2017

The Digitization of Healthcare: Understanding Personal Health Information Disclosure by Consumers in Developing Countries - An Extended Privacy Calculus Perspective

Ernest Kwadwo 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

The Digitization of Healthcare: Understanding Personal Health Information Disclosure by Consumers in Developing Countries - An Extended Privacy Calculus Perspective

Ernest K. Adu
Department of Accounting and Information Systems
UC School of Business
University of Canterbury, New Zealand
Email: ernest.adu@pg.canterbury.ac.nz

Annette M. Mills
Department of Accounting and Information Systems
UC School of Business
University of Canterbury, New Zealand
Email: annette.mills@canterbury.ac.nz

Nelly Todorova
Department of Accounting and Information Systems
UC School of Business
University of Canterbury, New Zealand
Email: nelly.todorova@canterbury.ac.nz

Abstract

Consumers' willingness to disclose and allow electronic storage of their personal health information (PHI) is critical to the successful digitization of healthcare. However, concern about privacy and potentially negative consequences of privacy loss (e.g., loss of jobs) can discourage PHI disclosure by consumers. It is thus imperative to identify and address key roadblocks from the perspective of consumers that may impede the progress of developing countries in digitizing healthcare. Toward this end, this research-in-progress integrates the privacy calculus model with procedural justice to investigate the willingness of individuals in developing countries to disclose PHI in order to receive care in contexts where the disclosed PHI is stored and used electronically. A comprehensive model is proposed to explain the determinants of consumer PHI privacy concerns and willingness to disclose PHI. We will test the proposed model using the survey method. Several theoretical contributions expected from the study are provided.

Keywords: privacy calculus, privacy concern, healthcare, developing countries, personal health information.

1 Introduction

Developing countries, especially in Sub-Saharan Africa, are plagued by the world's deadliest epidemics including HIV/AIDS and tuberculosis (Akanbi et al. 2012). An efficient record keeping system is required to ensure the continuous treatment and long-term care for patients with these infectious diseases (Ohuabunwa et al. 2016). The need for efficient collection and management of personal health information (PHI[1]), among other factors, has led to broad IT use in the health sector of developing countries (Lewis et al. 2012).

Prior studies conducted in developed countries (e.g., Anderson and Agarwal 2011) show that concerns about PHI privacy have heightened with the digital transformation of healthcare. These concerns stem from factors such as the susceptibility of digital information to criminal attacks (e.g., hacking), and the ease and speed with which custodians of personal information can carry out opportunistic activities. 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. This lends support to the privacy threat posed by digitizing health information.

Concerns about PHI privacy have long existed in the traditional healthcare environment in developing countries, especially in Africa. Several studies (e.g., Dapaah and Senah 2016) show that individuals with heavily stigmatized diseases (e.g., HIV/AIDS) hide their infection and avoid needed care for fear of the negative consequences (e.g., loss of relationships, jobs, etc.) that can result from disclosure of their infection. As developing countries migrate to electronic healthcare (e-health) systems, emerging research shows PHI privacy concern may pose a threat to the success of digitizing healthcare. In a recent study in Ghana, Bedeley and Palvia (2014) found that individuals are concerned about the privacy of PHI with the introduction of computer systems in hospitals. Studies in other developing countries (e.g., Kuo et al. 2014; Willyard 2010) similarly report consumer concerns about privacy regarding the digitization of healthcare.

However, the privacy and security of consumers' PHI remain peripheral in the development of e-health systems in developing countries (PEN 2010). For example, recent studies show that patient information is often not secured well in existing e-health systems in Ghana (Gyamfi 2016; IICD 2014). When the privacy of their disclosed PHI is not assured, consumers will sometimes avoid needed healthcare (PEN 2010; Rindfleisch 1997). Furthermore, when individuals learn they are potentially vulnerable to abuse through weak privacy protection in e-health systems, they may resist digitization of their health information.

At the same time, securing consumers' cooperation and willingness to allow their PHI to be stored in digital form is crucial to the successful digitization of healthcare (Angst and Agarwal 2009). It is thus imperative to identify and understand the factors that both support and hinder consumers' PHI disclosure for electronic storage in developing countries. Prior research addressing this problem has produced findings that may not readily generalize to developing countries' context. For example, much of this research has been conducted almost exclusively in developed countries (Bélanger and Crossler 2011). Most of the studies employ tech-savvy samples as they used online surveys (Kokolakis 2015). However, the majority of individuals in many developing countries have limited or no digital experience compared to those in developed countries. Consequently, their concerns and willingness to disclose PHI in a digital environment may be different from individuals in developed countries.

