences in values, cultures, and laws across countries may lead to differences in individuals' privacy perceptions and their impacts. Findings from studies that use multi-country samples lend support to the authors' claim. Kenny and Connolly (2016) found differences in the significant predictors (e.g., gender, privacy media coverage, trust and risk beliefs) of PHI privacy concerns between Irish and U.S. samples. Dinev, Bellotto, Hart, and Russo (2006) also found that Italians expressed lower Internet privacy concerns than individuals in the U.S. However, it is thus likely that the findings of this study may not generalize to developing countries that differ significantly from Ghana in terms of factors such as cultural beliefs regarding privacy, privacy regulations/policies, and educational development. Future research investigating whether the findings of this study extend to other developing countries is encouraged.

A second limitation relates to the study sample. On the one hand, this study used a diverse sample compared to most prior studies (e.g., Bansal et al., 2010; Miltgen et al., 2013). However, despite a concerted effort to recruit individuals with varying backgrounds, there was underrepresentation in some of the demographic groups. Examples include individuals with little or no computer experience and education, and those with varying health conditions. A number of demographics such as marital status and family size were also not considered in this study. Chen, Zhang, and Heath (2001) have suggested that economic well-being may affect privacy concerns. According to the authors, if the primary preoccupation of an individual is basic necessities such as food and shelter, concerns about privacy may be secondary. A recent World Bank report (2016b) indicates that the number of poor people in Africa has increased substantially since 1990. Thus, future studies should also investigate associations between income levels of individuals and other measures of socioeconomic well-being (e.g., employment status), and privacy concerns. In general, a larger sample reflecting more closely the demographic distribution of the population in a developing country should be considered in future studies.

The third limitation relates to the research model of the study. This study presented a detailed model which represents an important starting point for exploring factors influencing PHI privacy concerns, trust in HIT, and PHI disclosure among individuals in developing countries. However, the research model does not include all factors that may affect individuals' PHI privacy concerns, trust in HIT, and PHI disclosure behaviours. As suggested in the preceding paragraph, other socioeconomic factors (e.g., income, employment status) should be identified and their relationships with PHI privacy concerns assessed. Prior research also shows that factors such as healthcare need and perceived health information sensitivity (Kenny &

Connolly, 2016) influence PHI privacy concerns. Future studies should explore the impact of these factors on PHI privacy concerns. Similar to Anderson and Agarwal (2011), the cognitive factors in the privacy calculus could be extended to include emotion related to one's health. In summary, future research can retest the model proposed in this study in other contexts, as well as explore other factors to improve our current understanding of their influences on PHI privacy concerns, trust in HIT, and PHI disclosure.

Fourth, this study measured intentions as opposed to actual behaviour. The main objective of this study was to understand individuals' PHI disclosure intentions. This was appropriate for while HIT has been deployed in Ghana's public hospitals, it is an emerging technology with some paper-based systems still in place; as such, not all visits to a hospital may involve direct interaction with HIT. The findings of this study thus should be viewed within the context of 'intention'. According to Lafky and Horan (2011), in exploring users' perceptions of IT innovations that have yet to be adopted, "a prospective, not a retrospective viewpoint is required". Therefore, similar to several studies in the healthcare context (e.g., Anderson & Agarwal, 2011; Angst & Agarwal, 2009; Kenny, 2016), given the nascence of e-health in developing countries (Lewis et al., 2012), behavioural intention as a dependent variable was appropriate for this study. This is also appropriate as the study was intended as an initial step toward understanding individuals' privacy concerns and trust beliefs as well as their PHI disclosure intentions in an emerging digitized healthcare setting. Besides, behavioural intention has been found to strongly predict actual behaviour (Webb & Sheeran, 2006) and is often used as a proxy for actual behaviour in IS privacy studies (Anderson & Agarwal, 2011; Malhotra et al., 2004). At the same time, some studies have shown that individuals' stated intentions may not translate into actual behaviour (Kenny, 2016). Future studies are therefore encouraged to re-examine intentions (as HIT matures) and assess actual PHI disclosure behaviour.

Finally, the study explored the influence of negative consequences that individuals perceive may result from the exposure of the PHI they disclose to receive care, on their PHI disclosure intentions. Examples of negative consequences associated with HIV/AIDS were investigated. However, it is not known whether the respondents themselves had this disease or had experience of the consequences that were explored. In Ghana (i.e., the geographic context of study), HIV/AIDS is heavily stigmatised and as a result, most infected individuals hide their infection (Kwansa, 2013). Consequently, it would have been difficult to recruit individuals who were living with HIV/AIDS. Perceptions of negative consequences associated with a particular health condition and their impact on information disclosure about the condition may differ between individuals who have the health condition and those not infected with this condition. Future studies should, therefore, include individuals living with sensitive conditions such as HIV/AIDS to further explore the influence of negative consequences of PHI disclosure on individuals PHI disclosure behaviours. As a further step, the results can also be compared with responses from persons with less sensitive conditions, other conditions or no conditions at all.

Aside from the opportunities for further research that the study limitations present (e.g., including larger sample, extending and retesting the proposed model in other countries, etc.), some of the study's findings raise interesting questions which future studies may explore. First,

this study found that individuals' concerns about the collection of their PHI are considerably lower than their concerns regarding the management of their PHI after it has been collected by healthcare providers and stored electronically (i.e., concerns regarding errors, secondary use, and unauthorised access). Yet, despite their greater concerns about PHI management, individuals are willing to disclose their PHI. As discussed in Section 6.2.3, the observed paradoxical relationship between PHI management concerns and willingness to disclose PHI may be further due to individuals' perceived lack of control over their PHI after it has been collected and stored electronically, coupled with their need for care which necessitates their PHI disclosure. The IS privacy research shows the lack of control over personal information as the main source of privacy concerns (Bélanger & Crossler, 2011; Stewart & Segars, 2002). Individuals may have little or no control over their PHI after it has been collected and is in the custody of healthcare providers, and this likely increases concerns about PHI management. However, health is of utmost importance to individuals (Anderson & Agarwal, 2011) and, therefore, to receive needed care to improve one's health, individuals may disclose PHI even if they are concerned about how the disclosed PHI will be managed. These speculations need to be explored in future research. Studies employing qualitative techniques such as interviews and using samples with different health conditions (e.g., individuals in good health versus those facing life-threatening diseases) may especially be helpful in providing deeper insights into the relationship between privacy concerns and personal information disclosure in the healthcare context.

This study explored the relationships between individual characteristics, experience and perceptions, and PHI privacy concerns. In contrast to existing studies (e.g., Ancker et al., 2013; Wilkowska & Ziefle, 2012), this study found that males and younger individuals are more concerned about the collection of their PHI than females and older individuals. Future studies employing qualitative methods such as interviews should explore what may account for these differences, that is, males and younger individuals' having higher concerns regarding the collection of their PHI.

A positive relationship between individuals' trust in healthcare providers and their concerns regarding PHI management was also observed in this study. In a related study, Kenny and Connolly (2016) also found that individuals' trust in healthcare professionals' does not decrease but rather increases health information privacy concerns. As healthcare providers are the primary custodians of PHI, individuals' trust in the providers' ability to properly manage and protect electronically stored PHI may encourage their PHI disclosure. It is thus important that future research further explores the relationship between trust in healthcare providers and PHI privacy concerns.

In general, the findings of the study suggest the need for further examination of the antecedents and consequences of PHI privacy concerns to improve our understanding of privacy concerns in the healthcare context. For example, control and awareness are seen as other important dimensions of privacy concerns, especially when examining Internet-based privacy concerns (Malhotra et al., 2004). Thus, for a more comprehensive assessment of PHI privacy concerns, future studies are encouraged to adapt the Internet Privacy Concerns (IPC) instrument (Hong

& Thong, 2013), which combines control and awareness with the four dimensions of concerns examined in this study, to the healthcare context.

The proposed research model in this study draws also largely on the existing IS privacy research, which has been mostly focused on developed countries. However, a few constructs that were included in the model to contextualize it to the developing country context are also relevant to and have yet to be explored in the context of developed countries (e.g., perceived negative consequences of PHI disclosure and perceived attitude of health workers). As indicated above, some of the study findings contradict findings in prior research. This may be due to differences in culture and privacy regulations between developed and developing countries, which according to Bélanger and Crossler (2011) may lead to differences in individuals' privacy perceptions and information disclosure. The digital divide and gender digital gap in developing countries (ITU, 2016, 2017) might have also accounted for some of the divergent findings of the study compared to prior research conducted in developed countries. Overall, the contrasting findings of the study compared to prior research suggest that while the proposed model may be applicable also to explaining PHI disclosure behaviour in developed countries, there may be differences in terms of the impact of some of the constructs in the model between developed and developing countries. To explore this further, future research using samples from both developed and developing countries is needed to test the research model and explain any differences in findings that may occur between the samples. Such research efforts may employ a mixed-method design by first quantitatively testing the research model, then further exploring the model results using qualitative techniques such as interviews.

7.4 Conclusion

As developing countries leverage HITs in support of health services, it is important to identify and understand from the individuals' perspective the factors that may pose a challenge to the successful digitization of healthcare in these countries. Toward this end, using the privacy calculus as the overarching theory and supported by justice theory and prior IS privacy research, this study developed a model which explains the factors influencing PHI privacy concerns, trust in HIT, and PHI disclosure among individuals in developing countries. The model was quantitatively tested using cross-sectional survey data.

The results of the study show convenience and trust in HIT as the main drivers of individuals' willingness to disclose PHI. Individuals with greater computer experience also express greater willingness to disclose PHI. However, trust in healthcare providers was found not to directly influence willingness to disclose PHI; rather, its impact is mediated by trust in HIT such that trust in healthcare providers increases trust in the HIT which in turn facilitates PHI disclosure. This suggests that to encourage PHI disclosure, healthcare stakeholders must pay attention to building trust in HITs. The study provides further insights in this regard by showing that government regulation, privacy risk, computer experience, and health concern shape trust in

HIT. Perceived attitude of health workers also builds trust in HIT by increasing trust in healthcare providers.

PHI privacy concerns, privacy risk and negative consequences associated with PHI disclosure were examined as the cost calculus factors which inhibit PHI disclosure. To assess the impact of negative consequences on PHI disclosure, a hypothetical situation concerning HIV/AIDS infection was presented. Individuals' perceptions that others would evaluate them negatively (i.e., perceived inferiority) should PHI indicating that they have HIV/AIDS be exposed is found to decrease their willingness to disclose PHI. However, other potential consequences such as employment discrimination or rejection by family do not impact PHI disclosure intentions.

The study revealed that individuals differentiate between concerns about the collection of PHI and concerns about the management of the collected and electronically stored PHI. Individuals have lower PHI collection concerns but are greatly concerned about PHI management. Further confirming that individuals differentiate between PHI collection and management concerns, the two dimensions had differential impacts on PHI disclosure, with PHI collection concerns having a strong negative impact on willingness to disclose PHI. However, contrary to expectations, PHI management concerns is associated with an increased willingness to disclose PHI.

Moreover, the two dimensions of PHI privacy concerns are also impacted differently by antecedent factors. Individuals with greater computer experience and those with a higher desire for privacy express greater PHI management concerns. Surprisingly, trust in healthcare providers is associated with increased concerns about PHI management. Further, trust in healthcare providers fully mediates the influence of government regulation and perceived attitude of health workers on PHI management concerns. On the other hand, PHI collection concerns are shaped by perceptions of risk, and individual characteristics such as age, gender, and health concern. Privacy experience is positively associated with PHI collection concerns but decreases PHI management concerns.

