12-12-2018

# Drivers of Personal Health Information Privacy Concerns among Individuals in Developing Countries: A Conceptual Model

Ernest K. Adu
*University of Canterbury*, ernest.adu@pg.canterbury.ac.nz

Annette Mills
*University of Canterbury*, annette.mills@canterbury.ac.nz

Nelly Todorova
*University of Canterbury*, nelly.todorova@canterbury.ac.nz

# Drivers of Personal Health Information Privacy Concerns among Individuals in Developing Countries: A Conceptual Model

**Ernest K. Adu**
University of Canterbury
ernest.adu@pg.canterbury.ac.nz

**Annette M. Mills**
University of Canterbury
annette.mills@canterbury.ac.nz

**Nelly Todorova**
University of Canterbury
nelly.todorova@canterbury.ac.nz

**Paper Category:** Research-in-progress

**ABSTRACT**

In recent years, there has been increased use of electronic healthcare (e-health) in developing countries. E-health can contribute immensely to addressing the myriad of health challenges facing these countries (e.g., extending geographic access to care, improving management of health information). The emergence of e-health, however, has raised individuals' concerns about personal health information (PHI) privacy, being often identified as a key barrier to the successful implementation of e-health. To ensure the sustained growth and development of e-health in developing countries it is important to understand and respond appropriately to individuals' concerns regarding the electronic storage, use and communication of PHI as well as the factors driving these concerns.

This paper reports on a study which seeks to address the above research problem by developing and examining a model of key determinants of individual PHI privacy concerns in developing countries. More specifically, the study examines a model of the impacts of individual characteristics such as gender, individual experiences such as computer experience, and individual beliefs such as trust in e-health systems and trust in health services providers, on PHI privacy concerns. A survey study which tests the proposed model in the healthcare setting of Ghana, a Sub-Saharan African nation, is outlined. Implications for research and practice are also discussed.

**Keywords:** privacy concerns, e-health, personal health information, healthcare, developing countries

## INTRODUCTION

In recent years, there has been widespread use of ICTs in support of health services in both developed and developing countries (World Health Organization [WHO], 2016). The social and individual benefits of digitizing healthcare are considerable, especially for developing countries which are plagued by a myriad of health problems. These benefits include extending access to care to rural communities, and the efficient collection and management of health information to address epidemics such as HIV/AIDS and tuberculosis.

However, as personal health information (PHI) is digitized and shared by various stakeholders for diverse purposes, the risks to the loss of PHI privacy increase (Fichman et al., 2011). This problem is compounded by the susceptibility of electronically stored PHI to criminal attacks (e.g., hacking) and the ease with which opportunistic activities related to PHI (e.g., sharing PHI with third parties) can be carried out by stakeholders entrusted with the protection of individuals' PHI. Lending support to this, a recent study by Ponemon Institute (2016) found that criminal attacks and malicious insiders represent the main sources of PHI privacy breaches. Therefore, even in developed countries where e-health has matured, concerns about PHI privacy have heightened and represent a barrier to the sustained growth of e-health (Kenny & Connolly, 2016).

In developing countries, e-health is relatively nascent (Lewis et al., 2012). However, a few case studies in some countries (e.g., Ghana) also indicate concerns among individuals regarding the security and privacy of PHI with the introduction of e-health systems (Bedeley & Palvia, 2014; Willyard, 2010). This perhaps is not surprising as in the traditional healthcare environment in developing countries, studies show that some individuals hide their infections, especially those related to stigmatized diseases, and even avoid needed healthcare due to the fear that others will learn about their illness (Kwansa, 2013).

Quite recently, general concerns about online privacy are said to have increased in Africa and lack of trust in the Internet is keeping people from using online services including e-commerce[1]. The successful implementation and operation of most e-health systems (e.g., electronic health record systems) depend on the availability of patient information (Li & Slee, 2014). Individuals' willingness to disclose and allow their PHI to be stored in an electronic

[1] Data privacy: new global survey reveals growing internet anxiety: http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1719 Retrieved 20 September, 2018

format is thus critical to the success of e-health (Bansal et al., 2010). Therefore, as developing countries migrate to e-health systems it has become imperative to understand individuals' concerns about the privacy of digitized PHI and the factors driving these concerns. Toward this end, this study addresses the following questions:

1) What is the extent of PHI privacy concerns among individuals in developing countries?
2) What factors influence PHI privacy concerns among individuals in developing countries?