This study extends the boundaries of extant IS privacy research by examining consumer willingness to disclose PHI in the e-health setting of a developing country, Ghana. The specific e-health setting considered is an electronic health record (EHR) system[2] usage within a hospital[3]. The main question addressed is: *What factors influence consumer willingness to disclose PHI in order to receive care from healthcare providers in developing countries where the disclosed PHI is stored and used electronically?*

[1] PHI includes any type of information that a patient submits to receive care and the information that is generated in the treatment process (Yoo et al. 2013).

[2] An EHR system enables the departments/units in a hospital to record, store, update and share PHI.

[3] Health service providers in Ghana are generally called hospitals. There are 2 major health service providers: public/government hospitals and privately-owned commercial hospitals. These hospitals (both public and private) are gradually introducing EHR systems to support their operations including the electronic storage of PHI. In general, the e-health field in Ghana, like many other developing countries (see Lewis et al. 2012), is relatively nascent. However, Ghana is considered as one of the few African countries with a sufficient ICT infrastructure and consumer identification system to implement an integrated health information systems solution (IICD 2014).

2 Theoretical Foundation

This study adopts the privacy calculus as the overarching theoretical framework. The privacy calculus is a major perspective employed in IS privacy research to explain the privacy paradox (Culnan and Armstrong 1999). The privacy 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. To explain this paradox, the calculus perspective suggests that the privacy disclosure decision results from a cost-benefit analysis in which individuals weigh the risk/cost of personal information disclosure against the benefits to be gained from disclosure. Individuals disclose personal information when the benefits of disclosure exceed or match the risk of disclosure.

The privacy calculus thus consists of an examination of the cumulative influence of contrary beliefs on information disclosure. The contrary beliefs include factors that drive the intention to disclose (i.e. drivers), and those that inhibit privacy disclosure by individuals (i.e. inhibitors). Drivers thus represent the benefit side of the calculus equation, whilst inhibitors represent the cost side.

Privacy risk and privacy concern are key inhibitors while perceived benefits and trust are key drivers that are often studied in the literature. In general, the research based on the privacy calculus has helped our understanding of the need to account for the relative influence of opposing factors in examining intentions regarding privacy disclosure. The following gaps, however, could be identified:

- When evaluating risk, individuals are said to assess the possibility of loss and the potential negative consequences that can result from the loss (Peter and Tarpey 1975). However, risk has been measured in prior privacy research largely in terms of beliefs about the possible loss of data (e.g., Malhotra et al. 2004). Several studies (e.g., Laric et al. 2009) suggest that consumer concerns about privacy and their eventual refusal to disclose health information are also due to the impact that such disclosure will have on their emotions and social and economic interactions. The perceived negative consequences of disclosure are therefore an important factor in an individual's desire to protect the privacy of their health information and hence must be studied closely.
- The core calculus constructs are often not examined together in a single study. Some studies (e.g., Anderson and Agarwal 2011) consider trust and privacy concern to be the major determinants of privacy disclosure and have thus examined the two constructs together. A review of these studies shows that trust more strongly predicts behaviour than privacy concern (Bélanger and Crossler 2011). This indicates that the calculus constructs may have differential impacts on diverse behavioural outcomes and their true relative impacts can only be ascertained when considered together.

This study addresses the above gaps by proposing a comprehensive model which includes all the core calculus constructs and also examines their relevant dimensions. Additionally, the study extends the privacy calculus model by integrating it with procedural justice (a core dimension of justice theory) to study important antecedents of privacy concern and trust which have received limited attention in health information privacy research.

3 Conceptual Model and Hypothesis

Based on the theoretical foundation outlined above, the study proposes a conceptual model which extends the privacy calculus model (see Figure 1), integrating it with concepts in procedural justice. The focus is on *willingness to disclose PHI*. This is defined as an individual's *willingness to disclose their* PHI to hospitals for the purpose of receiving care where the disclosed information is stored and used electronically. The hypothesized relationships between the constructs in the model are discussed below.