Overall, the findings of the study provide insights into the drivers and inhibitors of PHI disclosure, the dimensions of PHI privacy concerns and their antecedents, as well as the antecedents to trust in HIT. Taken together these findings extend the current understanding regarding privacy concerns, trust and personal information disclosure in the healthcare context, providing useful contributions to the IS privacy literature. The study findings also provide actionable insights which can assist healthcare stakeholders to address individuals' PHI privacy concerns, build their trust in HITs, and facilitate disclosure of their PHI. A number of opportunities for future research are presented. For example, future studies can explore seeming contradictions such as why is it that despite individuals expressing greater concerns about PHI management, they are willing to disclose their PHI? The positive relationship observed between trust in healthcare providers and PHI management concerns also needs further investigation.

REFERENCES

Achampong, E. (2012). Electronic health record system: a survey in Ghanaian hospitals. *Open Access Scientific Reports, 1*(02).

Acquah-Swanzy, M. (2015). *Evaluating Electronic Health Record Systems in Ghana: the case of Effia Nkwanta Regional Hospital* (Master's thesis). The Artic University of Norway, Norway.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *In Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21-29). New York, NY: ACM Press.

Acquisti, A. (2009). Nudging privacy: The behavioural economics of personal information. *IEEE security & privacy, 7*(6), 82-85.

Acquisti, A. (2010). From the Economics to the Behavioral Economics of Privacy: A note. In A. Kumar & D. Zhang (Eds.), *International Conference on Ethics and Policy of Biometrics* (Vol. 6005, pp. 23-26). Berlin, Heidelberg: Springer.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *Science, 347*(6221), 509-514.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*(2), 249-274.

Afarikumah, E. (2014). Electronic health in Ghana: current status and future prospects. *Online journal of public health informatics, 5*(3), 230.

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2013). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association, 21*(2), 374-378.

Agarwal, R., Gao, G., DesRoches, C., & Jha, A. K. (2010). Research commentary—The digital transformation of healthcare: Current status and the road ahead. *Information systems research, 21*(4), 796-809.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly*, 665-694.

Aiken, K. D., & Boush, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science, 34*(3), 308-323.

Ajzen, I. (1988). *Attitudes, personality, and behaviour*. Chicago, IL: Dorsey Press.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behaviour, 8*(1), 7-29.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of social issues, 33*(3), 66-84.

Anafi, P., Mprah, W. K., & Asiamah, E. (2014). HIV/AIDS stigma and persons living with HIV/AIDS in rural Ghana. *International quarterly of community health education, 34*(3), 269-282.

Ancker, J. S., Silver, M., Miller, M. C., & Kaushal, R. (2013). Consumer experience with and attitudes toward health information technology: a nationwide survey. *Journal of the American Medical Informatics Association, 20*(1), 152-156.

Andersen, H. M. (2004). "Villagers": differential treatment in a Ghanaian hospital. *Social science & medicine, 59*(10), 2003-2012.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information systems research, 22*(3), 469-490.

Anderson, J. G. (2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues. *International journal of medical informatics, 60*(2), 111-118.

Angst, C. M., & Agarwal, R. (2006) Getting Personal About Electronic Health Records: Modeling the Beliefs of Personal Health Record Users and Non-Users. In. *Robert H. Smith School Research Paper No RHS-06-007*: Available at SSRN: http://ssrn.com/abstract=902904.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly, 33*(2), 339-370.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management, 6*(4), 279-314.

Ariely, D. (2009). The end of rational economics. *Harvard business review, 87*(7-8), 78-84.

Aryee, S., Budhwar, P. S., & Chen, Z. X. (2002). Trust as a mediator of the relationship between organizational justice and work outcomes: Test of a social exchange model. *Journal of Organizational Behaviour*, *23*(3), 267-285.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107-123.

Austin, L. (2003). Privacy and the Question of Technology. *Law and Philosophy, 22*(2), 119-166.

Badu, E., Opoku, M. P., & Appiah, S. C. (2016). Attitudes of health service providers: The perspective of people with disabilities in the Kumasi Metropolis of Ghana. *African journal of disability*, *5*(1), a181. http://dx.doi.org/10.4102/ajod.v5i1.181

Baltussen, R., & Ye, Y. (2005). Quality of care of modern health services as perceived by users and non-users in Burkina Faso. *International journal for quality in health care, 18*(1), 30-34.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American psychologist, 37*(2), 122-147.

Bansal, G., Fatemeh, Z., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems, 49*(2), 138-150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Barclay, D., Higgins, C., & Thompson, R. (1995). The Partial Least Squares (pls) Approach to Causal Modeling: Personal Computer Adoption Ans Use as an Illustration. *Technology studies*, *2*(2), 285-309.

Bates, A. P. (1964). Privacy—a useful concept? *Social forces, 42*(4), 429-434.

Beckerman, J. Z., Pritts, J., Goplerud, E., Leifer, J., Borzi, P., Rosenbaum, S., & Anderson, D. (2008). A delicate balance: Behavioural health, patient privacy, and the need to know. *California Healthcare Foundation: Issue Brief*, 1-12.

Bedeley, R., & Palvia, P. (2014). A study of the issues of E-health care in developing countries: The case of Ghana. *In Proceedings of the Twentieth Americas Conference on Information Systems*. Savannah, GA.

Belanche, D., Casaló, L. V., Flavián, C., & Schepers, J. (2014). Trust transfer in the continued usage of public e-services. *Information & Management, 51*(6), 627-640.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*(4), 1017-1042.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245-270.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in human behaviour*, *26*(5), 857-869.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313-324.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: the practice of relevance. *MIS quarterly*, 3-16.

Berry, L. L., Seiders, K., & Grewal, D. (2002). Understanding service convenience. *Journal of marketing*, *66*(3), 1-17.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211-241.

Bies, R., & Moag, R. (1986). Interactional justice: Communication criteria of fairness In R. Lewicki, B. Sheppard, & M. Bazerman (Eds.), *Research on negotiations in organizations* (pp. 43-55). Greenwich, CT: JAI Press.

Bies, R. J. (2001). Interactional (in)justice: The sacred and the profane. In J. Greenberg & R. Cropanzano (Eds.), *Advances in organizational justice* (pp. 89-118). Stanford, CA: Stanford University Press.

Blumenthal, D., & Glaser, J. P. (2007). Information Technology Comes to Medicine. *The New England Journal of Medicine, 356*(24), 2527-2534.

Brady, M. K., & Cronin, J. J. (2001). Some new thoughts on conceptualizing perceived service quality: a hierarchical approach. *Journal of marketing*, *65*(3), 34-49.

Caine, K., & Hanania, R. (2012). Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association, 20*(1), 7-15.

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

Campos-Castillo, C., & Anthony, D. L. (2014). The double-edged sword of electronic health records: implications for patient disclosure. *Journal of the American Medical Informatics Association, 22*(e1), e130-e140.

Caro, L. M., & García, J. A. M. (2008). Developing a multidimensional and hierarchical service quality model for the travel agency industry. *Tourism Management, 29*(4), 706-720.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, *6*(2-3), 181-202.

Chen, J., Zhang, Y., & Heath, R. (2001). An Exploratory Investigation of the Relationships between Consumer Characteristics and Information Privacy. *Marketing Management Journal*, *11*(1).

Chen, K., & Rea, A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems*, *44*(4), 85-92.

Chhanabhai, P., & Holt, A. (2007). Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine*, *9*(1), 8.

Chiasson, M. W., & Davidson, E. (2004). Pushing the contextual envelope: developing and diffusing IS theory for health information systems research. *Information and Organization*, *14*(3), 155-188.
Chiasson, M. W., & Davidson, E. (2005). Taking industry seriously in information systems research. *Mis Quarterly*, *29*(4), 591-605.
Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (Vol. 295, pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.
Chiu, C.-M., Lin, H.-Y., Sun, S.-Y., & Hsu, M.-H. (2009). Understanding customers' loyalty intentions towards online shopping: an integration of technology acceptance model and fairness theory. *Behaviour & Information Technology*, *28*(4), 347-360.
Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60-67.
Clemmer, E. C., & Schneider, B. (1996). Fair service. In T. A. Swartz, D. E. Bowen, & S. W. Brown (Eds.), *Advances in services marketing and management* (pp. 109-126). Greenwich, CT: JAI Press.
Cohen, J. E. (2001). Privacy, ideology, and technology: A response to Jeffrey Rosen. *Geo. LJ*, *89*, 2029.
Colquitt, J. A. (2001). On the dimensionality of organizational justice: A construct validation of a measure. *Journal of applied Psychology*, *86*(3), 386-400.
Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information systems journal*, *23*(5), 401-417.
Consumer Reports. (2008). *Poll: Consumers Concerned About Internet Privacy*. Retrieved from https://advocacy.consumerreports.org/press_release/poll-consumers-concerned-about-internet-privacy/
Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce research and applications*, *2*(3), 203-215.
Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.
Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*: Sage publications.
Cropanzano, R., & Greenberg, J. (1997). Progress in organizational justice: Tunneling through the maze. *International review of industrial and organizational psychology*, *12*, 317-372.
Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*(2), 10-19.
Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.
Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, *59*(2), 323-342.
Dapaah, J. M. (2012). *HIV/AIDS treatment in two Ghanaian hospitals: experiences of patients, nurses and doctors*. Leiden, The Netherlands: African Studies Centre.
Dapaah, J. M., & Senah, K. A. (2016). HIV/AIDS clients, privacy and confidentiality; the case of two health centres in the Ashanti Region of Ghana. *BMC medical ethics*, *17*(1), 41.
Darko, S. (2015). *Inside the world of Ghana's internet fraudsters.* Retrieved from https://www.bbc.com/news/world-africa-32583161
Data Protection Act, 2012. Retrieved from https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf

Davies, S. G. (1997). Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In P. E. Agre & M. Rotenber (Eds.), Technology and Privacy: The New Landscape (pp. 143-165). Cambridge, MA: MIT Press.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Debrah, K. (2019). *'Sextortion': 10 cases recorded in less than a month*. Retrieved from https://www.myjoyonline.com/news/2019/January-21st/sextortion-10-cases-recorded-in-less-than-a-month.php

DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2018 ed.). Retrieved from https://plato.stanford.edu/archives/spr2018/entries/privacy/

Dickerson, S. S. (2003). Gender differences in stories of everyday Internet use. *Health Care for Women International, 24*(5), 434-451.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective. In A. Gupta, V. L. Patel, & R. A. Greenes (Eds.), *Advances in Healthcare Informatics and Analytics, Annals of Information Systems* (pp. 19-50). Switzerland: Springer Publishing.

Dinev, T., Bellotto, M., Hart, P., & Russo, V. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management, 14*(4), 57.

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

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research, 17*(1), 61-80.

Dinev, T., Hu, Q., & Yayla, A. (2008). Is there an on-line advertisers' dilemma? A study of click fraud in the pay-per-click model. *International Journal of Electronic Commerce, 13*(2), 29-60.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioural Economics: Thinking Outside the "APCO" Box. *Information systems research, 26*(4), 639-655.

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

Doty, D. H., & Glick, W. H. (1998). Common methods bias: does common methods variance really bias results? *Organizational research methods, 1*(4), 374-406.

Dowling, G. R. (1986). Perceived risk: the concept and its measurement. *Psychology & Marketing, 3*(3), 193-210.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research, 21*(1), 119-134.

Duffy, L. (2005). Suffering, shame, and silence: The stigma of HIV/AIDS. *Journal of the Association of Nurses in AIDS Care, 16*(1), 13-20.