Addressing the above questions are important as scant research has focused on examining the antecedents of PHI privacy concerns (Kenny & Connolly, 2016). More importantly, the available research has been conducted mostly in developed countries producing findings that may not generalize readily to the context of developing countries (Bélanger & Crossler, 2011). One important factor may be the difference in digital experience between respondents from developed and developing countries. Several studies (e.g., International Telecommunication Union [ITU], 2016, 2017; Pew Research Center [PRC], 2015) show that most individuals in developed countries have greater digital experience compared with their counterparts in developing countries where the digital divide and gender digital gap still exist. It is thus possible that concerns about PHI privacy in digital environments and the factors driving these concerns may be different between developed and developing countries.

By examining the drivers of PHI privacy concerns among an understudied population—individuals in developing countries, this study responds to calls to study antecedents of PHI privacy concerns (Kenny & Connolly, 2016), and to extend the geographic boundaries of IS privacy research (Bélanger & Crossler, 2011). The study is expected to provide a comprehensive understanding of privacy concerns among individuals in developing countries in relation to the collection, storage and use of PHI in e-health systems. Additionally, the study aims to shed light on factors that are significant predictors of PHI privacy concerns in these settings. The study also is expected to contribute to our understanding as to whether the digital divide and gender digital gap in developing countries impact the privacy perceptions of individuals in these countries.

The rest of the paper is organized as follows. The immediately following section reviews extant IS privacy research to identify antecedents to PHI privacy concerns relevant to the context of the current study. Next, the theoretical background, research model, and

hypotheses are presented. Subsequently, we describe the research method and analysis technique for testing the proposed research model. Finally, we present the expected contributions of the study.

## LITERATURE REVIEW

Privacy concerns have severally been conceptualized and measured in the IS literature. However, the definition by Smith et al. (1996) which emphasizes individuals' worry and anxiety regarding organizational practices related to the collection and use of their personal information is commonly used by researchers. According to the authors, individuals' concerns about privacy reflect four dimensions: collection, secondary use, errors and unauthorized access. The corresponding Concern for Information Privacy (CFIP) measure which the authors developed is often used and may be considered as the de facto measure of information privacy concerns (Bélanger & Crossler, 2011).

To date, most IS privacy studies conducted in the healthcare context have examined the impact of privacy concerns on behavior-related variables such as willingness to disclose PHI (Anderson & Agarwal, 2011). This study focuses on the factors that influence individuals' concerns about their PHI. Adapting the definition by Smith et al. (1996) to the healthcare context, we define PHI privacy concerns as *"individuals' concerns regarding healthcare organizations' practices related to the collection, storage and use of their PHI"*.

## ANTECEDENTS TO PHI PRIVACY CONCERNS

Several factors have been studied as antecedents to privacy concerns, including studies conducted in the healthcare context. According to Smith et al. (2011), the influential antecedents of privacy concerns will be largely determined by the context of the study. As such, in Table 1, we present some of the commonly studied antecedents which are most relevant given the IS domain (healthcare) and geographic context (developing country) that is the focus of this study. These antecedents, though not exhaustive, are an initial attempt to understand the predictors of PHI privacy concerns in developing countries.

In the healthcare context, several studies show that health status, healthcare need, and perceived health information sensitivity are important factors in influencing individuals' PHI privacy concerns (Bansal et al., 2010; Kenny & Connolly, 2016; Laric et al., 2009). Among these three factors, health status has received considerable empirical support as a significant antecedent to individuals' PHI privacy concerns and their willingness to disclose PHI

(Esmaeilzadeh, 2018; Flynn et al. 2003). Consequently, in addition to the antecedents in Table 1, we will examine the impact of health status on PHI privacy concerns.

Table 1: Antecedents to PHI Privacy Concerns

| **Factor** | **Findings (IS in general)** | **Findings (Healthcare)** | **Relevant to Current study?** |
|---|---|---|---|
| Gender | Females express greater privacy concerns (Joinson et al., 2010). | Females express greater PHI privacy concerns (Laric et al., 2009). | YES. Influence of gender supported in various contexts including healthcare. |
| Age | Age has a positive influence on privacy concerns (Joinson et al., 2010) | PHI privacy concerns increase with age (Esmaeilzadeh, 2018; Laric et al., 2009) | YES. Several studies support the influence of age on concern. |
| Education | Most studies found no significant influence on concern (e.g., Chen et al., 2009) | Mixed findings (Esmaeilzadeh, 2018; Papoutsi et al., 2015) | YES. Education is likely to influence PHI privacy concerns in developing countries. |
| Computer experience | Internet experience examined with mixed findings (Janda & Fair, 2004; Yao & Zhang, 2008). | Computer experience reduces PHI privacy concerns in a single study (Perera et al., 2011) | YES. Given the digital divide in developing countries, computer experience is likely to influence concern. |
| Previous Privacy Experience | Consistently found to increase concern (e.g., Smith et al., 1996) | Examined in a single study which shows a significant positive effect (Bansal et al., 2010) | YES. Positive influence on concern supported in existing studies. |
| Perceived effectiveness of government regulation | Reduces privacy concerns (Xu et al., 2012) | Reduces PHI privacy concerns (Ermakova et al., 2014) | YES. Examined in a few studies and expected to affect concern. |
| Risk beliefs | Risk beliefs positively affect concern (Dinev & Hart, 2006) | Examined in a single study which shows a significant positive effect (Kenny & Connolly, 2016) | YES. Risk is expected to negatively influence privacy concern. |
| Trust beliefs | Trust beliefs reduce privacy concerns (Pavlou et al., 2007) | Examined in a few studies with mixed findings (Dinev et al., 2016; Kenny & Connolly, 2016) | YES. Trust beliefs will have positive effect on PHI privacy concern. |

