Abstract

The benefits of digitization of personal health information have been identified in many studies (Anderson and Agarwal 2011; Glaser et al. 2008; Noffsinger and Chin 2000). The studies suggest that such digitization can reduce medical errors and costs, improve patient safety and public health monitoring efficiency, and etc. However, the impact of healthcare privacy breaches on behavioral reactions is not well known although this phenomenon is an important source of healthcare privacy concern. Hence, this study attempts to examine the influence of healthcare privacy breach on health information disclosure, and the moderating role of trust in privacy assurance and perceived disease severity in healthcare privacy invasion context. To achieve these goals, we adopt communication privacy management theory, and privacy calculus. A scenario-based survey method is employed to explore the influence of privacy breaches. Several theoretical contributions and managerial implications are discussed.

Keywords: Privacy concern, privacy calculus, personal health information disclosure, trust in privacy assurance, perceived disease severity
Introduction

The benefits of digitization of personal health information have been identified in many studies (Anderson and Agarwal 2011; Glaser et al. 2008; Noffsinger and Chin 2000). The studies suggest that such digitization can reduce medical errors and costs, improve patient safety and public health monitoring efficiency, and etc. Therefore, various healthcare entities and individual physicians are encouraged to digitize health records, and personal health information is often monitored and managed in digital format by healthcare related organizations such as hospitals (Kush et al. 2008). The amount of personal health information stored in database systems continues increase (Edmonds et al. 2006). Concern regarding digitized health information is becoming significant since improper disclosures of identifiable electronic health information of patients are being reported regularly (Anderson and Agarwal 2011).

However, the impact of healthcare privacy breaches on behavioral reactions is not well known although this phenomenon is an important source of healthcare privacy concern. An individual’s cognitive process and behavioral reaction could be drastically changed if an individual faces healthcare privacy invasion. We suggest that with privacy invasion, privacy concerns regarding digitizing personal health information might increase (Yoo et al. 2012), negative impacts on behavioral reaction may occur (Smith et al. 2011), and protective measures (e.g., privacy assurance) could be emphasized (Krasnova and Veltri 2010). A review of extant literature shows that there is sparse research on the impact of healthcare privacy breaches, as well as healthcare related contextual variables on private information disclosure behavior. For instance, perceived disease severity could take priority over healthcare privacy. Besides, the role of patient's trust in privacy assurance also should be examined in the context of privacy invasion. Trust in privacy assurance can be potentially assumed to offset the negative effect of healthcare privacy breaches.

At this point, we pose two focal research questions: (1) Does awareness of healthcare privacy breaches change the balance of privacy calculus that critically influences personal health information disclosure? (2) Does trust in privacy assurance and perceived disease severity change the influence of healthcare privacy concern on personal health information disclosure? To test these questions, we adopt communication privacy management theory, and privacy calculus. A scenario-based survey method is employed to explore the influence of privacy breaches.

This study has a twofold contribution. First, it extends the boundary turbulence aspect of communication privacy management theory by applying the scenario of healthcare privacy breaches. The study incorporates privacy invasion experience of an individual as a factor that forms privacy boundaries in the healthcare context. It contributes by presenting the cognitive changing process of an individual patient in confronting a privacy invasion incident. Second, privacy calculus in the healthcare context is extended by adopting moderators, (i.e., contextual factors such trust in privacy assurance and perceived disease severity). These factors are not well researched even though they are potentially important in the privacy disclosure decision making process of an individual patient. By adopting these as moderators, this study can illustrate complex mechanisms about how they work on privacy disclosure along with other risks and benefit factors.

The rest of this paper is organized as follows. We begin with the theoretical foundations, reviewing prior work on the privacy boundary, and privacy calculus. This is followed by arguments of the research hypotheses. Methodology is briefly explained. Finally the paper discusses the expected theoretical and practical contributions.

Theoretical Background

Privacy Concern in Healthcare

The tension between organizational use of personal information and a person’s information privacy has been suggested as an important ethical issue of the information age (Mason 1986). Information privacy
refers to the ability to control how an individual’s personal information is acquired and used (Westin 1967). Privacy concern stems from the anxiety that personal information could be used without approval, and have a detrimental impact on individual behaviors in terms of transaction intention, online service adoption intention, and personal information disclosure (George 2004; Pavlou et al. 2007; Van Slyke et al. 2006).