Dutta-Bergman, M. (2003). Trusted online sources of health information: differences in demographics, health beliefs, and health-information orientation. *Journal of medical Internet research, 5*(3), e21.

Edney, J. J., & Buda, M. A. (1976). Distinguishing territoriality and privacy: Two studies. *Human Ecology, 4*(4), 283-296.

Enkin, A. (2012). *Privacy*. Retrieved from https://www.torahmusings.com/2012/07/privacy/

Ermakova, T., Fabian, B., & Zarnekow, R. (2014). Acceptance of Health Clouds-a Privacy Calculus Perspective. *In Proceedings of the Twenty Second European Conference on Information Systems.* Tel Aviv, Israel.

Esmaeilzadeh, P. (2019). The effects of public concern for information privacy on the adoption of Health Information Exchanges (HIEs) by healthcare entities. *Health communication, 34*(10), 1202-1211.

Esmaeilzadeh, P. (2018b). Healthcare consumers' opt-in intentions to Health Information Exchanges (HIEs): An empirical study. *Computers in human behaviour, 84*, 114-129.

Fang, Y.-H., & Chiu, C.-M. (2010). In justice we trust: Exploring knowledge-sharing continuance intentions in virtual communities of practice. *Computers in human behaviour, 26*(2), 235-246.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies, 59*(4), 451-474.

Fichman, R. G., Kohli, R., & Krishnan, R. (2011). Editorial overview—the role of information systems in healthcare: current research and future trends. *Information systems research, 22*(3), 419-428.

Fischer, S. H., David, D., Crotty, B. H., Dierks, M., & Safran, C. (2014). Acceptance and use of health information technology by community-dwelling elders. *International journal of medical informatics, 83*(9), 624-635.

Flynn, H. A., Marcus, S. M., Kerber, K., & Alessi, N. (2003). Patients' concerns about and perceptions of electronic psychiatric records. *Psychiatric services, 54*(11), 1539-1541.

Folger, R., & Bies, R. J. (1989). Managerial responsibilities and procedural justice. *Employee responsibilities and rights journal, 2*(2), 79-90.

Folger, R., & Greenberg, J. (1985). Procedural justice: An interpretive analysis of personnel systems. *Research in personnel and human resources management, 3*(1), 141-183.

Folger, R., & Konovsky, M. A. (1989). Effects of procedural and distributive justice on reactions to pay raise decisions. *Academy of Management Journal, 32*(1), 115-130.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.

Frost, J., Vermeulen, I. E., & Beekers, N. (2014). Anonymity versus privacy: selective information sharing in online cancer communities. *Journal of medical Internet research, 16*(5), e126.

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems, 3*(2), 112-126.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 33*(3), 38-53.

Genberg, B. L., Kawichai, S., Chingono, A., Sendah, M., Chariyalertsak, S., Konda, K. A., & Celentano, D. D. (2008). Assessing HIV/AIDS stigma and discrimination in developing countries. *AIDS and Behaviour, 12*(5), 772-780.

Gettleman, J. (2011, January 27). Ugandan who spoke up for gays is beaten to death. *The New York Times*. Retrieved from https://www.nytimes.com/2011/01/28/world/africa/28uganda.html

GhanaDistricts. (2018). 38 New MMDAs. Retrieved from http://www.ghanadistricts.com/Home/LinkData/7025

Ghana Health Service. (2015). *About Us.* Retrieved from http://www.ghanahealthservice.org/ghs-category.php?cid=2

Ghana Statistical Services. (2012). *2010 Population & Housing Census – Summary Report of Final Results*. Accra, Ghana: Author

Ghana Statistical Service. (2016). *2010 Population Projection by Sex, 2010-2016*. Retrieved from http://www2.statsghana.gov.gh/docfiles/2010phc/Projected%20population%20by%20sex%202010%20-%202016.pdf

Glaser, J., Henley, D. E., Downing, G., & Brinner, K. M. (2008). Advancing personalized health care through health information technology: an update from the American Health Information Community's Personalized Health Care Workgroup. *Journal of the American Medical Informatics Association, 15*(4), 391-396.

Goldman, J. (1998). Protecting Privacy To Improve Health Care: As the deadline for passing health privacy legislation in Congress nears, consensus is needed on a framework that values both patients' privacy and public health goals. *Health Affairs, 17*(6), 47-60.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 149-166.

Goss, K., Gilbert, P., & Allan, S. (1994). An exploration of shame measures—I: The other as Shamer scale. *Personality and Individual differences, 17*(5), 713-717.

Gostin, L. O., & Nass, S. (2009). Reforming the HIPAA privacy rule: safeguarding privacy and promoting research. *Jama, 301*(13), 1373-1375.

Grabner-Kraeuter, S. (2002). The role of consumers' trust in online-shopping. *Journal of Business Ethics, 39*(1-2), 43-50.

Grossklags, J., & Acquisti, A. (2007). When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. *In Proceedings of the Sixth Workshop Econom. Inform. Security (WEIS '07)*. Pittsburgh, PA.

Gyamfi, A. (2016). *Use of electronic medical records in emergency care at Komfo Anokye Teaching Hospital in Kumasi Ghana* (Bachelor's thesis). Kwame Nkrumah University of Science and Technology, Ghana.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*. Essex, England: Pearson Education Limited.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Hajar, R. (2017). The physician's oath: Historical perspectives. *Heart Views, 18*(4), 154-159

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Harris, K. L. (2003). *Justice Theory in Online and Offline Complaint Satisfaction: An Empirical* Study (Doctoral dissertation). George Washington University, Washington, DC.

Hayat, M. A. (2007). Privacy and Islam: From the Quran to data protection in Pakistan. *Information & Communications Technology Law, 16*(2), 137-148.

Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. *The Information Society, 18*(2), 101-112.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135.

Hodge Jr, J. G., Gostin, L. O., & Jacobson, P. D. (1999). Legal issues concerning electronic health information: privacy, quality, and liability. *Jama, 282*(15), 1466-1471.

Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2013). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111-136.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS quarterly*, *37*(1), 275-298.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45.

Hughes, K. (2012). A behavioural understanding of privacy and its implications for privacy law. *The Modern Law Review, 75*(5), 806-836.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *MIS quarterly*, 19-33.

Hwang, H.-G., Han, H.-E., Kuo, K.-M., & Liu, C.-F. (2012). The differing privacy concerns regarding exchanging electronic medical records of internet users in Taiwan. *Journal of medical systems, 36*(6), 3783-3793.

Ibrahim, L. M., Hadjia, I. S., Nguku, P., Waziri, N. E., Akhimien, M. O., Patrobas, P., & Nsubuga, P. (2014). Health care workers' knowledge and attitude towards TB patients under Direct Observation of Treatment in Plateau state Nigeria, 2011. *The Pan African medical journal, 18*(Suppl 1), 8.

International Institute for Communication and Development. (2014). *Toward e-health 2.0 in Ghana: A Programme and Opportunities for Private and Public ICT Initiatives*. The Hague, The Netherlands: Author.

Im, S., Bayus, B. L., & Mason, C. H. (2003). An empirical study of innate consumer innovativeness, personal characteristics, and new-product adoption behaviour. *Journal of the Academy of Marketing Science, 31*(1), 61-73.

International Telecommunication Union. (2016). *ICT Facts and Figures 2016*. Geneva, Switzerland: Author.

International Telecommunication Union. (2017). *ICT Facts and Figures 2017*. Geneva, Switzerland: Author.

Janda, S., & Fair, L. L. (2004). Exploring consumer concerns related to the internet. *Journal of Internet commerce, 3*(1), 1-21.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information technology and management, 1*(1-2), 45-71.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of consumer research, 30*(2), 199-218.

Jena, R. (2015). *Sharing Personal Health Information: Personalization versus Privacy. In Proceedings of the Twenty-first Americas Conference on Information Systems*. Puerto Rico.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behaviour in synchronous online social interactions. *Information systems research, 24*(3), 579-595.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1-24.

Jourard, S. M. (1966). Some Psychological Aspects of Privacy. *Law and Contemporary Problems, 31*(2), 307-318.

Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association, 15*(6), 729-736.

Kahn, L. (2004). *Experiences of HIV/AIDS diagnosis, disclosure and stigma in an urban informal settlement in the Cape Peninsula: A qualitative* exploration (CSSR Working Paper No. 94): Centre for Social Science Research (CSSR), University of Cape Town.

Kam, L. E., & Chismar, W. G. (2005). Online self-disclosure: model for the use of internet-based technologies in collecting sensitive health information. *International journal of healthcare technology and management, 7*(3-4), 218-232.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS quarterly, 12*(04), 571-586.

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organizational influence. *European Journal of Information Systems, 26*(6), 688-715.

Kemper, E. A., Stringfield, S., & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioural research* (pp. 273-319). Thousand Oaks, CA: Sage.

Kenny, G. (2016). *'To protect my health, or to protect my health data?'Eexamining the influence of health information privacy concerns on citizens' health technology adoption* (Doctoral dissertation). Dublin City University, Ireland.

Kenny, G., & Connolly, R. (2015). Citizens' Health Information Privacy Concerns: A Multifaceted Approach. *In Proceedings of the Twenty-Third European Conference on Information Systems*. Münster, Germany.

Kenny, G., & Connolly, R. (2016). Drivers of Health Information Privacy Concern: A Comparison Study. *In Proceedings of the Twenty-second Americas Conference on Information Systems*. San Diego, CA.

Kernan, M. C., & Hanges, P. J. (2002). Survivor reactions to reorganization: Antecedents and consequences of procedural, interpersonal, and informational justice. *Journal of Applied Psychology, 87*(5), 916-928.

Kifle, M., Mbarika, V. W., & Datta, P. (2006). Telemedicine in sub-Saharan Africa: The case of teleophthalmology and eye care in Ethiopia. *Journal of the American Society for Information Science and Technology, 57*(10), 1383-1393.

Kim, H.-W., Chan, H. C., & Kankanhalli, A. (2012). What motivates people to purchase digital items on virtual community websites? The desire for online self-presentation. *Information systems research, 23*(4), 1232-1245.

Kim, Y. (2016). Trust in health information websites: A systematic literature review on the antecedents of trust. *Health informatics journal, 22*(2), 355-369.

King, T., Brankovic, L., & Gillard, P. (2012). Perspectives of Australian adults about protecting the privacy of their health information in statistical databases. *International journal of medical informatics, 81*(4), 279-289.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS quarterly, 23*(1), 67-94.

Klein, R. (2007). Internet-based patient-physician electronic communication applications: patient acceptance and trust. *E-Service Journal, 5*(2), 27-51.

Klein, R., & Rai, A. (2009). Interfirm strategic information flows in logistics supply chain relationships. *MIS quarterly, 33*(04), 735-762.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration (IJeC), 11*(4), 1-10.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546-580.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

Kordzadeh, N., & Warren, J. (2014). Personal Characteristics, Privacy Concern, and Membership in Virtual Health Communities: An Empirical Study. *In Proceedings of the Twentieth Americas Conference on Information Systems*. Savannah, GA.

Kordzadeh, N., & Warren, J. (2017). Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment. *Journal of the Association for Information Systems, 18*(1), 45-81.

Kordzadeh, N., Warren, J., & Seifi, A. (2016). Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management, 36*(5), 724-734.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioural intentions. *Journal of Computer Information Systems, 48*(4), 15-24.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology, 25*(2), 109-125.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127-135.