Based on the review of prior IS privacy literature by Li (2011) and the classification of antecedents used in Kenny and Connolly (2016), we classify the individual factors influencing PHI privacy concerns as: (1) individual characteristics, (2) individual

experiences, and (3) individual perceptions. The proposed research model following this classification of the reviewed antecedents (Table 1) is provided in Figure 1.

## THEORETICAL BACKGROUND

Reviewing prior IS privacy research, Li (2012) identified several theories that have been used to explain individual factors that influence information privacy concerns. This study draws mainly on the protection motivation theory (PMT) (Rogers, 1975). PMT helps to explain individuals' behaviour when faced with threats. Threat in the current study's context can be anything that causes exposure of an individual's PHI. According to PMT, individuals use two cognitive processes of appraisal to cope with threats: threat appraisal, and coping appraisal. Threat appraisal includes an individual's perception of the threat they face, its severity, and the likelihood of its occurrence. Coping appraisal, on the other hand, comprises an individual's assessment of the efficacy of responses to a threat and his or her ability to perform the responses in mitigating the threat.

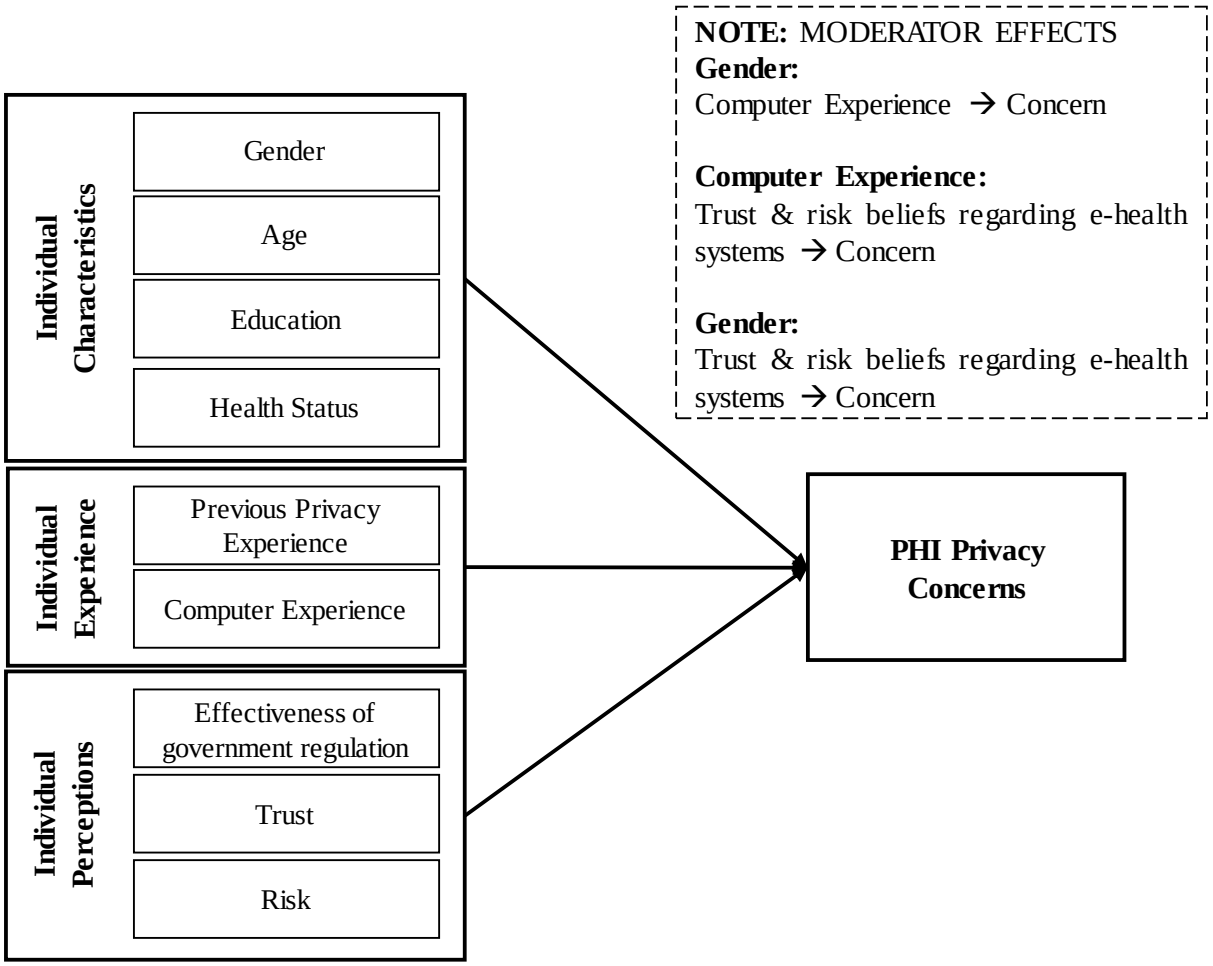


Figure 1: Proposed Research Model

In the IS privacy context, Li (2012) argues that threat and coping appraisals serve as the basis of individuals' privacy concerns. According to the author, when individuals perceive threats to privacy of their information as severe and likely to occur, and they lack the ability to take effective preventive action to address the threat, they are likely to become concerned about providing information. On the other hand, individuals are less likely to be concerned about privacy and more willing to provide information when threats to privacy is highly unlikely, and they can cope with any threats that may exist.

In the current study, *threat appraisal* is represented by two constructs: privacy experience and risk beliefs. Individuals who have suffered privacy breaches of their PHI in the past are likely to believe that such breaches may occur again in the future. Previous privacy experience thus represents individuals' awareness/perception of threats to the privacy of their PHI. Risk includes individuals' perceptions that potentially negative outcomes (e.g. loss of privacy of PHI) will result from disclosing PHI to healthcare providers where the disclosed PHI is stored and used electronically. In this study, we examine individuals risk beliefs regarding e-health systems and healthcare providers. The threat appraisal constructs are expected to increase PHI privacy concerns.