3.1 Privacy antecedents

Procedural justice refers to an individual's perceived fairness of the procedures used by a transaction party to arrive at outcomes in an exchange relationship (Martínez-Tur et al. 2006). In the context of IS privacy research, procedural justice refers to individuals' perceived fairness of the procedures employed by firms for the collection and use of their personal information (Xu et al. 2009). Recent IS privacy research (e.g., Culnan and Bies 2003; Xu et al. 2009) indicates that a critical component of consumers' privacy concerns are their fairness judgements regarding how firms handle their information. In this study we consider two factors (namely, perceived privacy policy and perceived effectiveness of government regulation) that can shape consumers' fairness perceptions regarding the information practices of hospitals and assess their impact on consumer trust and concern beliefs.

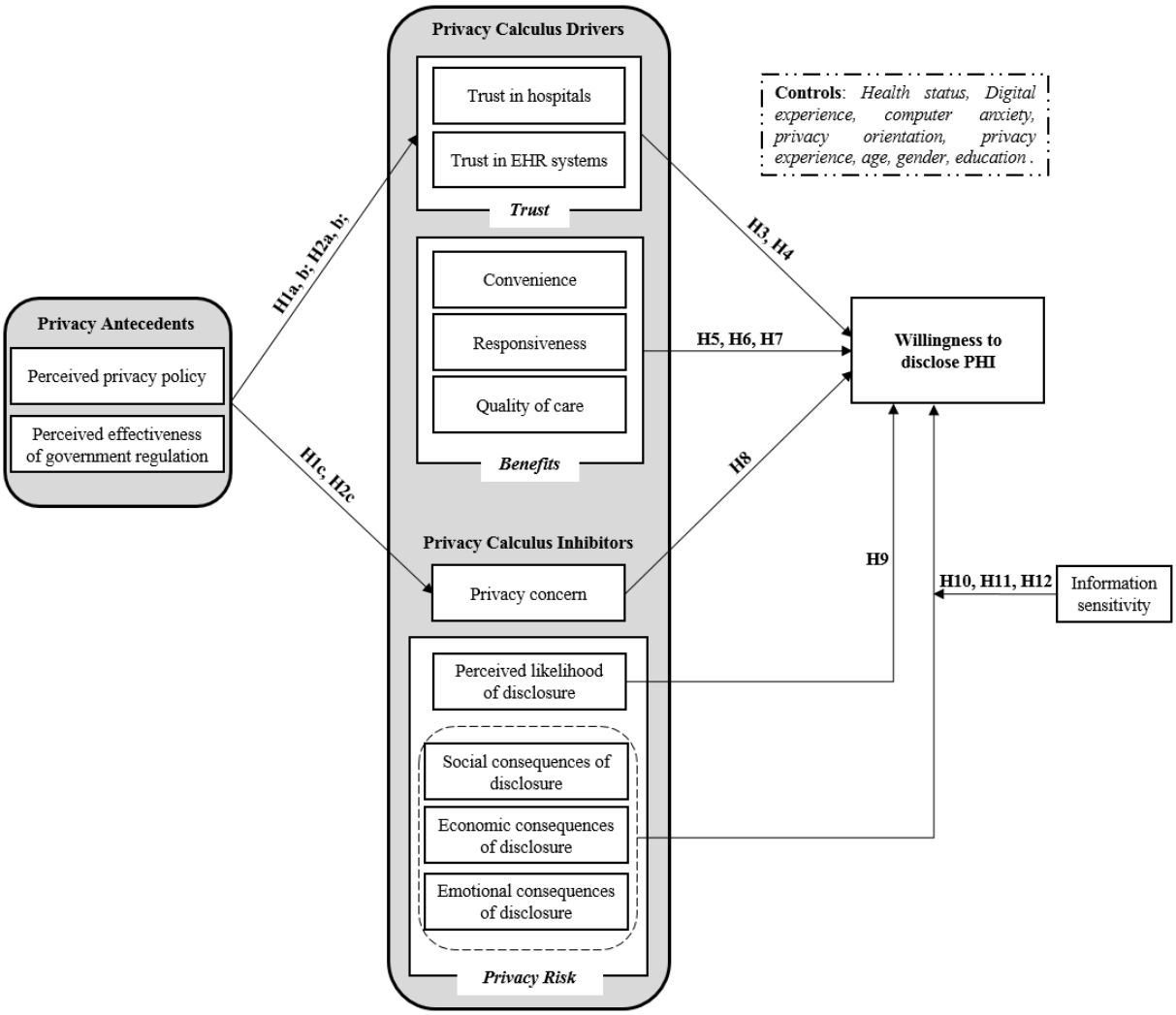

Figure 1: Research Model

3.1.1 Perceived Privacy Policy

Perceived privacy policy refers to consumers' views of the policies and practices of hospitals regarding the handling of their PHI. Consumers expect information obtained about them in the process of receiving care to be kept confidential. To assess whether this expectation is met, they compare the handling of their information to some normative standards of respectful behaviour (Xu et al. 2009). Fair information practices (FIPs) which serves as the global standards for the ethical use of personal information (Culnan and Armstrong 1999) may be used to judge the information practices of hospitals.

When consumers assess the policy and practices of care providers adhere to FIPs, they are likely to consider the information practices of the hospitals as fair. This will likely lead to consumer trust in the hospitals as well as trust in the EHR systems used to manage their health information. On the other hand, consumers are less likely to be concerned about PHI privacy.

H1a, b, c: Perceived privacy policy will be positively related to (a) trust in hospitals and (b) trust in EHR systems, but (c) negatively related to privacy concern.

3.1.2 Perceived effectiveness of government regulation

Perceived effectiveness of government regulation refers to the extent to which individuals believe that government regulations are able to provide effective and reliable protection against privacy breaches on their PHI (Dinev et al. 2016).

Consumers' primary concern relating to privacy is the lack of control over their personal information (Nowak and Phelps 1995). Government regulations which establish the procedures for collection, use, storage and sharing of PHI can give consumers a sense of control over their PHI. They can ensure organizations comply with FIP principles and deter non-compliance through the threat of punishment.

They can also empower consumers with the ability to seek redress in case of privacy breaches on their medical data. These are expected to encourage consumers to believe that firms would conform to FIP principles and would therefore collect and use information appropriately. This will likely alleviate consumer concerns about privacy and increase their trust in hospitals and in the EHR systems they use to store consumer PHI.