Previous research has accumulated a considerable body of knowledge about privacy concern mechanisms and its effects on transaction intentions, willingness to share personal information, and online service acceptance (Belanger et al. 2002; Chellappa and Sin 2005; Dinev and Hart 2006; Eastlick et al. 2006; George 2004; Lee and Lee 2012; Milberg et al. 1995; Pavlou et al. 2007; Resnick and Montania 2003; Van Slyke et al. 2006; Zhou 2013). These studies show that privacy concern is negatively related to various behavior or behavioral intentions. If an individual has great concern about information privacy, concern leads the individual to have less willingness to act.

Some studies point out that an individual uses information disclosure as a commodity that can be evaluated using cost benefit analyses (Chen and Li 2009; Drennan et al. 2006). When an individual perceives benefits exist more than costs, s/he reveals the personal information. To explain this phenomenon, several approaches have been adopted. For instance, some researchers employ the lens of privacy calculus to explain the nature of consumer privacy concerns (Dinev and Hart 2006; Xu et al. 2010). The privacy calculus approach assumes that a consumer conducts risk-benefit analysis with all the factors relevant to a specific personal information disclosure situation.

In the healthcare context, the role of privacy concern also has been examined. Prior studies pay attention to the negative impact of privacy concerns on electronic health record adoption. Tang et al. (Tang et al. 2006) point out that privacy concerns of individuals is one of main barriers to personal health record adoption. Kam and Chisman (2006) reveal that health information disclosure is influenced by three motivating factors: patient perceptions of privacy, context sensitivity, and the information value of content and feedback. Simon et al. (2009) point out privacy concern is one of the main factors that influence attitudes toward electronic health information exchange.

Privacy calculus is used to illuminate the role of privacy concern regarding individual’s personal health information disclosure decision (Anderson and Agarwal 2011). The study suggests that privacy concerns influence health information disclosure. It also suggests that since different contexts contain different risks, they can moderate the influence of healthcare privacy concern differently on personal health information disclosure. Bansal et al. (2010) focus on the role of personal dispositions (i.e., trust, privacy concern, information sensitivity, which are determined by personal dispositions—personality traits, information sensitivity, health status, prior privacy invasions, risk beliefs, and experience) in disclosing health information online with lab experiment data.

Prior studies have considered privacy concern carefully, but there still remain many issues that need to be researched. For instance, the influence of privacy breaches on patient’s decision making regarding health information disclosure, privacy assurance, and physical conditions have not been studied.

Communication Privacy Management Theory

Communication Privacy Management (CPM) theory explains the mechanism of how the privacy boundary of people is managed and how private information of people is disclosed (Petronio 1991). In CPM, private information is regarded as something that can be owned by people, and should be decided to be shared with a co-owner by an owner (Petronio 2002). CPM theory uses the metaphor of the boundary to illustrate the flow of private information. This boundary determines whether private information could be concealed in the private sphere or if it could be revealed in the public sphere (Petronio et al. 1998). When the boundary is open, private information will be disclosed and vice versa. An individual's private information is safeguarded by the individual’s boundaries. However, based on changes in contexts and relational actors, the permeability of the boundary varies. The boundary can allow certain parts of the public to access certain pieces of information belonging to an individual. The degree of permeability of boundary, regarded as thick or thin boundary, varies according to the rules for access and protection (Petronio 2002).

CPM argues that there exist conflicts whenever a private information owner decides to disclose or conceal
information. It involves a psychological computation process similar to privacy calculus (Dinev and Hart 2006). The benefits of disclosure range from self-expression to relationship development. The risks include loss of face, status, or control (Metzger 2007). Costs (or risk) and benefits are weighed, compared, and calculated using multiple viewpoints at the time the decision must be made, and consideration is taken to determine how private information will be owned, used, and spread (Petronio and Reierson 2009). These considerations call for deeper understanding of healthcare privacy contexts since there exist various unexplored contextual factors that influence risk or benefit perception in information disclosure.