Kuan, H.-H., & Bock, G.-W. (2007). Trust transference in brick and click retailers: An investigation of the before-online-visit phase. *Information & Management, 44*(2), 175-187.

Kwansa, B. K. (2013). *Safety in the midst of stigma: experiencing HIV/AIDS in two Ghanaian communities*. Leiden: African Studies Centre.

Kyei-Boateng, J. (2018). *Of The Nudity Spree, What Storm Is Breaking In Our Digital World?* Retrieved from https://www.modernghana.com/news/836482/of-the-nudity-spree-what-storm-is-breaking-in-our-digital-w.html

Lafky, D. B., & Horan, T. A. (2011). Personal health records: Consumer attitudes toward privacy and security of their personal health information. *Health informatics journal, 17*(1), 63-71.

Laric, M. V., Pitta, D. A., & Katsanis, L. P. (2009). Consumer concerns for healthcare information privacy: a comparison of US and Canadian perspectives. *Research in Healthcare Financial Management, 12*(1), 93-111.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social issues, 33*(3), 22-42.

Lewis, T., Synowiec, C., Lagomarsino, G., & Schweitzer, J. (2012). E-health in low-and middle-income countries: findings from the Center for Health Market Innovations. *Bulletin of the World Health Organization, 90*(5), 332-340.

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

Li, H., Gupta, A., Zhang, J., & Sarathy, R. (2014). Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision support systems, 57*, 376-386.

Li, T., & Slee, T. (2014). The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology, 65*(8), 1541-1554.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems, 17*(1), 39-71.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communication of the Association for Information Systems, 28*(28), 453-496.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems, 54*(1), 471-481.

Libert, T. (2015). Privacy Implications of Health Information Seeking on the Web. *Communications of the ACM, 58*(3), 68-77.

Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice*. New York, NY: Plenum Press.

Lishan, X., Chiuan, Y. C., Choolani, M., & Chuan, C. H. (2009). The perception and intention to adopt female-focused healthcare applications (FHA): A comparison between healthcare workers and non-healthcare workers. *International journal of medical informatics, 78*(4), 248-258.

Lu, Y., Tan, B., & Hui, K.-L. (2004). Inducing customers to disclose personal information to internet businesses with social adjustment benefits. *In Proceedings of the Twenty-Fifth International Conference on Information Systems*. Washington, DC.

Maass, W., & Varshney, U. (2012). Design and evaluation of Ubiquitous Information Systems and use in healthcare. *Decision support systems, 54*(1), 597-609.

Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance*. Retrieved from https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance

Maiga, G., Makori, A. C., & Miph, M. (2013). User issues on the adoption of health informatics systems in level 5 Hospitals in Nyanza, Kenya. *Interdisciplinary Journal of Contemporary Research in Business, 5*(1).

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.

Martínez-Tur, V., Peiró, J. M., Ramos, J., & Moliner, C. (2006). Justice perceptions as predictors of customer satisfaction: the impact of distributive, procedural, and interactional justice. *Journal of Applied Social Psychology, 36*(1), 100-119.

Maya, E. T., Adu-Bonsaffoh, K., Dako-Gyeke, P., Badzi, C., Vogel, J. P., Bohren, M. A., & Adanu, R. (2018). Women's perspectives of mistreatment during childbirth at health facilities in Ghana: findings from a qualitative study. *Reproductive health matters, 26*(53), 70-87.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

Mbonu, N. C., van den Borne, B., & De Vries, N. K. (2009). Stigma of people with HIV/AIDS in Sub-Saharan Africa: a literature review. *Journal of tropical medicine, 2009*.

McKnight, D. H. (2005). Trust in information technology. In G. B. Davis (Ed.), *The Blackwell Encyclopedia of Management*. Malden, MA: Blackwell.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of management review, 23*(3), 473-490.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*(3), 155-179.

Mikula, G., Petri, B., & Tanzer, N. (1990). What people regard as unjust: Types and structures of everyday experiences of injustice. *European journal of social psychology, 20*(2), 133-149.

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision support systems, 56*, 103-114.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behaviour. *Information & Management, 52*(6), 741-759.

Mitchell, V.-W. (1999). Consumer perceived risk: conceptualisations and models. *European Journal of marketing, 33*(1/2), 163-195.

Ministry of Health. (2010). *National E-Health Strategy*. Accra, Ghana: Author.
Moloney, M., & Potìa, V. (2013). *A Behavioural Perspective on the Privacy Calculus Model*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2310535.
Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management, 47*, 120-130.
Mou, J., & Cohen, J. (2014). Trust, risk barriers and health beliefs in consumer acceptance of online health services. *In Proceedings of the Thirty Fifth International Conference on Information Systems*. Auckland, New Zealand.
Mou, J., Shin, D.-H., & Cohen, J. F. (2017). Tracing College Students' Acceptance of Online Health Services. *International Journal of Human–Computer Interaction, 33*(5), 371-384.
Moyer, C. A., Adongo, P. B., Aborigo, R. A., Hodgson, A., & Engmann, C. M. (2014). 'They treat you like you are not a human being': maltreatment during labour and delivery in rural northern Ghana. *Midwifery, 30*(2), 262-268.
Mugo, D. M., & Nzuki, D. (2014). Determinants of electronic health in developing countries. *International Journal of Arts and Commerce, 3*(3), 49-60.
Myjoyonline. (2018). *CID stops GH₵326m bank theft*. Retrieved February from https://www.myjoyonline.com/news/2018/July-30th/cid-stops-gh326m-bank-theft.php
Newell, P. B. (1995). Perspectives on privacy. *Journal of environmental psychology*, *15*(2), 87-104.
Ohuabunwa, E. C., Sun, J., Jubanyik, K. J., & Wallis, L. A. (2016). Electronic Medical Records in low to middle income countries: the case of Khayelitsha Hospital, South Africa. *African Journal of Emergency Medicine, 6*(1), 38-43.
Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research, 2*(1), 1-28.
Oxford Business Group. (2014). *The Report: Ghana 2014*. Retrieved from https://www.oxfordbusinessgroup.com/ghana-2014
Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC medical informatics and decision making, 15*(1), 86.
Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.
Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS quarterly*, *35*(4), 977-988.
Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information systems research, 15*(1), 37-59.
Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly, 31*(01), 105-136.
Payton, F. C., Pare, G., LeRouge, C., & Reddy, M. (2011). Health care IT: Process, people, patients and interdisciplinary considerations. *Journal of the Association for Information Systems, 12*(2/3), i-xiii.
Policy Engagement Network. (2010). *Electronic health privacy and security in developing countries and humanitarian operations*. London: London School of Economics and Political Science.
Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International journal of medical informatics*, *80*(2), 94-101.

Peter, J. P., & Tarpey, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of consumer research*, *2*(1), 29-37.
Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.
Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS quarterly*, *31*(04), 623-656.
Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.
Pitta, D. A., Franzak, F., & Laric, M. (2003). Privacy and one-to-one marketing: resolving the conflict. *Journal of Consumer Marketing*, *20*(7), 616-628.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioural research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.
Ponemon Institute. (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. Retrieved from https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf
Posner, R. A. (1978). An economic theory of privacy. *Regulation*, *2*, 19.
Posner, R. A. (1981). The economics of privacy. *The American economic review*, *71*(2), 405-409.
Pew Research Center. (2015). *Internet seen as positive influence on education but negative on morality in emerging and developing nations*: Author.
Rahman, M. S. (2017). Does personality matter when we are sick? An empirical study of the role of personality traits and health emotion in healthcare technology adoption decision. *In Proceedings of the 50th Hawaii International Conference on System Sciences.* Waikoloa Beach, Puako, Hawaii.
Rahman, M. S., & Ko, M. (2012). Factors Influencing patients' perceptions toward electronic medical record (EMR) use: A conceptual model. *In Proceedings of the Eighteenth Americas Conference on Information Systems*. Seattle, Washington, DC.
Rakhmawati, T., Sumaedi, S., Bakti, I. G. M. Y., Astrini, N. J., Widianti, M. Y. T., Sekar, D. C., & Vebriyanti, D. I. (2013). Developing a service quality measurement model of public health center in Indonesia. *Management Science and Engineering*, *7*(2), 1-15.
Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, *26*(1-2), 81-99.
Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, *40*(8), 92-100.
Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH, http://www.smartpls.com
Rogers, E. M. (1995). *Diffusion of Innovations* (4 ed.). New York: Free Press.
Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000-1011.
Romanow, D., Cho, S., & Straub, D. (2012). Editor's comments: riding the wave: past trends and future directions for health IT research. *MIS quarterly*, *36*(3), III-A18.
Rothstein, M. A. (2007). Health privacy in the electronic age. *The Journal of legal medicine*, *28*(4), 487-501.
Rykwert, J. (2001). Privacy in antiquity. *Social Research*, 29-40.
Safran, C. (2001). Electronic medical records: a decade of experience. *Jama*, *285*(13), 1766-1766.

Saleh, K. (2012). *The health sector in Ghana: a comprehensive assessment*. Washington, DC: The World Bank.

Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research methods for business students* (5 ed.). Essex, England: Pearson Education Limited.

Schneider, B., & Bowen, D. E. (1995). *Winning the service game*. Boston, MA: Harvard Business School Press

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*(3), 2-16.

Schwartz, P. M. (1997). Privacy and the economics of personal health care information. *Texas Law Review, 76*(1), 1-75.

Seiders, K., Voss, G. B., Godfrey, A. L., & Grewal, D. (2007). SERVCON: development and validation of a multidimensional service convenience scale. *Journal of the Academy of Marketing Science, 35*(1), 144-156.

Seiders, K., Voss, G. B., Grewal, D., & Godfrey, A. L. (2005). Do satisfied customers buy more? Examining moderating influences in a retailing context. *Journal of marketing, 69*(4), 26-43.

Serianu. (2016). *Africa Cyber Security Report 2016*. Lavington, Kenya: Author.

Serva, M. A., Benamati, J. S., & Fuller, M. A. (2005). Trustworthiness in B2C e-commerce: An examination of alternative models. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 36*(3), 89-108.

Shaw, N. T., Kulkarni, A., & Mador, R. L. (2011). Patients and health care providers' concerns about the privacy of electronic health records: a review of the literature. *Electronic Journal of Health Informatics, 6*(1), 1-5.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18*(1), 21-32.

Shiferaw, F., & Zolfo, M. (2012). The role of information communication technology (ICT) towards universal health coverage: the first steps of a telemedicine project in Ethiopia. *Global health action, 5*(1), 15638.

Sirdeshmukh, D., Singh, J., & Sabol, B. (2002). Consumer trust, value, and loyalty in relational exchanges. *Journal of marketing, 66*(1), 15-37.

Skarlicki, D. P., & Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. *Journal of Applied Psychology, 82*(3), 434.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly, 35*(4), 989-1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly, 20*(02), 167-196.

Söllner, M., & Leimeister, J. (2013). What we really know about antecedents of trust: A critical review of the empirical information systems literature on trust. In D. Gefen (Ed.), *Psychology of Trust: New Research* (pp. 127-155). Hauppauge, NY: Nova Science Publishers.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS quarterly, 32*(03), 503-529.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behaviour. *In Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38-47). New York, NY.