*Coping appraisal* is represented by factors such as computer experience, effectiveness of government regulation, and trust beliefs (i.e. trust in healthcare providers and trust in e-health systems). We argue that the coping appraisal constructs enhance individuals' abilities to cope with the risks facing their PHI as they alleviate their concerns and fears regarding the privacy of their PHI.

As already highlighted in the introduction section, several studies show that digital divide and gender digital gaps still exist in developing countries (ITU 2016, 2017; PRC, 2015). A few people own computers (PRC, 2015) and about 75% of people in developing countries, especially in Africa, are not using the Internet (ITU, 2016). Also, according to ITU (2017), gender digital gap is wider in Africa compared to other regions in the world. The proportion of women using the Internet is 25% lower than the proportion of men using the Internet. In contrast, in the Americas, a higher percentage of women than men are using the Internet.

Given the digital divide and gender digital gap, we argue that computer experience and gender will moderate the influence of trust and risk perceptions regarding e-health systems on PHI privacy concerns. We also expect gender to moderate the influence of computer experience on concerns.

The next section discusses the relationships in the proposed model in Figure 1 based on the theoretical foundation outlined above.

## RESEARCH MODEL AND HYPOTHESES

### Individual Characteristics

Past research shows that gender has a significant influence on privacy concerns (Joinson et al., 2010). In these studies, females have consistently been found to express greater concerns about privacy of their personal information (e.g., Joinson et al., 2010; Laric et al., 2009). Women have been found also to express greater anxiety in using computers than men (Frenkel, 1990). Some studies further show that anxiety about computers and the Internet has a positive impact on privacy concerns (e.g., Li, 2014; Schwaig et al., 2013). Hence, the following is proposed:

*H1. Females will express greater PHI privacy concerns than males would.*

Similar to gender, several studies in the healthcare and other IS contexts have consistently found a positive relationship between age and privacy concerns (Esmaeilzadeh, 2018; Joinson et al., 2010). Some authors (e.g., Laric et al. 2009) suggest the relationship between age and privacy concerns may be due to the fact that younger individuals have fewer health problems, and therefore they do not pay much attention to issues related to their PHI privacy. Following past empirical findings, it is hypothesized:

*H2. Age will be positively related to PHI privacy concerns.*

Past research on the influence of education on privacy concerns reveal mixed findings. Some studies found that higher levels of education is associated with increased PHI privacy concerns (Papoutsi et al., 2015). However, most studies indicate a negative relationship between education and PHI privacy concerns (Esmaeilzadeh, 2018; Vodicka et al., 2013).