H2a, b, c: Perceived effectiveness of government regulation will be positively related to (a) trust in hospitals and (b) trust in EHR systems, but (c) negatively related to privacy concern.

3.2 Privacy Calculus Drivers

3.2.1 Trust

Trust reflects a willingness to assume the risk of disclosure and become vulnerable to the actions of an entity that one trusts (Culnan and Bies 2003). 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 and Thoen 2000). In this study, the two trust targets refer to trust in hospitals, and trust in EHR systems, respectively.

Trust in hospitals refers to an individual's perception regarding the integrity and benevolence of hospitals in protecting the privacy of PHI. Integrity reflects the consumer's belief that healthcare providers will be honest and keep their promises while benevolence refers to the motivation of healthcare providers to act in the best interest of consumers (McKnight et al. 2002). It is argued that 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.

Following past IS privacy research (e.g., Anderson and Agarwal 2011), trust in an EHR system is defined as individuals' beliefs that an EHR system offers a reliable and safe environment in which to store health information. Trust in electronic medium has been found to strongly influence willingness to disclose personal information (Anderson and Agarwal 2011). It is expected that individuals' trust that their digitized health information will be stored safely and reliably will positively influence their PHI disclosure intentions.

H3: Trust in hospitals will be positively related to willingness to disclose PHI.

H4: Trust in EHR systems will be positively related to willingness to disclose PHI.

3.2.2 Benefits

Benefits comprise the value an individual expects to gain from the use of EHR systems by hospitals to support delivery of services. This study includes convenience, responsiveness, and quality of care as the benefit factors derived from use of EHR systems (Krishna 2010; Menachemi and Collum 2011).

Convenience concerns consumers' perceptions of the reduction in time and effort spent in receiving care. EHR systems can enable constant availability of patient's information and the sharing of this information by departments/units within a hospital. This can help reduce the time a patient takes to receive care, lessen documentations, and minimise unnecessary medical tests (Krishna 2010) enabling the patient to expend less effort and time in the process of receiving care.

Responsiveness refers to perceptions of improvement in hospitals' readiness to provide care services to patients. The availability of patient information through EHR systems can enable care providers to respond to patients' needs even in times of emergency. For example, an introduction of EHR systems in some hospitals in Ghana (e.g., Acquah-Swanzy 2015; Gyamfi 2016) has helped prevent loss of patient information and ensured they are readily accessible. This has helped the hospitals to effectively attend to patients including those requiring emergency care.

