An Examination of Risk Perceptions and Protected Health Information Disclosure Intentions: A Construal Level Theory Perspective

Emergent Research Forum (ERF)

Tripti Singh  
University of Alabama  
tsingh3@crimson.ua.edu

Allen C. Johnston  
University of Alabama  
ajohnston@cba.ua.edu

Paul M. Di Gangi  
University of Alabama at Birmingham  
pdigangi@uab.edu

Gregory J. Bott  
University of Alabama  
gjborgt@cba.ua.edu

Abstract

As the healthcare industry becomes increasingly digitalized, the promise of increased quality patient care must be weighed against the negative consequences of data breaches that include protected health information (PHI). In this paper, we develop a research model by integrating construal level theory as an antecedent to privacy calculus, operationalized as perceived privacy risk and perceived benefits, and privacy concern to explain PHI disclosure intention. We plan to test this model using scenario-based factorial survey. In doing so, we provide guidance to healthcare organizations seeking to alleviate privacy concern that may inhibit disclosure of PHI necessary for ensuring quality patient care.

Keywords

construal level theory, privacy calculus, data breach, protected health information

Introduction

Electronic health records (EHRs) and health information exchanges (HIEs) promise an array of benefits to individuals including improved clinical care and reduced healthcare cost. EHRs store data in a digital file designed to be shared across networks while HIEs enable the exchange of information across organizational boundaries. Unfortunately, adoption of these technologies carries risks to the confidentiality, integrity, and availability of PHI (Harman et al. 2012). According to the Department of Health and Human Services, over 5.1 million records containing PHI were exposed by data breaches in 2017.¹ Such breaches increase the likelihood of financial and medical identity theft along with psychological and social harm to individuals.

When privacy risks and concerns are high, individuals may choose to engage in non-disclosure as a protection mechanism (Agaku et al. 2014). Patients weigh the risks of non-disclosure against its impact on the quality of care received impacting their health. In information systems (IS) discipline, this risk-benefit analysis is addressed via privacy calculus (Dinev and Hart 2006). However, research has yet to explore whether existing findings generalize to settings in which individuals evaluate the costs of unauthorized PHI disclosure against its health benefits (e.g., correct diagnosis and adequate medical care). Therefore, this study seeks to understand:

RQ1: How does an individual's perceptions of risk and concern for PHI privacy influence his/her PHI disclosure intentions?

¹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Privacy risk and concerns are complex in terms of how they are formulated. Prior research has suggested that security threats that are more immediate, proximal, and probable elicit greater concern among those threatened and lead to more immediate and substantial responses. However, the IS literature has yet to fully explain how these psychological processes interact and influence PHI privacy risk perceptions. Therefore, this study also seeks to understand:

**RQ2: How does the psychological distance of healthcare data breaches influence how an individual forms perception of risk and concern for the privacy of his/her PHI?**

This study integrates privacy calculus with construal level theory (CLT), incorporating the psychological distance of data breaches as part of the privacy cost calculus that individuals undertake when deciding to disclose their PHI. This paper is organized as follows. We begin with a review of privacy calculus and CLT further presenting the research model, hypotheses, preliminary research methodology and expected contributions.

**Theoretical Background and Research Hypotheses**

Information privacy is defined as the “ability to control information about oneself” (Bélanger and Crossler 2011, p.1027). When an individual’s privacy is violated, the individual can not control his/her interactions with the social and physical environment. From a healthcare perspective, privacy is a key governing principle of the patient–physician relationship, where complete information disclosure is required by patients to facilitate correct diagnoses and treatments and to avoid adverse drug interactions.

**Privacy calculus for information disclosure**

Privacy calculus views privacy-related decision-making as a rational process where an individual’s disclosure intentions are the result of an assessment of the perceived risk and benefits related to disclosure (Anderson and Agarwal 2011; Dinev and Hart 2006). When perceived benefits are equal or greater than the risks, individuals ignore privacy concerns (Dinev and Hart 2006). In the healthcare context, privacy calculus explains individual’s intent to disclose PHI and has been extended by incorporating situational factors in the PHI disclosure decision, such as: 1) type of health information requested, 2) purpose information will be used, and 3) by entity requesting information (Anderson and Agarwal 2011).

In prior research, risk has been based on our immediate experience; however, situations beyond our immediate experience also influence our risk perception. To understand how privacy risk influences privacy calculus, we examined the extant research on privacy calculus and showed that individuals translate objects, events, and threats, at different levels based on their ability to conceive them as near or distant from their immediate reality. Trope and Liberman (2010) described this translation as the function of psychological distance and construal levels.

**Construal Level Theory of psychological distance**

According to Trope and Liberman (2010), CLT explains the extent of deviation from direct experience that changes peoples’ response to events. CLT presents these experiences in terms of psychological distance and construal levels. Psychological distance is a multi-dimensional construct, involving different aspects of 1) social, 2) temporal, 3) spatial, and 4) hypothetical distance. Psychologically distant events are presented in terms of high-level mental construals characterized as abstract, coherent, decontextualized, and superordinate features while psychologically proximal events are presented as low-level construals having concrete, contextual and incidental details of the events. In combination with privacy calculus, CLT explains how abstract and psychologically distant privacy perceptions are trivialized over more tangible and psychologically proximal healthcare benefits.