Sprague, L., Simon, S., & Sprague, C. (2011). Employment discrimination and HIV stigma: survey results from civil society organizations and people living with HIV in Africa. *African Journal of AIDS Research, 10*(sup1), 311-324.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information systems research, 13*(1), 36-49.
Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization science, 14*(1), 5-17.
Stigler, G. J. (1980). An introduction to privacy in economics and politics. *The Journal of Legal Studies, 9*(4), 623-644.
Sumaedi, S., Yarmen, M., & Yuda Bakti, I. G. M. (2016). Healthcare service quality model: A multi-level approach with empirical evidence from a developing country. *International Journal of Productivity and Performance Management, 65*(8), 1007-1024.
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.
Tan, Y.-H., & Thoen, W. (2000). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce, 5*(2), 61-74.
Taylor, J. F., Ferguson, J., & Ellen, P. S. (2015). From trait to state: Understanding privacy concerns. *Journal of Consumer Marketing, 32*(2), 99-112.
Taylor, S. E., & Brown, J. D. (1988). Illusion and well-being: a social psychological perspective on mental health. *Psychological bulletin, 103*(2), 193-210.
Technomag. (2018). *520 000 Zim Healthcare Records Leaked*. Retrieved from https://www.technomag.co.zw/2018/04/17/520-000-zim-healthcare-records-leaked/
Teo, T. S., & Lim, V. K. (2001). The effects of perceived justice on satisfaction and behavioural intentions: the case of computer purchase. *International Journal of Retail & Distribution Management*, 29(2), 109-125.
Thibaut, J. W., & Walker, L. (1975). *Procedural justice: A psychological analysis*. Hillsdale, NJ: Lawrence Erlbaum Associates.
Thiebes, S., Lyytinen, K., & Sunyaev, A. (2017). Sharing is About Caring? Motivating and Discouraging Factors in Sharing Individual Genomic Data. *In Proceedings of the Thirty Eighth International Conference on Information Systems*. Seoul, South Korea.
Tittle, C. R. (1980). *Sanctions and social deviance: The question of deterrence*. New York: Praeger.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behaviour: An experimental study. *Information systems research, 22*(2), 254-268.
Tyler, T. R., & Degoey, P. (1996). Trust in organizational authorities. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 331-356). Thousand Oaks, CA: Sage.
Ulasi, C. I., Preko, P. O., Baidoo, J. A., Bayard, B., Ehiri, J. E., Jolly, C. M., & Jolly, P. E. (2009). HIV/AIDS-related stigma in Kumasi, Ghana. *Health & place, 15*(1), 255-262.
United Nations. (2014). *World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352)*: Department of Economic and Social Affairs, Population Division.
UNAIDS. (2018). *Fact Sheet - World Aids Day 2018*. Retrieved from http://www.unaids.org/sites/default/files/media_asset/UNAIDS_FactSheet_en.pdf
Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415-444.
Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly, 37*(1), 21-54.
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.

Victor, V. (1964). *Work and motivation*. New York, NY: *Willey.*
Vodicka, E., Mejilla, R., Leveille, S. G., Ralston, J. D., Darer, J. D., Delbanco, T., . . . Elmore, J. G. (2013). Online access to doctors' notes: patient concerns about privacy. *Journal of medical Internet research, 15*(9), e208.
Walsham, G., Robey, D., & Sahay, S. (2007). Foreword: Special issue on information systems in developing countries. *MIS quarterly, 31*(02), 317-326.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review, 4*(5), 193-200.
Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS quarterly, 29*(1), 35-57.
Webb, T. L., & Sheeran, P. (2006). Does changing behavioural intentions engender behaviour change? A meta-analysis of the experimental evidence. *Psychological bulletin, 132*(2), 249.
Webster, P. C. (2011). The rise of open-source electronic health records. *The lancet, 377*(9778), 1641-1642.
Weinstein, W. L. (2017). The private and the free: A conceptual inquiry. In J. R. Pennock & J. W. Chapman (Eds.), *Privacy and Personality* (pp. 27-55). New York, NY: Routledge.
Westin, A. F. (1967). *Privacy and freedom* (Vol. 1). New York: Atheneum.
Westin, A. F. (2000). Intrusions. *Public Perspective, 11*(6), 8-11.
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues, 59*(2), 431-453.
Whetstone, M., & Goldsmith, R. (2009). Factors influencing intention to use personal health records. *International Journal of Pharmaceutical and Healthcare Marketing, 3*(1), 8-25.
White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology, 14*(1-2), 41-51.
World Health Organization (2006). *Electronic Health Records: Manual for Developing Countries*. Geneva, Switzerland: Author.
World Health Organization. (2016). *Global diffusion of eHealth: making universal health coverage achievable: report of the third global survey on eHealth*. Geneva, Switzerland: Author.
Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. *Health informatics journal, 18*(3), 191-201.
Willison, D. J., Schwartz, L., Abelson, J., Charles, C., Swinton, M., Northrup, D., & Thabane, L. (2007). Alternatives to project-specific consent for access to personal information for health research: what is the opinion of the Canadian public? *Journal of the American Medical Informatics Association, 14*(6), 706-712.
Willison, D. J., Steeves, V., Charles, C., Schwartz, L., Ranford, J., Agarwal, G., . . . Thabane, L. (2009). Consent for use of personal information for health research: Do people with potentially stigmatizing health conditions and the general public differ in their opinions? *BMC medical ethics, 10*(10).
Willyard, C. (2010). Electronic records pose dilemma in developing countries. *Nature Medicine, 16*, 249-249.
Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. *In Proceedings of the Thirty Third International Conference on Information Systems*. Orlando, FL.
Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concern. *Journal of Service Research, 12*(2), 190-207.
World Bank. (2016a). *World Development Indicators*. Washington, DC: Author.

World Bank. (2016b). *While Poverty in Africa Has Declined, Number of Poor Has Increased*. Washington, DC: Author.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *In Proceedings of the Twenty Ninth International Conference on Information Systems*. Paris, France.

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

Xu, H., Teo, H.-H., & Tan, B. (2005). Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *In Proceedings of the Twenty-Sixth International Conference on Information Systems*. Las Vegas, NV.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information systems research, 23*(4), 1342-1363.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the Association for Information Science and Technology, 58*(5), 710-722.

Yao, M. Z., & Zhang, J. (2008). Predicting user concerns about online privacy in Hong Kong. *CyberPsychology & Behaviour, 11*(6), 779-781.

Yoo, C. W., Yim, M.-S., & Rao, H. R. (2013). Role of Trust in Privacy Assurance and Perceived Disease Severity on Personal Health Information Disclosure. *In Proceedings of the Thirty Fourth International Conference on Information Systems*. Milan, Itlay.

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

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce, 16*(4), 53-90.

Zheng, S., Shi, K., Zeng, Z., & Lu, Q. (2010). The exploration of instrument of users' privacy concerns of Social Network Service. *In Proceedings of the International Conference on Industrial Engineering and Engineering Management* (pp. 1538-1542).

Zhou, J. (2018). Factors Influencing People's Personal Information Disclosure Behaviours in Online Health Communities: A Pilot Study. *Asia Pacific Journal of Public Health, 30*(3), 286-295.

Zviran, M. (2008). User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems, 48*(4), 97-105.

APPENDIX A: DEMOGRAPHICS AND PRIVACY CONCERNS

Table A1 Influence of Gender on Privacy Concerns

Study	Sample	Context	Findings		
			Females have higher privacy concerns	Males have higher privacy concerns	No statistical differences
Sheehan (1999)	889 Internet users in the U.S.	online marketing	✓		
Phelps et al. (2000)	556 consumers in the U.S.	Direct marketing			✓
Chen et al. (2001)	340 respondents in the U.S.	Internet	✓		
Bellman et al. (2004)	534 responses from Europe and the U.S.	Internet	✓		
Janda and Fair (2004)	440 Internet users in the U.S.	Internet	✓		
Yao et al. (2007)	413 undergrad students in the U.S.	Internet			✓
Fogel and Nehmad (2009)	205 undergrad students in the U.S.	SNS*	✓		
Youn (2009)	144 middle school students in the U.S.	Internet	✓		
Hoy and Milne (2010)	589 Facebook users aged 18-24 in the U.S.	SNS	✓		
Joinson et al. (2010)	759 members of an online research panel	Internet	✓		
Laric et al. (2009)	225 MBA students from Canada & U.S.	Healthcare	✓		
Perera et al. (2011)	511 patients in Canada	Healthcare	✓		
Hwang et al. (2012)	213 Internet users in Taiwan	Healthcare			✓
Wilkowska and Ziefle (2012)	Germany: focus group – 19; surveys – 104.	Healthcare	✓		
Ancker et al. (2013)	1000 respondents in the U.S.	Healthcare			✓
Vodicka et al. (2013)	3874 patients in the U.S.	Healthcare	✓		
Ermakova et al. (2014)	260 responses from Germany and Switzerland	Healthcare			✓
Kordzadeh and Warren (2014)	315 students in the U.S..	Healthcare	✓		
Kenny and Connolly (2016)	202 U.S. and 245 Ireland samples	Healthcare		✓ – Irish sample	✓ – U.S. sample
Esmaeilzadeh (2018)	826 health consumers in the U.S.	Healthcare			✓

Note: *Social Networking Site

Table A2 Influence of Age on Privacy Concerns

Study	Sample	Context	Findings		
			Age positively affects concern	**Age negatively affects concern**	**No statistical differences**
Phelps et al. (2000)	556 consumers in the U.S.	Direct marketing			✓
Zhang et al. (2002)	Online consumers: U.S. (340), China (106).	Internet	✓ – U.S. sample	✓ – Chinese sample	
Bellman et al. (2004)	534 responses from Europe and the U.S.	Internet	✓		
Janda and Fair (2004)	440 Internet users in the U.S.	Internet	✓		
Hart (2008)	821 Internet Users in South Africa	Internet			✓
Chen et al. (2009)	150 university students in Singapore	SNS			✓
Ji and Lieber (2010)	1623 Internet users in the U.S.	Internet	✓		
Joinson et al. (2010)	759 members of an online research panel	Internet	✓		
Tsai et al. (2011)	272 respondents in the U.S.	E-commerce			✓
Laric et al. (2009)	225 MBA students from Canada & U.S.	Healthcare	✓		
Hwang et al. (2012)	213 Internet users in Taiwan	Healthcare			✓
King et al. (2012)	700 respondents in Australia	Healthcare	✓	✓ – 60 and above	
Wilkowska and Ziefle (2012)	Germany: focus group – 19; surveys – 104.	Healthcare	✓		
Ancker et al. (2013)	1000 respondents in the U.S..	Healthcare	✓		
Vodicka et al. (2013)	3874 patients in the U.S.	Healthcare		✓ – above 55	
Ermakova et al. (2014)	260 responses from Germany and Switzerland	Healthcare			✓
Kordzadeh and Warren (2014)	315 students in the U.S..	Healthcare			✓
Papoutsi et al. (2015)	Over 2000 respondents in the UK	Healthcare	✓		
Kenny and Connolly (2016)	447 respondents in the U.S. (202) and Ireland (245)	Healthcare	✓		
Kordzadeh et al. (2016)	235 members and non-members of VHCs* in the U.S.	Healthcare		✓ – non-members	✓ -actual members
Esmaeilzadeh (2018)	826 health consumers in the U.S.	Healthcare	✓		

Note: *Virtual Health Communities

Table A3 Influence of Education on Privacy Concerns

Study	Sample	Context	Findings		
			Education positively affects concern	Education negatively affects concern	No statistical differences
Chen et al. (2001)	340 respondents in the U.S.	Internet			✓
Zhang et al. (2002)	Online consumers: U.S. (340), China (106).	Internet			✓
Sheehan (2002)	889 Internet Users in the U.S.	Internet	✓		
Bellman et al. (2004)	534 responses from Europe and the U.S.	Internet			✓
Jin Chen et al. (2009)	150 university students in Singapore	SNS			✓
Hwang et al. (2012)	213 Internet users in Taiwan	Healthcare	✓		
King et al. (2012)	700 respondents in Australia	Healthcare		✓	
Vodicka et al. (2013)	3874 patients in the U.S.	Healthcare		✓	
Rogith et al. (2014)	100 female cancer patients in the U.S.	Healthcare			✓
Papoutsi et al. (2015)	Over 2000 respondents in the UK	Healthcare	✓		
Esmaeilzadeh (2018)	826 health consumers in the U.S.	Healthcare		✓	