Quality of care refers to the users' perceptions of hospital care that avoids injuries to patients and waste (e.g. duplication of effort). EHR systems enable access to past medical records which helps physicians in their current diagnoses and treatment of patients (Acquah-Swanzy 2015). This also helps to prevent or reduce repeated medical tests (Niès et al. 2010). EHR systems have also been shown to reduce medical errors. For example, an EHR system in one Ghanaian hospital has helped to prevent wrong dosage prescription based on a patient's age (Acquah-Swanzy 2015).

It is expected that convenience, responsiveness, and quality of care will positively influence consumers' willingness to disclose PHI for storage and use in such systems.

H5: Convenience will be positively related to willingness to disclose PHI.

H6: Responsiveness will be positively related to willingness to disclose PHI.

H7: Quality of care will be positively related to willingness to disclose PHI.

3.3 Privacy Calculus Inhibitors

3.3.1 Privacy Concern

Privacy concern refers to individuals' concerns about what happens to their digitized health information and how this information is used by healthcare providers. These concerns stem from consumers' inability to control how their disclosed information is used and the anxiety that their information could be used without their approval (Yoo et al. 2013).

Several empirical studies (e.g., Anderson and Agarwal 2011; Dinev et al. 2016) show that privacy concern negatively relates to various behavioural outcomes including willingness to provide access to PHI. Following past research findings, we test the following hypothesis.

H8: Privacy concern will be negatively related to willingness to disclose PHI.

3.3.2 Privacy Risk

In contrast to prior research, aside from the conceptualization of privacy risk as beliefs about the possibility of privacy loss (i.e., perceived likelihood of disclosure), the proposed model also considers the consequences of PHI privacy loss which we conceptualize as perceived disclosure consequences.

Perceived likelihood of disclosure reflects beliefs that a high potential for loss is associated with disclosing PHI for use in online environments (Malhotra et al. 2004). Sources of risk as identified in prior research include criminal attacks (Rindfleisch 1997) and opportunistic activities of organizations including unauthorised access to and selling of personal data (Xu et al. 2009). It is expected that individuals who perceive digitized health information as susceptible to risk of privacy loss are likely to be concerned about disclosing PHI for digitization.

H9: Perceived likelihood of disclosure will be negatively related to willingness to disclose PHI.

Perceived disclosure consequences refer to consumers' assessment of the potential adverse consequences of PHI privacy disclosure. People keep certain information private because there is a "fear of the real or imagined repercussions the hidden information would bring with exposure" (Petronio 2002). This is especially true with health information due to its highly sensitive and personal nature, the disclosure of which can have undesirable consequences on the lives of individuals. Reviewing the relevant literature (e.g., Laric et al. 2009), the impact of the social, economic, and emotional consequences of PHI disclosure on willingness to disclose PHI is examined.

The perceived consequences of a given disclosure are closely related to the type of information (i.e., the sensitive nature of the information) to be disclosed (White 2004). Various types of health information are differentially sensitive given the legal protection offered to some health information (e.g., sexual or mental health information) (Anderson and Agarwal 2011). It is thus argued that the influence of the social, economic, and emotional consequences of disclosure on willingness to disclose PHI will vary depending on the sensitivity of the health information.

Perceived social consequences of disclosure reflect beliefs about the potential damage to one's social standing and social relationships that can result from PHI privacy disclosure. 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). Lending support to this, in Ghana and many other African countries, HIV patients are avoided and ill-treated in some cases even by family and friends (Dapaah 2012). Therefore, fearing stigma, discrimination, and resulting isolation, people do not easily, if ever, disclose their diagnosis (Dapaah and Senah 2016).

Perceived economic consequences of disclosure refer to beliefs about the potential impaired economic opportunities (with focus on employment) that can result from PHI privacy disclosure. Evidence suggests companies use medical records of their personnel in employment decision making and any disorders or diseases can impair their employment (Laric et al. 2009). In Ghana, Dapaah (2012) have observed job loss as one of the consequences of contracting HIV/AIDs. To avoid various economic risks, people conceal their health conditions (e.g., pregnant women hiding their condition to stay employed (Laric et al. 2009)).