The technology adoption literature shows that individuals with a higher level of education are early adopters of technological innovations such as personal computers (Dickerson & Gentry, 1983). Studies in developing countries similarly show that most Internet users are those with secondary school education or higher (PRC, 2015). The adoption of new IT innovations is said to entail risks including risk to personal information (Keith et al., 2015). Since individuals with higher education tend to like to try new technologies (Dickerson & Gentry, 1983), it is likely that these individuals will be more willing to take on (or feel they can cope better with) technologies that have some risks associated with them such as e-health. As such, it is expected that higher educated individuals would have less privacy concerns, and those

with less education would have more concerns. Taken altogether and based on the findings in most studies, it is expected that:

*H3. Education will be inversely related to PHI privacy concerns.*

Individuals' perceptions of their overall health condition (i.e., health status) has been well-studied as an important antecedent to PHI privacy concerns. Two dominant positions have been argued in the literature. One position is that individuals with poor health will be less concerned about privacy due to the benefits of improved care through e-health and the support they can gain by disclosing their PHI to others. In support of this, Esmaeilzadeh (2018) found that individuals who perceived themselves as unhealthy and ill were less concerned about their physicians exchanging their PHI with other healthcare organizations.

However, other studies have argued that individuals with poor health will be protective of their health information as they may have more sensitive information, the disclosure of which can result in negative consequences. For example, Flynn et al. (2003) found that individuals with mental health conditions expressed extremely high privacy concerns. Several studies (e.g., Kwansa, 2013) also show that some health conditions are heavily stigmatized in developing countries, especially in Africa. It is therefore reasoned that due to the negative consequences (e.g., loss of job or relationships) that can result from privacy breaches on PHI, individuals with poor health are likely to be more concerned about PHI privacy as they may have more sensitive health information, than those in good health. Hence:

*H4. Health status will be positively related to PHI privacy concerns.*

**Individual Experiences**

This section discusses two antecedents to PHI privacy concerns related to individual experiences: *Computer experience* and *previous privacy experience*.

Computer experience refers to general knowledge about using computers for any tasks including surfing the Internet. Computer experience has received scant attention in the healthcare context. One study found that computer experience reduces PHI privacy concerns (Perera et al., 2011). Other studies have found privacy concerns to be associated with anxieties toward computers and the Internet (Li, 2014; Schwaig et al., 2013). These anxieties, however, decrease with increased computer self-efficacy (Compeau & Higgins, 1995). Since increased computer use leads to individuals' greater beliefs in their ability to use computers (i.e., higher computer self-efficacy) (Compeau & Higgins, 1995), it is expected that individuals with greater computer experience will express less anxieties about the electronic

storage and use of PHI due to their higher computer self-efficacy. Therefore, similar to the finding by Perera et al. (2011), we propose the following hypothesis:

*H5. Computer experience will be inversely related to PHI privacy concerns.*

Previous experience of privacy invasion is expected to sensitize individuals to the threats posed to the privacy of their PHI. Individuals who have suffered privacy breaches in the past are likely to believe that this will occur again, leading to their concerns about privacy. Lending support to this, several studies indicate that individuals who have experienced previous online privacy invasions express higher levels of online privacy concerns (Zviran, 2008). For example, in the healthcare context, Bansal et al. (2010) found that past privacy breaches significantly increased PHI privacy concerns. From the past empirical findings, the following hypothesis is proposed:

*H6. Previous experience of privacy invasion will be positively related to PHI privacy concerns.*

**Individual Perceptions**

Individuals' perceptions regarding the effectiveness of regulations meant to protect personal information privacy have been shown to reduce privacy concerns in the context of location-based services (Xu et al., 2012), and in the healthcare context (Ermakova et al., 2014). Regulations can give individuals a sense of control over their PHI as they establish the procedures for collection, use, storage and sharing of PHI by healthcare providers and other stakeholders. They also aim to deter non-compliance with these procedures through threat of punishment. They can also empower consumers with the ability to seek redress in case of privacy breaches on their PHI. It is expected that regulations that provide effective and reliable protection against privacy breaches on PHI will reduce individuals' concerns regarding PHI privacy.

*H7. Perceived effectiveness of government regulation will be inversely related to PHI privacy concerns.*

Trust is an important construct often studied in IS privacy research. 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 et al., 2008). With the emergence of IT services, two important targets of trust are suggested for consideration by researchers: the entity providing a service, and the electronic medium through which the service is provided (Tan & Thoen, 2000). In line with this suggestion, in the healthcare context, Dinev et al. (2016) argue that

trust includes both trust in the healthcare institution and trust in the health information system. Following the above recommendations, trust in healthcare providers and trust in e-heath systems are considered in this study.