The boundaries help individuals to maximize benefits while minimizing the risks of disclosure of private information. However, according to Petronio (2007), turbulence happens when there is a breach in the coordination of privacy protection or when someone's privacy boundary is interrupted. The best example of turbulence occurs when identity is stolen or private information is divulged by mistake. If digitized personal health information is misused or stolen, victims experience boundary turbulence and will consider health information disclosure seriously. Even though they may have allowed healthcare entities to use their health information previously, after an incident, personal health information disclosure could decline. Boundary turbulence results in mistrust, unwillingness, or uncertainty about sharing and non-disclosure of private information. However, the impact of privacy invasion has not been well examined in the healthcare context.

In summary, we argue that the determinants of private information disclosure decisions are significantly more complex than a simple consideration of privacy concern. Through the CPM lens, boundary turbulence will be explored and extended. For the extension, we adopt different healthcare contexts and privacy breach scenarios. The differences (i.e., before privacy breach and after privacy breach) of individual’s personal health information disclosure intention and other issues would contribute to understanding of unique characteristics of healthcare privacy. Further, as suggested by prior work, the extent that an individual’s perception of risk varies is based on situational factors, such as trust on privacy assurance, and perceived disease severity. These healthcare oriented situational factors will alter the salience of the level of risk and resulting rules applied to the individual's privacy boundaries.

**Hypothesis Development**

Based on the arguments described above, Figure 1 presents a conceptual model of drivers of individual's information disclosure. This model extends previous works on privacy calculus and health information by adopting the privacy breach scenario. We include two moderators that we believe will help explain the context of possible privacy breaches and also two components of benefits. Perceived benefits are theorized by considering patient’s expectation toward health improvement and convenience. For risks, as discussed in previous literature, privacy concern from personal health information disclosure is adopted as the main source of privacy risk in the study because privacy concern has been used as proxy of information privacy (Smith et al. 2011).

This study uses one main dependent variable, personal health information disclosure. Personal health information includes any type of information that is submitted by the patient and that is generated in the treatment processes. Health information could be required in the provision of medical care or be beneficial in facilitating medical research and services (Anderson and Agarwal 2011). Our dependent variable reflects the distinct healthcare situation.

Consistent with previous Internet privacy or consumer privacy studies, it is anticipated that we will find a negative relationship between an individual's privacy concern and privacy risk regarding the digitization of personal health information and the willingness to disclose personal health information in the study (Anderson and Agarwal 2011; Smith et al. 2011; Son and Kim 2008). However, as described in Figure 1, we propose that this phenomenon is more complicated than has been seen in prior explanations and conceptualizations. It is assumed that contextual factors (i.e., perceived disease severity and trust in privacy assurance) interact with privacy risk influenced by privacy concern in the relationship with willingness to disclose health information. That is, these moderators will be tested.
Privacy Concern and Privacy Risk

Privacy calculus is a cost (risk) - benefit framework established on rational based assumptions, which assert that an individual behaves in ways that maximize positive outcomes and minimize negative outcomes (Dinev and Hart 2006). This calculus perspective has been supported with enough evidence in empirical studies of consumer privacy concern (Culnan 1993; Dinev and Hart 2006; Xu et al. 2010). Privacy concern and privacy risk are key factors when an individual tries to weigh and balance the costs and benefits involved in privacy disclosure (Chellappa and Sin 2005; Dinev and Hart 2006; Sheng et al. 2008). Privacy risk, in this sense, is defined as the degree to which an individual believes that a high potential for loss is associated with the disclosure of personal health information (Featherman and Pavlou 2003; Malhotra et al. 2004). Prior privacy literature has identified sources of privacy risk such as organizational opportunistic behaviors, including unauthorized access and selling personal data (Featherman and Pavlou 2003; Xu et al. 2010). Some other researchers also argue that privacy concerns, an individual aspect, enhance the level of perception of privacy risk (Milne and Culnan 2004; Smith et al. 2011; Van Slyke et al. 2006). In the healthcare context, rising privacy concerns about losing control over individual’s personal health information could be expected to have a positive impact on perception of privacy risk. We propose this hypothesis.

H1: Privacy concern has a positive impact on perceived risk.