Perceived emotional consequences of disclosure refer to beliefs about the potential embarrassment or shame that one can suffer from PHI privacy disclosure. People desire to keep certain health information private because their disclosure may cause embarrassment. For example, a survey of Canadian and USA samples found that females were more concerned about the privacy of plastic surgery procedures due to the potential embarrassment if these procedures were publicized (Laric et al. 2009). In another study, White (2004) found that while consumers were more likely to reveal

personal information such as address and phone number, they were more reluctant to reveal embarrassing information including purchase history of condoms.

Following from the above, we expect perceived social, economic, and emotional consequences of PHI disclosure to have a negative effect on willingness to disclose PHI. We further argue that the effect will be greater for more sensitive information than less sensitive information.

> *H10, 11, 12: The negative influence of perceived (11) social, (12) economic, and (13) emotional consequences of disclosure on willingness to disclose will be moderated by information sensitivity, such that the effect will be stronger for more sensitive information.*

4 Research Method

To test the proposed research model, the survey method is adopted for data collection. The unit of analysis is the individual. Measurement items for the constructs in the proposed model will be derived from existing validated measures and adapted for the context of this study. The sample of the study will be drawn from individuals living in Ghana who receive care from the existing hospitals. A diverse sample will be considered such that it reflects the general demographic (in terms of gender, age, and education) of the Ghanaian population (excluding children). Measurement items will seek to capture the perceptions of individuals.

To ensure survey participants answer the questionnaire with a common understanding of an EHR system and how it can be used by hospitals, following prior research (e.g., Anderson and Agarwal 2011; Dinev et al. 2016), a description of an EHR system will be provided on the questionnaire. The preliminary questionnaire will be pilot tested to ensure that all survey instructions, the described technological context, and questionnaire items are well understood.

A scenario-based survey will be used to explore the moderation role of information sensitivity. Two hypothetical health conditions (e.g., Diabetes, HIV/AIDS) will be presented to the survey participants. For each health condition, participants will be asked to imagine they have the condition. Next, on a 1-7 Likert-type scale with an anchor of 1 for "Not at all sensitive" to 7 for "Extremely sensitive", participants will be asked to rate the extent to which they would consider certain information about each health condition as sensitive. Here, sensitive information is defined as information that an individual wants to keep as private. Finally, for each health condition, participants will be asked their opinions regarding the potential social, economic, and emotional consequences to them, should people know they have the condition. For this study we aim to collect over 300 responses[4], and test the model using the partial least square approach to path modelling.

5 Conclusion

This research-in-progress proposes a comprehensive model based on the privacy calculus which examines the determinants of PHI disclosure intentions of individuals in developing countries. The study is expected to make the following contributions to IS privacy research. First, Kokolakis (2015) argues that the diversity of privacy harms have yet to be considered in empirical models used in IS privacy research. This study contributes to addressing this gap by accounting for the negative consequences of privacy disclosure in the consumer's PHI privacy calculus analysis.

Second, adding to the prior research this study investigates a more comprehensive model that will provide a more in-depth and nuanced understanding and insight into the relative importance of the various factors (both drivers and inhibitors) that influence PHI privacy disclosure intentions.

Third, the study responds to the call to increase the generalizability of IS privacy research (Bélanger and Crossler 2011) by extending its boundaries to the understudied context of developing countries. By maintaining the underlying theoretical framework of the privacy calculus, the study will evaluate the model's applicability to explaining privacy behaviour in developing countries.

Fourth, several researchers (e.g., Chiasson and Davidson 2004) have recommended that existing IS research constructs, and theories must be reshaped to deal with the unique setting of healthcare. Following this call, where applicable this study provides context-sensitive versions of the constructs in the proposed research model (e.g., benefits, disclosure consequences) drawing on the healthcare literature. The study thus can provide valuable insights of practical relevance (e.g., guiding

[4] For a reliable survey, the minimum sample size should at least be 10 times as many observations as there are number of constructs in a conceptual model (Kankanhalli et al. 2011).

development of e-health systems that maximizes users' desired benefits). In this regard, the study also responds to the increasing calls for more richness and practical relevance in IS research.

Finally, the study integrates the privacy calculus model with procedural justice and argues that consumer concerns about privacy and their trust beliefs are influenced by their evaluation of how fairly and respectfully they have been treated in an information exchange transaction.