Following past studies (Anderson & Agarwal, 2011), trust in e-health systems is defined as individuals' beliefs that e-health systems offers a safe and reliable environment to conduct PHI-related transactions including storing, updating, and sharing of PHI. Dinev et al. (2016) found that trust in electronic health record reduces PHI privacy concerns. Similarly, trust in the electronic medium has also been found to influence consumers' PHI disclosure intentions in a context where PHI is exchanged electronically by various healthcare stakeholders (Anderson & Agarwal, 2011). If individuals believe that e-health systems have the necessary components to facilitate the safe and reliable storage, use, and communication of PHI, they are likely to be less concerned about privacy of their digitized PHI. Thus, we hypothesize:

*H8. Trust in e-health systems will be inversely related to PHI privacy concerns.*

Trust in healthcare providers has yet to receive considerable attention in the healthcare context. Following past studies (Doney & Cannon, 1997), trust in healthcare providers reflects individuals' willingness to depend on healthcare providers based on their belief that these providers will be honest and act in the individual's best interest. Kenny and Connolly (2016) found that trust perceptions regarding health professionals reduce health information privacy concerns. When individuals trust that healthcare providers are honest and will act in their best interest they are likely to believe that their disclosed PHI will not be used opportunistically. This is expected to lead to reduced concerns about PHI privacy.

*H9. Trust in healthcare providers will be inversely related to PHI privacy concerns.*

Similar to trust, we examine individuals' risk perceptions regarding e-health systems and healthcare providers. Individuals' risk perceptions regarding e-health systems relate to their perceptions that high probability of PHI privacy loss is associated with the electronic storage, use, and communication of PHI. IT systems are vulnerable to criminal attacks (e.g., hacking) and they also facilitate opportunistic activities (e.g., selling or sharing of PHI) by organizations and their employees. Most privacy breaches on individuals PHI occur through these means (Ponemon Institute, 2016). Studies in other contexts show that risk beliefs regarding technology increase online privacy concerns (Dinev & Hart, 2006). If individuals believe negative outcomes will result from digitizing PHI, they may be more concerned about privacy of their PHI.

*H10. Risk perceptions regarding e-health systems will be positively related to PHI privacy concerns.*

Risk perceptions regarding healthcare providers relate to individuals' beliefs that there will be high probability of PHI privacy loss associated with providing healthcare providers with their PHI. Studies in developing countries show many individuals suffer various forms of abuse by healthcare providers including unauthorized disclosure of their sensitive PHI (Dapaah & Senah, 2016). If individuals suspect privacy of their PHI may be threatened by disclosing it to healthcare providers, they are likely to be more concerned about PHI privacy. Risk beliefs regarding health professionals have been found to increase PHI privacy concerns (Kenny & Connolly, 2016). The following hypothesis is thus proposed:

*H11. Risk perceptions regarding healthcare providers will be positively related to PHI privacy concerns.*

**Moderating Role of Gender and Computer Experience**

The technology adoption literature shows that frequent computer users have higher computer self-efficacy (Compeau & Higgins, 1995). Individuals with higher computer self-efficacy experience less anxieties about using computers (Compeau & Higgins, 1995), and those with lower computer self-efficacy exhibit technology avoidance and anxiety (Dinev & Hart, 2005). The IS privacy literature also shows that computer anxiety is positively related to information privacy concerns (Schwaig et al., 2013). Similarly, a positive correlation is reported between Internet anxiety and individuals' privacy concerns about technology use (Li, 2014).

Based on the above empirical findings, and the discussion on hypothesis H5, we expect individuals with greater computer experience to have fewer concerns about privacy of PHI stored in e-health systems. This is based on the reasoning that individuals with greater computer experience are likely to have higher computer self-efficacy which is expected to decrease their anxieties regarding the electronic storage and use of PHI.

As discussed, a number of recent studies (e.g., ITU, 2016, 2017) indicate that males have greater computer and/or Internet experience than females in developing countries. Since increased computer use leads to higher computer self-efficacy (Compeau & Higgins, 1995), males are expected to have higher computer self-efficacy than females. Some studies have also shown that compared with men, women tend to experience higher anxiety in using computers (Frenkel, 1990). Taken altogether, it is expected that males will express fewer

concerns about privacy of digitized PHI as they are likely to have lower levels of anxiety toward the storage and use of PHI in e-health systems due to their higher computer self-efficacy. Gender is thus expected to moderate the hypothesized relationship between computer experience and PHI privacy concerns in H5.