The Moderating Role of Trust in Privacy Assurance

In online context, prior privacy studies empirically examined the negative effect of perceived privacy risk on willingness to disclose personal information (Cazier et al. 2008; Malhotra et al. 2004; Van Slyke et al. 2006). In CPM theory, it is also argued that perceived risk influences the formation of privacy boundaries (Petronio 2002). Further, boundary turbulence, that is, healthcare privacy breach in this context, makes individuals’ boundaries unstable. In the case of turbulence, an individual’s boundary formation decision is more dependent on outside environment (Petronio 2002; Petronio et al. 1998) and patients’ health
information provision could decline. Contextual factors, such as privacy assurance systems, could help an individual to restore the privacy boundary, balance cost-benefit analysis, and consequently stabilize privacy disclosure. In prior research, the moderating role of trust in privacy assurance in healthcare context has not been tested.

Researchers demonstrate that a well-structured institution or system helps the consumer to have willingness to make transactions (Pavlou and Gefen 2004; Pavlou and Gefen 2005). From the perspective of regarding trust as a facilitator of communication, trust is conceptualized as a direct determinant of information sharing on social network services (Dwyer et al. 2007). Studies in other contexts also suggest that trust is associated with enhancement of evaluation of benefits and privacy related risk (Pavlou 2003). McKnight et al. (2002) point out that positive beliefs regarding the effectiveness of legal structures help consumers to have trust. A assurance framework is effective to protect people against abuse, to relieve privacy concerns, and to enhance information disclosure (Krasnova and Veltri 2010). Considering that the level of privacy protection systems varies from institution to institution, trust in privacy assurance is integrated into our conceptual model. It is appropriate because subjective decision making process on health information disclosure is well associated with subjective perception on privacy assurance systems. Trust in privacy assurance refers to individual confidence that privacy assurance systems of a hospital and government protect one’s health information privacy.

Based on prior literature, it could be assumed that perceived privacy risk and trust in privacy assurance not only have a direct relationship with personal health information disclosure, but also have an interaction effect on personal health information disclosure. Even though privacy risk is perceived by an individual, if there is high trust in privacy assurance, risk could be overridden. In the case of privacy breaches, the moderating role could be enforced, because uncertainty toward future damage is increased. Some studies argue that trust involves actively facing the future by committing to action even though consequences may be partly uncertain and uncontrollable (Giddens 1990; Sztompka 1999).

The behaviors of individuals who have trust in privacy systems or who do not, could be tremendously different, although they perceive similar level of risks. If there is only high risk of privacy breach, or actual privacy related loss happens, it will negatively influence future behavioral reactions. However, if there is trust involved in the situation, the benefit aspect could be emphasized since privacy risk could be solved by privacy assurance systems. Dependent on individual’s trust, attitude toward privacy risk changes. Hence, we suggest these hypotheses.

H2: Trust in privacy assurance moderates the relationship between perceived risks and personal information disclosure.

The Moderating Role of Perceived Disease Severity

From the perspective of information privacy as a commodity, it could be expected that an individual’s health condition could be a critical criterion in determining the value of private information. Prior studies suggest that one important indicator of personal need for health-related information is an individual’s health status (Anderson and Agarwal 2011). When an emotional part of one’s mind is dominant, it can confuse the cognitive evaluation process (Loewenstein 2005). Mental status influenced by health conditions gives disproportionate weights on decisions related to health (Loewenstein et al. 2001). Perceived seriousness of disease has also been studied as a predictor of patients’ adherence to treatment, and it has been proposed that greater disease severity threat would be associated with better adherence (DiMatteo et al. 2007). Other studies argue that an individual with good health conditions comprehends and evaluates information about risks and side-effects better than others (Schaeffer et al. 1996).

In this study, we define perceived disease severity as a belief that an individual has on her/his health status. It ranges from severe to not severe. As previous research identifies, an individual’s health condition influences the evaluation process regarding health information disclosure. The direct relationship has been examined in the context of health status emotion (Anderson and Agarwal 2011), but its moderating role regarding the relationship between privacy risk and information disclosure has not been investigated. Further, in terms of the communication privacy management perspective, perceived disease severity could also offset boundary turbulence, which may in turn result in information disclosure. Hence, we suggest that when an individual perceives high disease severity, risk could be evaluated in a different way according to health status even though privacy breach may happen to the same victim group.
Therefore:

H3: Perceived disease severity moderates the relationship between privacy risk and personal information disclosure.