6 Reference

Acquah-Swanzy, M. 2015. "Evaluating Electronic Health Record Systems in Ghana: The Case of Effia Nkwanta Regional Hospital." Norway: The Artic University of Norway.

Akanbi, M.O., Ocheke, A.N., Agaba, P.A., Daniyam, C.A., Agaba, E.I., Okeke, E.N., and Ukoli, C.O. 2012. "Use of Electronic Health Records in Sub-Saharan Africa: Progress and Challenges," *Journal of Medicine in the Tropics* (14:1), p 1.

Anderson, C.L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp 469-490.

Angst, C.M., and 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), pp 339-370.

Bedeley, R., and Palvia, P. 2014. "A Study of the Issues of E-Health Care in Developing Countries: The Case of Ghana," in: *Twentieth Americas Conference on Information Systems*. Savannah.

Bélanger, F., and Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp 1017-1042.

Chiasson, M.W., and Davidson, E. 2004. "Pushing the Contextual Envelope: Developing and Diffusing Is Theory for Health Information Systems Research," *Information and Organization* (14:3), pp 155-188.

Culnan, M.J., and Armstrong, P.K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp 104-115.

Culnan, M.J., and Bies, R.J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp 323-342.

Dapaah, J.M. 2012. *Hiv/Aids Treatment in Two Ghanaian Hospitals: Experiences of Patients, Nurses and Doctors*. African Studies Centre, Leiden.

Dapaah, J.M., and 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), p 41.

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

Gyamfi, A. 2016. "Use of Electronic Medical Records in Emergency Care at Komfo Anokye Teaching Hospital in Kumasi, Ghana." Ghana: Kwame Nkrumah University of Science and Technology.

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

Kankanhalli, A., Lee, O.-K.D., and Lim, K.H. 2011. "Knowledge Reuse through Electronic Repositories: A Study in the Context of Customer Service Support," *Information & Management* (48:2), pp 106-113.

Kokolakis, S. 2015. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers & Security* (64), pp 122-134.

Krishna, S. 2010. "Taking Medical Records into the Digital Age." https://www.ibm.com/developerworks/websphere/library/techarticles/ind-openemr/ Retrieved 18 August, 2017.

Kuo, K.-M., Ma, C.-C., and Alexander, J.W. 2014. "How Do Patients Respond to Violation of Their Information Privacy?," *Health Information Management Journal* (43:2), pp 23-33.

Laric, M.V., Pitta, D.A., and Katsanis, L.P. 2009. "Consumer Concerns for Healthcare Information Privacy: A Comparison of Us and Canadian Perspectives," *Research in Healthcare Financial Management* (12:1), p 93.

Lewis, T., Synowiec, C., Lagomarsino, G., and 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), pp 332-340.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp 336-355.

Martínez-Tur, V., Peiró, J.M., Ramos, J., and 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), pp 100-119.

McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp 334-359.

Menachemi, N., and Collum, T.H. 2011. "Benefits and Drawbacks of Electronic Health Record Systems," *Risk Manag Healthc Policy* (4), pp 47-55.

Niès, J., Colombet, I., Zapletal, E., Gillaizeau, F., Chevalier, P., and Durieux, P. 2010. "Effects of Automated Alerts on Unnecessarily Repeated Serology Tests in a Cardiovascular Surgery Department: A Time Series Analysis," *BMC health services research* (10:1), p 70.

Nowak, G.J., and Phelps, J. 1995. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters," *Journal of Direct Marketing* (9:3), pp 46-60.

Ohuabunwa, E.C., Sun, J., Jubanyik, K.J., and 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), pp 38-43.

Peter, J.P., and Tarpey, L.X. 1975. "A Comparative Analysis of Three Consumer Decision Strategies," *Journal of consumer research* (2:1), pp 29-37.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.

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

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

Rindfleisch, T.C. 1997. "Privacy, Information Technology, and Health Care," *Communications of the ACM* (40:8), pp 92-100.

Tan, Y.-H., and Thoen, W. 2000. "Toward a Generic Model of Trust for Electronic Commerce," *International Journal of Electronic Commerce* (5:2), pp 61-74.

White, T.B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14:1-2), pp 41-51.

Willyard, C. 2010. "Electronic Records Pose Dilemma in Developing Countries," *Nature Medicine* (16), pp 249-249.

Xu, H., Teo, H.-H., Tan, B.C., and 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), pp 135-174.