*H12. The inverse influence of computer experience on PHI privacy concerns will be moderated by gender, such that the effect will be stronger for males.*

Aside from decreased technology anxiety (Compeau et al., 1999), individuals with high computer self-efficacy are also said to be more willing to try out new information technologies (Agarwal et al., 2000). Higher computer self-efficacy thus enables individuals to cope with the uncertainties and risks (including risk to their information) associated with adopting a new technology (Keith et al., 2015). In support of this, in the e-commerce context, consumers with high computer self-efficacy have been found to be less likely to avoid risky online shopping (Milne et al., 2009). Other self-efficacy beliefs have been found to influence trust and risks beliefs in diverse domains. For instance, Keith et al. (2015) found that mobile-computing self-efficacy has a positive influence on users' trust in mobile app venders and negative influence on perceived mobile-app risk. Kim and Kim (2005) also found that online transaction self-efficacy positively influences trust in a web vendor and negatively influences perceived risks regarding websites.

From the observed relationship between self-efficacy, and trust and risk beliefs in other contexts, it is expected that individuals with greater computer experience and hence higher computer self-efficacy will have lower risk perceptions regarding e-health systems and increased trust in these systems. Hence we propose:

*H13a: The inverse influence of trust in e-health systems on PHI privacy concerns will be moderated by computer experience, such that the effect will be stronger for individuals with greater computer experience.*

*H13b: The positive influence of risk perceptions regarding e-health systems on PHI privacy concerns will be moderated by computer experience, such that the effect will be stronger for individuals with less or no computer experience.*

As earlier argued, in developing countries, males are expected to have higher computer self-efficacy than females as males in general use computers and/or the Internet more than females (ITU, 2016, 2017; PRC, 2015). Therefore, from the above discussion regarding the relationship between self-efficacy, trust and risk beliefs, we expect that males will have

greater trust in e-health systems and express lower risk perceptions regarding these systems due to their higher computer self-efficacy. Hence:

*H14a: The inverse influence on trust in e-health systems and PHI privacy concerns will be moderated by gender, such that the effect will be stronger for males.*

*H14b: The positive influence of risk perceptions regarding e-health systems on PHI privacy concerns will be moderated by gender, such that the effect will be stronger for females.*

## RESEARCH METHOD

The proposed model of the study will be tested using empirical data from Ghana. In recent years, healthcare providers in Ghana have introduced various e-health systems to support their operations. Despite the nascence of the e-health field in the country, Ghana is deemed to be one of the few African countries with the necessary infrastructure (including ICT) to implement an integrated e-health solution (International Institute of Communication and Development [IICD], 2014). Ghana thus represents a suitable context for this study.

The survey method is adopted for data collection. The unit of analysis is the individual. Survey participants will include individuals (aged 18 years and older) living in Ghana who have visited (or may have occasion to visit) a healthcare provider for their healthcare needs. To improve diversity of the survey sample in terms of demographic characteristics and participants' perceptions, participants will be recruited so as to ensure a spread across gender, age, and education groups. Toward this end, participants will be drawn from various settings including college campuses, hospitals, business/government organizations, and local neighbourhoods.

Measurement items for the main constructs in the proposed model will be derived from existing validated measures (Dinev & Hart, 2006; Dinev et al., 2016; Hong & Thong, 2013; Smith et al., 1996) and adapted to the context of this study. Examples of the measurement items are provided in Appendix A.

A description of e-health systems will be provided to ensure participants answer the survey with a common understanding of these systems. The questionnaire will be pilot tested to ensure that all survey instructions, the described technological context, and questionnaire items are well understood. Any necessary changes prompted by the pilot study will be made to the questionnaire design before the main survey. The data obtained from the actual survey will be statistically analyzed using the partial least squares structural equation modeling

(PLS-SEM) technique with the purpose of ascertaining the impact of the antecedents of PHI privacy concerns.

## EXPECTED CONTRIBUTIONS

This study is expected to make several contributions to research. A key gap in the current literature lies with limited research examining antecedents of PHI privacy concerns (Kenny & Connolly, 2016). More studies are needed to clarify the nature and direction of the impact of certain antecedents such as health status and education on privacy concerns. There is also the need to extend the boundaries of current research examining the antecedents to PHI privacy concerns beyond developed countries to ensure increased generalizability of this research stream (Belanger & Crossler, 2011; Kenny & Connolly, 2016). By examining a broad range of antecedents in an understudied context of developing countries, this research will contribute to addressing the above gaps in the IS privacy literature. The study also expects to provide insights into whether and to what extent the digital divide and gender digital gap in developing countries contribute to privacy perceptions of individuals in these countries.