Table A4 Influence of Health Status on Privacy Concerns

Study	Sample	Context	Findings		
			Poor health status positively influence concern	**Poor health status negatively influence concern**	**No statistical differences**
Wilkowska and Ziefle (2012)	Germany: focus group (19), surveys (104).	Healthcare		✓[1]	
Vodicka et al. (2013)	3874 patients in the U.S.	Healthcare			✓
Ermakova et al. (2014)	260 responses from Germany and Switzerland	Healthcare			✓
Kordzadeh and Warren (2014)	315 students in the U.S.	Healthcare			✓
Kenny and Connolly (2016)	447 respondents in the U.S. (202) and Ireland (245)	Healthcare			✓
Kordzadeh et al. (2016)	235 members and non-members of VHCs in the U.S.	Healthcare	✓[2]		
Esmaeilzadeh (2018)	826 health consumers in the U.S.	Healthcare		✓[3]	
Flynn et al. (2003)	80 psychiatric patients in the U.S.	Healthcare	✓		
Lafky and Horan (2011)	28 interviewees and 210 survey respondents in the U.S.	Healthcare		✓	

Note:

1. Healthy adults require and insist on the highest security and privacy standards compared with males and the ailing elderly.
2. For non-members of virtual health communities (VHCs), poor health status had positive influence on concerns. However, the relationship was insignificant for actual members.
3. Individuals who perceive their health status to be good have a higher level of privacy concern related to the use of health information exchange (HIE) by healthcare providers than those who perceive themselves unhealthy and ill.

APPENDIX B: SUMMARY OF IS PRIVACY RESEARCH IN HEALTHCARE

Author	Focus	User Base	Methodology	Theory Applied	Major Findings
Klein (2007)	Patients' acceptance of an Internet-based patient-physician communication application	143 first-time users of the email application in the U.S.	Online survey	Technology Acceptance Model (TAM), Trust Beliefs	Behavioural intention to use the application has significant effect on actual usage of the application. Patients' trust beliefs in both their healthcare provider and the Web site vendor have significant positive effect on behavioural intentions. Perceived ease of use (PEOU) impacts perceived usefulness which in turn influences behavioural intention. Trust in a website vendor was predicted by perceived vendor reputation and PEOU.
Angst and Agarwal (2009)	Individuals' attitudes and opt-in behavioural intentions toward electronic health records (EHRs)	366 respondents in the U.S.	Experiment using online survey	Elaboration Likelihood Model, Concern For Information Privacy (CFIP)	The study investigates whether individuals can be persuaded to change their attitudes and opt-in behavioural intentions toward EHR systems and allow digitization of their PHI. Argument framing, issue involvement and CFIP significantly influence attitudes toward EHR use by individuals. The three constructs also interact to influence attitudes toward EHR use. An important finding from these interactions is that in the presence of high privacy concerns, attitudes of individuals can be positively altered with messages that endorse the use of EHR systems. Attitude toward EHR use and CFIP have significant direct effect on opt-in behavioural intentions.
Whetstone and Goldsmith (2009)	Consumers' intention to create and use personal health records	542 college students in the U.S.	Online questionnaire	TAM	Personal innovativeness, perceived usefulness, confidence in privacy and security were positively associated with intention to create and use personal health records.
Bansal and Davenport (2010)	Intention to transact with health websites	190 college students in the U.S.	Online scenario-based survey	Utility Theory	The study investigates the moderating role of perceived poor health status on the relationship between the four dimensions of privacy concerns (collection, errors, secondary use, and improper access) and intention to transact with high trust websites (offering no discount) versus low trust websites (offering high discount). Collection and errors had a positive impact on individuals' preference of trust over discount, whereas improper access had a negative impact indicating a preference of discount over trust. The influence of secondary use was not significant. The relationship between secondary use and preference of trust over discount was significantly moderated by perceived poor health status. The other moderating relationships were not supported.

Author	Focus	User Base	Methodology	Theory Applied	Major Findings
Bansal et al. (2010)	Individuals' intention to disclose health information online	367 college students in the U.S.	Online Lab Experiment	Utility Theory	Poor health status positively affects perceived health information sensitivity which in turn significantly affects privacy concerns. Privacy concerns, trust in health website, and prior positive experience with health website significantly predict intention to disclose health information online. Prior positive experience with a health website and risk beliefs also predict trust in the health website.
Anderson and Agarwal (2011)	Individuals' willingness to provide access to their electronic PHI	1,089 U.S. adults	Online Scenario-based quasi-experiment	Privacy Calculus, Communication Privacy Management Theory, Risk-as-Feelings	The study examines the role played by type of information (general health, mental, genetic), the purpose for which it is to be used (care, research, marketing), and the requesting stakeholder (hospitals, the government, pharmaceutical companies) in influencing the impact of trust in the electronic medium and electronic information privacy concerns on individuals' willingness to provide access to their electronic PHI. Type of PHI does not moderate concern/willingness to disclose, and trust/willingness to disclose relationships. Consumers concerns are greater when requests are made for marketing or research purposes but are less for the purpose of care. Individuals with higher levels of trust are more willing to provide access to PHI if request is made for the purpose of research. However, those with lower levels of trust are less willing to provide PHI access for the purpose of research than for patient care or marketing purposes. Though there is no significant difference between individuals' willingness to provide PHI access for patient care and marketing purposes, individuals are less willing to provide access for marketing purposes. Consumer concerns are greater in disclosing to government than to hospitals or pharmaceutical companies. Consumers, however, trust and are more willing to disclose PHI to hospitals than government or pharmaceutical companies. Emotion related to health also significantly influences willingness to disclose. Individuals who feel more negative about their health are more willing to provide access to their PHI.
Hwang et al. (2012)	Privacy concerns of individuals regarding electronic medical	213 Respondents from Taiwan	Online Survey	CFIP	The study examines the influence of Internet users' age, gender, occupation, educational level, and EMR awareness on their privacy concerns regarding EMRs. The results the respondents had substantial privacy concerns regarding EMRs and their educational level and EMR awareness significantly influenced their privacy concerns regarding unauthorised access and secondary use of EMRs.

Author	Focus	User Base	Methodology	Theory Applied	Major Findings
	records (EMRs)				
Miltgen et al. (2013)	Individuals' acceptance and recommendation of biometric identification systems	326 young (15-25years old) European citizens	Online scenario-based survey	TAM, DOI, UTAUT, Privacy Calculus	Privacy calculus factors, trust in technology and perceived risk, strongly predicted biometric systems acceptance and recommendation than constructs from the traditional adoption models including compatibility, perceived usefulness, and facilitating conditions. The only exception was innovativeness which also had a strong impact on biometric systems acceptance and recommendation.
Ermakova et al. (2014)	Individuals' intention to allow sharing of their medical records in the cloud	266 respondents from Germany and Switzerland	Online survey	Privacy Calculus, UTAUT	Perceived benefits and privacy concern both had significant effect on individuals' intentions to allow sharing of their medical records in cloud computing environment with perceived benefits exerting greater influence. Trust in cloud providers, trust in privacy-preserving technological mechanisms, and trust in privacy-preserving regulatory mechanism were significant antecedents to privacy concerns.
Kordzadeh and Warren (2014)	Individuals' intention to join online health communities (OHCs)	315 students in the U.S. enrolled in IS courses	Paper-based survey	APCO Model	Compared with men, women were more concerned about privacy of PHI in OHCs. PHI privacy concern is negatively related to the likelihood of joining OHCs. Age and health status were not significant predictors of PHI privacy concerns.
Kuo et al. (2014)	Explores the relationship between patients' privacy concerns and their protective responses.	204 patients in a Taiwanese hospital	Manual Survey	Protection Motivation Theory	Patients' concerns about the collection of information about themselves, the secondary use of this information and the possibility of errors in the recorded information were associated with their information privacy-protective responses. Concern for unauthorised access to their information by other staff in the medical facility was not. Protective responses items include refusal to disclose information, misrepresentation, etc.

Author	Focus	User Base	Methodology	Theory Applied	Major Findings
Mou and Cohen (2014)	Individuals' intention to use online health services	703 college students enrolled in computer courses from South Africa	Online experiment	Health Belief Model, Extended Valence Framework	Trust in the online health service provider had the strongest effect on the intention to use online health services. It also had significant positive effect, and negative effect on perceived benefit and perceived risk barriers, respectively. Perceived risk barriers and perceived benefit also had significant impact on usage intention. Health belief variables, perceived susceptibility and severity were also significant predictors of usage intention.
Li and Slee (2014)	Users' intention to opt in to an EHR system	160 Users of EHR system in the Netherlands	Online Experiment	Theory of Reasoned Action	Privacy concerns had a significant negative effect on opt-in behaviour. This relationship is moderated by the type of EHR system (stand-alone vs. networked), and ability to control information. The negative effect of privacy concerns on opt-in behaviour is greater for a networked EHR system than for a stand-alone system. Giving users greater ability to control their information alleviate their privacy concerns when they make opt-in decisions. Attitude toward EHR use, and perceived usefulness were significant positive predictors of opt-in behaviour.
Jena (2015)	Individuals' willingness to share PHI in a digitized format	154 U.S. citizens in the Amazon Mechanical Turk crowdsourcing platform	Online survey	Information Boundary Theory	Value for personalization and trust in the electronic medium significantly predict willingness to share PHI, whereas privacy concern was insignificant. The study also found that trust in the electronic medium significantly moderate the influence of value for personalization. There is a significant interaction effect between privacy concern and value for personalization.
Dinev et al. (2016)	Factors affecting individuals' attitudes toward EHRs	217 respondents from the U.S. and 188 respondents from Itlay	Manual survey	Privacy Calculus	Perceived benefits of EHR, convenience, and information privacy concerns have significant influence on attitude toward EHR. Perceived control and trust in EHR system reduce privacy concerns. Perceived effectiveness of technological mechanisms and perceived effectiveness of regulatory mechanisms were significant predictors of trust in EHR system. Internet experience was insignificant in predicting attitude toward EHR.
Li et al. (2016)	Explores predictors of individuals' adoption of healthcare wearable devices	333 actual users of healthcare wearable devices in China	Online survey	Privacy Calculus	Individuals' intention to adopt has significant positive effect on their actual adoption of healthcare wearable devices. Perceived privacy risk and perceived benefit were significant predictors of adoption intention. Perceived benefit has significant positive effect on perceived privacy risk. Perceived privacy risk is formed by perceived prestige, legislative protection, personal innovativeness, and information sensitivity. perceived informativeness and functional congruence determined perceived benefit.