Benefits

In this study, we include convenience, and health improvement as benefit factors derived from digitized health information. The advantages of using digitized health information has been well addressed in literature (Anderson and Agarwal 2011; Angst and Agarwal 2009). The studies suggest that it can reduce medical errors and costs, improve patient safety and public health monitoring efficiency (Anderson and Agarwal 2011; Glaser et al. 2008; Noffsinger and Chin 2000). From a patient’s perspective, patient can expect the reduced waiting time, less documentations in hospital and pharmacy, and etc (Krishna 2010; Manos 2010). The convenience derived from digitized health records could be maximized in many cases such as when a patient goes to several different departments with necessary documents in a large hospital, when the repeated expensive medical test can be avoided in meeting different physicians, and etc (Goldman 2009). Digitization of health records can potentially reduce patients’ unnecessary efforts and wasted time spent with processing documents. In this study, convenience is defined as patient’s perception on convenience that can be made by using digitized health records. Since this variable conceptualizes the patient’s perception, it is influenced by individual’s previous experience of using other digitized records management systems, indirect experience of others (e.g., family, friends, and etc.), or expectations from having relevant knowledge or reading articles. For example, if a patient have good knowledge on the advantages and conveniences of using digitized health records, s/he is likely to have willingness to disclose personal health information. Therefore, it can be generally hypothesized that when a patient perceives there is a high likelihood in using digitized health records by disclosing personal health information, s/he can have high intention to disclose personal health information. Health improvement refers to a patient’s perception on health improvement that can be achieved by using certain medical service with digitized health record. Health improvement can be regarded as a patient’s main purpose of looking for healthcare service providers. Normally healthcare providers utilizing digitized health records provide their service only to patients who disclose their personal health information. Hence, a belief that a patient can receive good treatments and achieve the health wise goal is significantly associated with perceived benefits of personal health information disclosure. Based upon these arguments, it is assumed that these two factors can positively influence an individual to provide personal health information. The study posits these hypotheses.

H4: Perceived convenience has a positive impact on personal health information disclosure.

H5: Health improvement has a positive impact on personal health information disclosure.

Methodology

Most of measurement items for the study’s main constructs are derived from existing measures (Dinev and Hart 2006; Krasnova and Veltri 2010; Pavlou and Gefen 2004; Xu et al. 2010), but they are adapted and adjusted for the unique healthcare setting of this study. The unit of analysis of this paper is an individual patient. Adopted theories, variables, and measurement items are targeting the individual’s perception. The main context is a hospital because a patient receives the services from hospital units, and personal information and privacy assurance are managed in hospital level in Korea. This study will be conducted in Korea. The term “hospital” is used in the measurement items. In Korea, “hospital” is the term that encompasses various healthcare service providers such as a big hospital, a small unit in the hospital, a physician, and a clinic. It is the most common term indicating those entities. Hence, adopting this term in a measurement item is appropriate and also enables us to investigate the patient’s general perception on focal variables.

This study embraces the impact of privacy governance systems of hospital as well as government regulation in measuring trust in privacy assurance. It is very likely that patient will think not only about privacy governance systems of hospital, but government regulations when a patient hears about privacy
breach in the hospital. Even though hospital is the context of this study, government regulations could be regarded as an important facilitator to privacy governance system of hospital by patients. So considering both factors seems appropriate in our research framework.

After measurement item development, items are translated into a Korean version of the survey. Since there are language-oriented differences such as nuance and interpretation, close attention is given to the translation. The preliminary instrument will be first pilot tested for comprehensiveness and clarity of meanings in Korea. Following these pretests, the measurement instrument will be shortened, refined, and validated for its statistical properties.

For exploring the boundary turbulence, scenario based survey is adopted. First respondents will be asked their opinions in regular conditions (i.e., without privacy breach), and subsequently be required to answer the questions in the context of privacy breaches. The differences between two scenarios will be compared in the overall model. We shall target patients, who have received medical services in the recent past, in certain hospitals in South Korea as the main respondent group. The respondents will be asked to answer all questions based on their experience along with a given scenario, using a 1–5 Likert-type scale with an anchor of 1 for “strongly disagree” to 5 for “strongly agree,” and 1 for “not severe” to 5 “very severe” for perceived disease severity measure. We expect over 300 responses will be collected.