Regarding practice, studies show that privacy of individuals' PHI is often overlooked in the development of e-health systems in developing countries (e.g., IICD, 2014; Policy Engagement Network [PEN], 2010). Developers of these systems are said to assume that individuals in developing countries do not care about privacy of their PHI as the risks of abuse of PHI are limited in these countries (PEN, 2010). It is hoped that this study will offer empirical evidence to challenge this assumption, and provide insights to governments and other stakeholders to encourage stringent regulations and policies requiring e-health systems that meet acceptable standards regarding the protection of individuals' PHI.

## APPENDIX A: MEASUREMENT ITEMS

| Construct | Examples of Measurement Items |
|---|---|
| Health Status | In general, how would you rate your overall health? |
| Computer Experience | How many years of experience do you have using computers? |
| Previous Privacy Experience | How frequently have you personally been a victim of what you felt was an invasion of your privacy? |
| Perceived Effectiveness of Government Regulation | I believe the privacy laws in Ghana would effectively govern how my PHI stored in e-health systems is used. |
| Trust in E-health Systems | E-health systems are safe environments in which to store PHI. |
| Trust in Healthcare Providers | Healthcare providers in general would be trustworthy in handling my PHI. |
| Risk Perceptions Regarding E-health Systems | In general, it would be risky to disclose my PHI to healthcare providers. |
| PHI Privacy Concerns: Collection | It bothers me when healthcare providers ask me for my PHI. |
| PHI Privacy Concerns: Secondary Use | When people disclose their PHI to healthcare providers to receive care, the healthcare providers should never use the information for any other purpose. |
| PHI Privacy Concerns: Errors | If healthcare providers store PHI in e-health systems, they should devote more time and effort to verifying the accuracy of the information. |
| PHI Privacy Concerns: Unauthorized Access | If healthcare providers store PHI in e-health systems, they should devote more time and effort to preventing unauthorized access to the information. |

## REFERENCES

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). The evolving relationship between general and specific computer self-efficacy—An empirical assessment. *Information Systems Research*, *11*(4), 418-430.

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.

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.

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

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.

Chen, J., Ping, W., Xu, Y., & Tan, B. C. (2009). Am I afraid of my peers? Understanding the antecedents of information privacy concerns in the online social context. *ICIS 2009 Proceedings*, 174.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS quarterly*, 145-158.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly*, 189-211.

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.

Dickerson, M. D., & Gentry, J. W. (1983). Characteristics of adopters and non-adopters of home computers. *Journal of consumer research, 10*(2), 225-235.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective *Advances in Healthcare Informatics and Analytics* (pp. 19-50): Springer.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

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

Doney, P. M., & Cannon, J. P. (1997). Trust in buyer-seller relationships. *Journal of marketing, 61*, 35-51.

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

Esmaeilzadeh, P. (2018). The Effects of Public Concern for Information Privacy on the Adoption of Health Information Exchanges (HIEs) by Healthcare Entities. *Health communication*, 1-10.

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.

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.

Frenkel, K. A. (1990). Women and computing. *Communications of the ACM*, *33*(11), 34-46.

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

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

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.

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.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information systems journal*, *25*(6), 637-667.

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

Kim, Y. H., & Kim, D. J. (2005). *A study of online transaction self-efficacy, consumer trust, and uncertainty reduction in electronic commerce transaction.* Paper presented at the System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on.

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

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.

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, 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, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *CAIS, 28*, 28.

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

Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce research and applications, 13*(1), 32-44.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer affairs, 43*(3), 449-473.

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., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105-136.

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.

Pew Research Center. (2015). *Internet Seen as Positive Influence on Education but Negative Influence on Morality in Emerging and Developing Nations.* USA: Author.

Policy Engagement Network (PEN). 2010. *Electronic health privacy and security in developing countries and humanitarian operations. Protecting medical information in eHealth projects.* London School of Economics and Political Science, 1-28. London: Author.

Ponemon Institute. 2016. "Sixth Annual Benchmark Study on Privacy and Security of HealthcareData."https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf Retreived 18 August, 2017.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93-114.

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50*(1), 1-12.

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*, 167-196.

Tan, Y.-H., & Thoen, W. (2000). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce, 5*(2), 61-74.

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).

Willyard, C. (2010). Electronic records pose dilemma in developing countries. *Nature Medicine, 16*, 249-249.

World Health Organization. (2016b). *Global Diffusion of eHealth: Making Universal Health Coverage Achievable. Report of the Third Global Survey on eHealth*. Geneva, Switzerland: Author.

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., & Zhang, J. (2008). Predicting user concerns about online privacy in Hong Kong. *CyberPsychology & Behavior, 11*(6), 779-781.

Zviran, M. (2008). User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems, 48*(4), 97-105.