Author	Focus	User Base	Methodology	Theory Applied	Major Findings
Kenny and Connolly (2016)	Antecedents to health information privacy concerns (HIPC)	202 U.S. and 245 Irish samples	Online survey	Information Boundary Theory, Protection Motivation Theory, APCO Model	The study examines antecedents to HIPC among citizens from the US and Ireland. Males expressed greater privacy concerns among the Irish sample but no significant effect was found in the US sample. Age was significant whereas poor health status was insignificant in both samples. Healthcare need was only significant among the Irish sample. Regarding individual perceptions, perceived sensitivity had significant influence on HIPC in both samples. Trust perceptions regarding health technology vendors and health professionals significantly predicted HIPC in the Irish sample. Trust in health professionals had a contrary effect on HIPC. Risk perceptions regarding health professionals was significant in both samples, whereas risk perceptions regarding health technology vendors was significant only in the US sample. Regarding individual experiences, privacy media coverage was significant only in the US sample, whereas past privacy experience was insignificant in both samples.
Kordzadeh and Warren (2017)	Users' willingness to communicate PHI in virtual health communities (VHCs)	A sample of 235 from the U.S., 127 were actual members of VHCs, whereas 108 were familiar with VHCs.	Paper-based Survey	Privacy Calculus, Affective Commitment	Privacy concerns, expected personal and community-related outcomes of communicating PHI significantly affected willingness to communicate PHI. Affective commitment was not a significant predictor of willingness to disclose PHI.
Rahman (2017)	Individuals' intention to use patient portal	251 undergraduate students in the U.S.	Manual survey	Personality traits and Health Status Emotion	The study examined the influence of personality traits and health status emotion on intention to use patient portals. The study also examined the interaction effect between patients' personality traits and health emotional state. Health status emotion has positive effect on intention to use. Among the five personality traits, only conscientiousness was a significant predictor of intention to use. Control variables including race, computer experience, and education were significant predictors of intention to use.

Author	Focus	User Base	Methodology	Theory Applied	Major Findings
Thiebes, Lyytinen, and Sunyaev (2017)	Individuals' willingness to donate their genomic data	30 genomic data donors and genomic researchers	Online Ranking-type Delphi study	Privacy Calculus	The study explores the motivating and discouraging factors that influence individuals' willingness to donate their genomic data to human genomic research. The results show that major motivators include altruistic factors such as contribution to scientific and medical research and personal benefits (e.g., identifying predispositions for certain diseases). Privacy concerns and fear of adverse consequences (e.g., discrimination) were the main discouraging factors. Concerns about privacy reflected in secondary use (e.g., commercial use and government abuse), lack of genomic data protection (e.g., insecure data handling), and lack of control once data is donated (e.g., no possibility to withdraw data).
Esmaeilzadeh (2018a)	Consumers' opt-in behavioural intention toward Health Information Exchanges (HIEs)	826 health consumers in the U.S. who were familiar with HIEs	Online survey	APCO Model	Privacy concern has significant negative effect on consumers' opt-in decision to HIEs. Perceived health information sensitivity and computer anxiety significantly predict privacy concern. Perceived poor health status significantly attenuates the negative effect of privacy concern on opt-in intention. Regarding control variables, age had a positive effect whilst education has a negative effect on privacy concerns. Age also has a significant negative influence on opt-in intention toward HIEs. In contrast, no effects of gender were found on privacy concern and opt-in intention. Education also has no effect on opt-in intention.
Esmaeilzadeh (2018b)	Consumers' opt-in behavioural intention toward HIEs	683 respondents in the U.S.	Online survey	Utility Theory	Perceived benefits and perceived risk associated with HIEs significantly influence perceived value with perceived benefits exerting greater influence than perceived risks. Perceived value fully mediates the influence of perceived benefits and perceived risks on opt-in intention to HIEs. Attitude toward HIE models, perceived trustworthiness of healthcare entities, perceived health information sensitivity, and perceived health status were significant predictors of perceived risk.
Zhou (2018)	Predictors of PHI disclosure behaviours in online health communities (OHCs)	376 members of a Chinese online cancer community	Online survey	N/A	Perceived usefulness, financial risk, and privacy risk were significant predictors of PHI disclosure behaviour in OHCs. The effect of emotional support was insignificant. Disease severity significantly moderates the effects of emotional support and financial risk on individuals' PHI disclosure behaviour.

APPENDIX C: ETHICS APPROVAL LETTER

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

HUMAN ETHICS COMMITTEE

Secretary, Rebecca Robinson
Telephone: +64 03 369 4588, Extn 94588
Email: human-ethics@canterbury.ac.nz

Ref: HEC 2017/45/LR-PS

13 September 2017

Ernest Kwadwo Adu
Accounting and Information Systems
UNIVERSITY OF CANTERBURY

Dear Ernest

Thank you for submitting your low risk application to the Human Ethics Committee for the research proposal titled "The Digitization of Healthcare: Examining Consumer Willingness to Disclose Personal Health Information In Developing Countries: the Case of Ghana".

I am pleased to advise that this application has been reviewed and approved.

Please note that this approval is subject to the incorporation of the amendments you have provided in your email of 8th September 2017.

With best wishes for your project.

Yours sincerely

pp. R. Robinson

Associate Professor Jane Maidment
Chair, Human Ethics Committee

APPENDIX D: SURVEY INVITATION TO HOSPITALS EXAMPLE

Department: Accounting and Information Systems
Researcher: Ernest Kwadwo Adu (ernest.adu@pg.canterbury.ac.nz)

September 04, 2017

The digitization of Healthcare in Developing Countries: Examining Individuals' Willingness to Disclose Personal Health Information

In July 2010, Ghana launched a national strategy[3] for the computerization of the health sector. In line with this strategy, many hospitals are gradually shifting from manually recording personal health information (PHI) on paper to storing this information in an electronic (or computer) format[4].

A recent study[5] in Ghana, however, found that individuals are concerned about the privacy of their PHI with the introduction of computer systems in hospitals. You are invited to participate in a research project which seeks to understand the factors that influence PHI disclosure by individuals when they receive care from hospitals where the disclosed health information is stored in an electronic format. The findings of the project will provide a better understanding of what may support or hinder the effort to computerize healthcare in Ghana.

The project is being carried out as a requirement for a Doctor of Philosophy degree by Ernest Kwadwo Adu under the supervision of A/Professor Annette Mills, who can be contacted at annette.mills@canterbury.ac.nz. She will be pleased to discuss any concerns you may have about participation in the project.

Your involvement in this project will be to facilitate the recruitment of voluntary participants. To this end, you can post a notice in a public space, such as a waiting room, to inform patients and other hospital visitors of this survey. Hard copies of the questionnaire will be distributed in person to volunteered participants by our research team or someone that you may designate in your organization. Participants will be rewarded five Ghana cedis (**GH₵3**) worth of mobile credits for their time and effort spent to take the survey.

The survey is anonymous, and participants will not be identified. Participation is completely voluntary, and participants have the right to withdraw at any stage up until we collect the questionnaire and add it to the others that have been collected. Once a participant's data is combined with the other data collected it cannot be retrieved as the survey is anonymous.

The survey will take about 25 minutes to complete. The results of the project may be published, but your identity (or that of participants) will not be made public. The thesis publishing the results of the study will be a public document and will be available through the UC Library. To ensure results are communicated to those wanting to receive a copy of the project results, contact details will be recorded at the time of the main data collection. To maintain anonymity this data is kept separate from the main survey.

This project has been reviewed and approved by the University of Canterbury Human Ethics Committee, and participants should address any complaints to The Chair, Human Ethics Committee, University of Canterbury, Private Bag 4800, Christchurch (human-ethics@canterbury.ac.nz).

If your organization is interested in participating in this study, please contact me and we will arrange the timing and method for the distribution of the questionnaires.

Yours sincerely,
Ernest Kwadwo Adu

---

[3] Ministry of Health. (2010). *National E-Health Strategy.* Accra, Ghana

[4] Acquah-Swanzy, M. (2015). Evaluating Electronic Health Record Systems in Ghana: the case of Effia Nkwanta Regional Hospital (Master's thesis, UiT Norges arktiske universitet)

[5] Bedeley, R., & Palvia, P. (2014). A study of the issues of E-health care in developing countries: The case of Ghana.

APPENDIX E: SURVEY INSTRUMENT

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Department: Accounting and Information Systems
Researcher: Ernest Kwadwo Adu *(ernest.adu@pg.canterbury.ac.nz)*

Please read the following before completing the questionnaire.

In July 2010, the government of Ghana launched a national strategy[6] for the computerization of the health sector. In line with this strategy, many hospitals are gradually shifting from manually recording patient health information on paper to storing this information in a computer.

You are invited to participate in a research project which seeks to understand the factors influencing individuals living in Ghana to disclose their health information when receiving care from hospitals where the disclosed information is stored in a computer. Your response is important and will help to identify what may support or hinder the effort to computerize healthcare in Ghana. The survey should take about 30 minutes to complete.

The project is being carried out as a requirement for a doctoral degree by Ernest Kwadwo Adu under the supervision of Prof. Annette Mills, who can be contacted at *annette.mills@canterbury.ac.nz.* She will be pleased to discuss any concerns you may have about participation in the project.

The questionnaire is anonymous, and you will not be identified. Participation is voluntary, and you may stop and withdraw any information you have provided, up until you submit your questionnaire to us, and it has been added to the other questionnaires collected. As the questionnaire is anonymous, your data cannot be withdrawn once it has been combined with the other data collected.

By completing the questionnaire it will be understood that you have consented to participate in the project and that you consent to the publication of the results of the project with the understanding that anonymity will be preserved. A thesis is a public document and will be available through the UC Library. If you are interested to receive a copy of the results of the project, please provide your contact details on the enclosed form.

This project has been reviewed and approved by the University of Canterbury Human Ethics Committee, and participants should address any complaints to: *The Chair, Human Ethics Committee, University of Canterbury, Private Bag 4800, Christchurch (human-ethics@canterbury.ac.nz).*

Participants could refer to the following support service should they feel distressed during the survey:

Open Door Counselling Services
Phone: 0274 441 544 or 0241 745 308
No 2 Child link Street Spintex,
Accra, Ghana.

Thank you for your participation in this research project.

[6] Ministry of Health. (2010). *National E-Health Strategy*. Accra, Ghana

INTRODUCTION

This survey seeks to understand the views of individuals living in Ghana regarding the use of computers by hospitals to store their personal health information. It is aimed at individuals (*18 years or older*) who may need to visit a hospital to receive care where they are asked to disclose their personal health information.

For each question, please select the response that you feel is appropriate and is to the best of your knowledge. If you find it difficult to determine your exact answer, please give your best estimate. ***There are no right or wrong answers – all we are interested in is your honest response to the questions.***

Some questions may appear very similar. This is intentional to ensure greater statistical reliability and accuracy. We would be greatly appreciative if you would answer all the questions.

Key Terms

- *Personal Health information* includes all information a patient discloses in response to a doctor's questions during a consultation (e.g., drug/alcohol use, smoking, diet, physical activity, allergies, etc.). It also includes any information generated in the process of receiving care (e.g., blood test results, x-ray photo, etc.).

- The computer system which hospitals in Ghana are introducing to store health information is referred to as an *electronic health record system*. In this study, we will refer to this system as a ***Computer Health System***.

  Very Important: Please you must read and understand a short description of a Computer Health System below before answering the survey questions. Should you require any clarification, please talk to the survey administrator.

Computer Health System

Traditionally, when you visit a hospital in Ghana, a folder is created for you. Doctors, nurses, etc. manually record your personal health information on paper which is then kept in your folder. A Computer Health System is different. Instead of recording your information on paper, doctors, and nurses will record your personal health information in a computer.

The Computer Health System will store personal information such as your name, phone number, email, and address, as well as your health information altogether in one place (i.e. a central database). Other departments in the hospital (e.g., Pharmacy, Laboratory) can then access your health data and add new information to it (e.g. test results, x-rays, etc). This prevents the duplication of your health information across the departments and makes it easier for all departments to access and update your information.