<table>
<thead>
<tr>
<th>Table 1. Measurement Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convenience</strong></td>
</tr>
<tr>
<td>Personal health information (PHI) disclosure could make me save time in hospital process.</td>
</tr>
<tr>
<td>PHI disclosure in the hospital allows me to put less effort in hospital process (e.g., check-in, check-out, prescription, repeated medical tests, and etc.).</td>
</tr>
<tr>
<td>PHI disclosure helps me to have treatments in the hospital conveniently.</td>
</tr>
<tr>
<td><strong>Health Improvement</strong></td>
</tr>
<tr>
<td>Having treatments in the hospital helps my body to function normally.</td>
</tr>
<tr>
<td>Having treatments in the hospital helps me to feel less pain.</td>
</tr>
<tr>
<td>Having treatments in the hospital helps me to have improved health.</td>
</tr>
<tr>
<td><strong>Privacy Concern</strong></td>
</tr>
<tr>
<td>I am concerned about potential loss, such as medical insurance rejection, PHI leakage and etc. caused by privacy invasion.</td>
</tr>
<tr>
<td>Compared with other subjects on my mind, personal privacy information such as my health status and PHI is very important.</td>
</tr>
<tr>
<td>Compared to others (e.g., friends, relatives and colleagues), I am more sensitive about the way hospitals handle my PHI.</td>
</tr>
<tr>
<td><strong>Trust in privacy Assurance</strong></td>
</tr>
<tr>
<td>I feel confident that existing privacy governance of the hospital protects me against abuse of my PHI in the hospital.</td>
</tr>
<tr>
<td>Existing privacy governance of the hospital adequately protects my PHI in the hospital.</td>
</tr>
<tr>
<td>The existing privacy governance of the hospital is good enough to make me feel comfortable disclosing PHI in the hospital.</td>
</tr>
<tr>
<td>I feel confident that existing privacy laws protect me against abuse of my PHI in the hospital.</td>
</tr>
<tr>
<td>Existing privacy laws adequately protect my PHI in the hospital.</td>
</tr>
</tbody>
</table>
The existing legal framework is good enough to make me feel comfortable disclosing PHI in the hospital.

Providing the hospital with my PHI would involve many unexpected problems.

It would be risky to disclose my PHI to the hospital.

There would be high potential for loss in disclosing my PHI to the hospital.

I am willing to provide my PHI, such as identifiable information, credit card information and etc, to hospital to received appropriate treatments.

I have a high willingness to consent to hospital’s request for using my PHI.

I do not feel uncomfortable in disclosing my PHI to the hospital.

Please evaluate the severity of disease that you received treatments for.

*Personal health information (PHI) is used in hospital information systems such as patient registration, prescription, physician’s patient management, and etc.

**Discussion**

There are two expected main contributions in the study. First, this study extends CPM theory involving boundary turbulence by adopting the scenario of healthcare privacy breaches. Results can demonstrate the impact of privacy invasion experience of an individual in forming privacy boundaries in healthcare contexts. Even though prior studies have studied the relationship between privacy concerns and prior privacy invasion (Awad and Krishnan 2006; Culnan 1993; Yoo et al. 2012), the results of this study will provide a more comprehensive view regarding the impact of boundary turbulence on health information disclosure, privacy calculus, and recommendation behavior.

Second, privacy calculus in the healthcare context is extended in this paper by adopting moderators. Contextual factors (i.e., trust in privacy assurance and perceived disease severity) are considered in the conceptual model. The influence of trust on privacy concerns and privacy calculus has been explored and tested by researchers (Belanger et al. 2002; George 2004; Van Slyke et al. 2006). This study will contribute to this body of literature by revealing the moderating role of trust in privacy assurance. Further, perceived disease severity, as a healthcare related factor, gives richer understanding of privacy in the healthcare context.

**Acknowledgement**

The authors would like to thank the track chairs, AE and referees for their detailed feedback regarding this paper. This research is funded in part by NSF under Grants 0916612, 1227353, and 1241709, The research of the last author is also supported by the World Class University program funded by the Ministry of Education, Science, and Technology through the National Research Foundation of Korea (R31-20002) and by the Sogang University Research Grant of 2011.

**References**