Let's assume that a hospital you may go to for care has implemented a Computer Health System. When you go for treatment, the staff from the different departments you interact with will be able to access your past health information stored on the system and update it with new information. For example, a doctor will add details from your current visit (e.g., illness type, blood pressure, prescribed medication). The hospital's Pharmacy will access the doctor's prescription, and similarly, update your information with the medicine that is given to you. This way, the hospital is able to track easily your health history and treatments (e.g., past illnesses, medication, etc.).

The Computer Health System allows a hospital to control who has access to patient information. For example, while doctors may access your complete personal health information, Laboratory staff may only be able to access your medical test results. The system may also enable a hospital to perform administrative tasks such as managing the appointments of patients and schedules of hospital staff.

The Computer Health System can also allow a patient to interact remotely with hospital services. For example, you can book an appointment with a doctor, pose a question to hospital staff, or access your personal health information online through the internet.

MEASUREMENT ITEMS OF CONSTRUCTS[7]

Trust in Healthcare Providers[8] & Perceived Attitude of Health Workers

The following question relates to your perceptions about hospital healthcare delivery. Based on your knowledge of or experience with receiving healthcare from a hospital in Ghana, please provide your **best** response to the statements below:

Trust in Healthcare Providers – Benevolence (BEN)

To what extent do you agree or disagree with the following statements?

BEN1: Hospitals do their best to help patients.
BEN2: Hospitals act in the best interest of patients.
BEN3: Hospitals are interested in the well-being of patients.

Trust in Healthcare Providers – Competence (COMP)

To what extent do you agree or disagree with the following statements?

COMP1: Hospitals are competent and effective in providing healthcare.
COMP2: Hospitals perform their role of giving healthcare very well.
COMP3: Overall, hospitals are capable and proficient healthcare providers.
COMP4: In general, hospitals are very knowledgeable about healthcare.

Trust in Healthcare Providers – Integrity (INTEG)

To what extent do you agree or disagree with the following statements?

INTEG1: Hospitals are truthful in their dealings with patients.
INTEG2: Hospitals are honest.
INTEG3: Hospitals are sincere and genuine.

Perceived Attitude of Health Workers (HW_ATT)

To what extent do you agree or disagree with the following statements?

Health workers (e.g., nurses, doctors, administrative staff, etc.) in hospitals…….

HW_ATT1: …… Show good hospitality and courtesy.
HW_ATT2: …… Show respect toward the patients.
HW_ATT3: …… Show care toward the patients.
HW_ATT4: …… Show a genuine desire to help patients.

[7] Unless otherwise specified, 7-point Likert type scales anchored with "strongly disagree" and "Strongly agree" was used to measure all items.

[8] Healthcare providers were referred to in the questionnaire as Hospitals as organizations providing healthcare services in Ghana are generally referred to as hospitals.

Willingness to Disclose Personal Health Information (WILL)

Let us assume that you need to visit a hospital for care. The following sets of questions relate to your willingness to disclose your personal information to receive care from a hospital that stores personal health information in a Computer Health System.

To what extent do you agree or disagree with the following statements?

If a hospital stores personal health information in a Computer Health System, _____ my personal health information to the hospital.

WILL1: I would be likely to disclose
WILL2: I would be willing to disclose
WILL3: I would be interested in disclosing
WILL4: I would probably disclose

Convenience (CONV)

The following question relates to your beliefs about the **benefits** to patients, of the use of Computer Health Systems by hospitals.

To what extent do you agree or disagree with the following statements?

If a hospital uses a Computer Health System, then……

CONV1: …… It would be easy for patients to receive care from the hospital.
CONV2: …… Patients would spend less effort to receive care from the hospital.
CONV3: …… Patients would be able to receive care quickly at the hospital.
CONV4: …… It would take little time for patients to receive care at the hospital.

Trust, Privacy and Risk

The following questions relate to your beliefs about trust, privacy and risks in relation to **storing personal health information in a Computer Health System**.

Trust in Health Information Technology (HIT[9]) (T_HIT)

To what extent do you agree or disagree with the following statements?

T_HIT1: A Computer Health System would be a safe environment in which to store personal health information.
T_HIT2: A Computer Health System would be a reliable environment in which to conduct personal health related transactions.
T_HIT3: Hospitals would handle personal health information stored in a Computer Health System in a competent manner.

[9] The health information technology (HIT) considered in the study is a stand-alone electronic health record (EHR) system. EHR system was replaced with the term computer health system in the questionnaire since it was reasoned that individuals in developing countries might not be familiar with the term EHR.

Privacy Risk (RISK)

To what extent do you agree or disagree with the following statements?

RISK1: In general, it would be risky to store personal health information in a Computer Health System.

RISK2: There would be high potential for privacy loss associated with storing personal health information in a Computer Health System.

RISK3: Personal health information stored in a Computer Health System could be inappropriately used.

RISK4: Storing personal health information in a Computer Health System would involve many unexpected problems.

PHI Privacy Concerns – Collection (COL)

To what extent do you agree or disagree with the following statements?

COL1: It usually bothers me when hospitals ask me for personal health information.

COL2: When hospitals ask me for personal health information, I sometimes think twice before providing it.

COL3: It bothers me to give my personal health information to hospitals.

COL4: I'm concerned that hospitals are collecting too much personal health information about me.

PHI Privacy Concerns – Errors (ERR)

To what extent do you agree or disagree with the following statements?

If hospitals store personal health information in a Computer Health System……

ERR1: …… the information should be double-checked for accuracy, no matter how much this costs.

ERR2: …… they should devote more time and effort to verifying the accuracy of the information.

ERR3: …… they should have better procedures to correct errors in the information.

ERR4: …… they should take more steps to make sure that the information is accurate.

PHI Privacy Concerns - Secondary Use (SU)

To what extent do you agree or disagree with the following statements?

SU1: Hospitals should not use personal health information for any purpose unless it has been authorised by the patients who provided the information.

SU2: When people disclose their personal health information to a hospital to receive care, the hospital should never use the information for any other purpose.

SU3: Hospitals should never share personal health information with other health service providers unless it has been authorised by the patient who provided the information.

SU4: If hospitals store personal health information in a Computer Health System they should never sell the information to other organizations.

PHI Privacy Concerns – Unauthorised Access (UA)

To what extent do you agree or disagree with the following statements?

If hospitals store personal health information in a Computer Health System……

UA1: …… the system should be protected from unauthorised access no matter how much it costs.

UA2: …… they should devote more time and effort to preventing unauthorised access to the information.

UA3: …… they should devote more time and effort to preventing unauthorised access to the information.

Perceived Effectiveness of Government Regulation (REGUL)

In the year 2000, the Ghana Health Service introduced the Patient's Charter to protect the rights of the patient. Sections (7) and (8) of the Patient's Rights stipulates that:

- *A patient's information must be kept confidential, and shall not be used for any other purpose or disclosed to a third party without his/her consent except where such information is required by law or is in the public interest.*

In May 2012, the parliament of Ghana passed a law (i.e., Data Protection Act) meant to protect the privacy of the individual and personal data. According to this law (Sections 32, 28, 88, and 43):

- *Individuals have right of access to data held about them by a data controller. A data controller can be any entity (e.g., hospital) that collects and holds personal data on individuals.*
- *A data controller must prevent unlawful or unauthorised access to personal data.*
- *A person who knowingly or recklessly discloses the personal data of another person is liable to a fine or to imprisonment or to both.*
- *An individual is entitled to compensation when he/she suffers damage or distress through the violation by a data controller of the requirements (such as above) of this law.*

Prior to reading the above, were you aware of these laws?

☐ Yes, I was aware of both of them.

☐ Yes, I was aware of some of them.

☐ No, I was not aware of any of them.

Assuming your personal health information were **stored in a Computer Health System**, to what extent do you agree or disagree with the following statements?

I believe that the above laws in Ghana would effectively govern how my personal health information stored in a Computer Health System ……

REGUL1: ……is used.

REGUL2: ……is protected.

I believe that the above laws in Ghana would be……

REGUL3: …… effective in protecting me from misuse of my personal health information stored in a Computer Health System.

REGUL4: …… able to address violations in the usage of my personal health information stored in a Computer Health System.

Potential Consequences of Personal Health Information Disclosure

The following sets of questions refer to a hypothetical health situation. Please read the scenario provided and respond honestly to the questions asked.

Scenario: HIV/AIDS

Imagine you do a HIV/AIDS test and the results indicate that you have HIV/AIDS.

How sensitive would be the information indicating that you have HIV/AIDS? (**Note**: *Sensitive information refers to information that you want to keep as secret*): 7-point scales anchored with "*Not sensitive at all*" and "*Very sensitive*".

To what extent do you agree or disagree with the following statements, should people know that you have HIV/AIDS?

Perceive Inferiority (INFE)

INFE1: People would see me as not measuring up to them.
INFE2: People would look down on me.
INFE3: People would see me as not good enough.
INFE4: People would see me as small and insignificant.
INFE5: People would see me as unimportant compared to others.

Family Rejection (FAMR)

FAMR1: I would be forced out of my home by my family.
FAMR2: I would face neglect from my family.

Employment Discrimination (EMPD)

If I am applying for a job and the employer learns that I have HIV/AIDS……..
EMPD1: …… I would be denied employment.
EMPD2: …… I would be discriminated against.
If I were employed and my employer learns that I have HIV/AIDS……...
EMPD3: …… I would lose my job.
EMPD4: …… I would be denied promotion.

Control Variables

Privacy Orientation (ORIENT)

To what extent do you agree or disagree with the following statements?

ORIENT1: Keeping my personal information and activities confidential is a high priority with me.

ORIENT2: Information about my personal life is strictly a private matter.

ORIENT3: Guarding my personal information is one of my highest priorities.

ORIENT4: Overall, I have a strong need to protect my personal information.

Privacy Experience (P_EXP)

P_EXP1: How frequently have you personally been a victim of what you felt was an invasion of your privacy? 7-point scales anchored with "*Not at all"* and *"Very often".*

P_EXP2: How often have you experienced incidents where your personal information was used by a service provider without your authorisation? 7-point scales anchored with "*Not at all"* and *"Very often".*

P_EXP3: How much have you heard or read during the last year about the use and potential misuse of computerized information about people? 7-point scales anchored with "*Not at all"* and *"Very much".*

Computer Experience

How many years of experience do you have using a computer?

Never used	Less than 6 months	6months to <1 year	1 year to <3 years	3 years to <5 years	5 years to <7 years	7 year to <10 years	More than 10 years
☐	☐	☐	☐	☐	☐	☐	☐

Health Status

In general, how would you rate the state of your health?

Very poor 1 2 3 4 5 6 7 **Very good**

☐ Prefer not to say

Health Concern

In general, how worried are you about your health?

Not at all worried 1 2 3 4 5 6 7 **Extremely worried**

☐ Prefer not to say

Age

☐ 18-24 years ☐ 25-34 years ☐ 35-44 years ☐ 45-54 years
☐ 55-64 years ☐ 65+ years ☐ Prefer not to say.

Gender

☐ Male ☐ Female ☐ Prefer not to say

Education

Which of the following *best describes* your highest level of **education?**

☐ Below Junior High School
☐ Junior High School
☐ Senior High School
☐ Some Undergraduate Degree Study
☐ Bachelor's Degree (e.g.: BSc, BArts, etc.)
☐ Graduate Degree (e.g.: Master's, PhD, etc.)
☐ Other (please specify) _____
☐ Prefer not to say.