CLT postulates ability of human mind to represent events at different levels (i.e., low vs high) based on one’s immediate reality. We propose that different levels of psychological distance from data breaches will influence privacy concern and perceived privacy risks. Figure 1 depicts research model for explaining individual PHI disclosure intentions based on their perceptions of privacy concern due to data breaches. Perceived high social distance between self and another person creates positivity effects such that individuals perceive themselves as less prone to negative event. Familiar events are perceived closer than
unfamiliar events. A physically distant retail store creates higher social distance and reluctance to purchase online, while owner’s name and appearance on website creates social proximity that improves purchase intentions (Darke et al. 2016). Thus,

**H1a:** The social distance of a breach is negatively related to an individual’s privacy concern.  
**H2a:** The social distance of a breach is negatively related to an individual’s perceived privacy risk.

![Research Model](image)

**Figure 1. Research model**

Research on temporal distance has found that past and future events are represented in abstract form compared to events happening in the immediate environment (Trope and Liberman 2010). Individuals prefer near future rather than distant future rewards and focus on contextualized and concrete details to prevent the losses in near future events. When temporal distance is higher, individuals pay more attention to the central features or desirability for pursuing positive outcomes. Thus,

**H1b:** The temporal distance of a breach is negatively related to an individual’s privacy concern.  
**H2b:** The temporal distance of a breach is negatively related to an individual’s perceived privacy risk.

The spatial distance shows that distant events are construed more abstractly than the near events. In online business, consumers feel safer buying from psychologically closer businesses (Darke et al. 2016). Hence, data breach in a different geographical location (other city or healthcare provider in same city), will be perceived as psychologically distant and construed at a higher level. Hence,

**H1c:** The spatial distance of a breach is negatively related to an individual’s privacy concern.  
**H2c:** The spatial distance of a breach is negatively related to an individual’s perceived privacy risk.

Hypothetical distance refers to the perception of how realistic an event’s occurrence is in terms of probability (Trope and Liberman 2010). Therefore, if an individual perceives that there is less likelihood of a healthcare data breach and invasion of PHI, the risk will be abstract, psychologically distant and result in low perceived privacy risk and concern. Thus,

**H1d:** The hypothetical distance of a breach is negatively related to an individual’s privacy concern.  
**H2d:** The hypothetical distance of a breach is negatively related to an individual’s perceived privacy risk.

In this study, we define privacy concern as the concern relating to loss of PHI resulting from disclosure due to a data breach. Medical needs are critical to survival, and people with special needs are more
interested in receiving treatment than in health information privacy protection. Individuals with disabilities and chronic illness have lower privacy concern compared with counterparts with no such conditions. Agaku et al. (2014) notes, individuals’ privacy and data breach concerns are higher when PHI is exchanged and shared electronically and individuals are less intent to share information when they have little information about how their health information is being used. Individuals whose providers use EHR are more likely to withhold information due to privacy concern. Therefore,

**H3: Privacy concern negatively relates to intent to disclose information (PHI).**

The extant privacy literature mentions privacy risk as the degree to which an individual believes that a high potential for loss is associated with the release of personal information. We define perceived privacy risk as the expectation of loss associated with disclosure of PHI in healthcare data breach and position it as an antecedent of privacy concern (Xu et al. 2011). Accordingly, we hypothesize that:

**H4: Perceived privacy risk positively relates to privacy concern.**

The extant privacy literature suggests that an individual’s risk perception is higher for health and financial information. Information sensitivity informs the degree of perceived discomfort when disclosing information to an external agent. All things being equal, individual risk perceptions are higher for disclosing more sensitive information (Dinev et al. 2013). Hence,

**H5: Perceived privacy risk negatively relates to intent to disclose information (PHI).**

Privacy calculus assesses the potential benefit against the likelihood and perceived severity of negative consequences from disclosure (Xu et al. 2011). PHI disclosure allows physicians to 1) avoid patient readmission, 2) improve diagnose accuracy, 3) avoid medication errors, and 4) decrease duplicate testing (Anderson and Agarwal 2011). EHRs have shown to increase consultation times with physician, reduce redundancies in medical questioning, and improve information sharing with providers. Thus,

**H6: Perceived benefits of PHI disclosure negatively relates to perceived privacy risk.**

**H7: Perceived benefits of PHI disclosure positively relates to intent to disclose PHI.**

**Methodology**

We propose to use the scenario-based factorial survey approach as mentioned by Johnston, Warkentin, McBride, & Carter, (2016). A form of vignette design, the factorial survey approach will allow us to immerse participants in the context of PHI disclosure decisions and assess their perceptions relative to the experiences of the primary actor(s) in the vignettes. By considering the vignettes from the position of the primary actors(s), the participants of this study are not reporting their personal decisions, which might interject socially desirability bias or acquiescence bias into the study. Rather, the participants are reporting how they might respond if presented with the circumstances faced by the primary actor(s) in the vignettes.

The participants will be a random sample of former or current healthcare patients in the U.S. These participants will be presented with an online survey containing a random selection of five vignettes from a universe of 128 possible vignettes in which the variables expressed in our research model are manipulated within the wording and structure of the vignettes (Taylor 2006). Each vignette will describe some version of a situation in which a patient, Joe, is made aware of a healthcare data breach involving his PHI and must contemplate the privacy risks stemming from the breach and the decision of whether or not to disclose his PHI in light of this news. After reading each of five randomly selected vignettes, we will ask the participants to respond to a survey, including a manipulation check, a realism check, and an estimate of the likelihood they would duplicate Joe’s PHI disclosure decision. We will then use a

---

2 This number is based on having the seven intendent variables in research model represented at two levels, high and low.
generalized form of the standard linear model to conduct an estimation of our research model based on the data received from the factorial survey.

Conclusion

This study proposes a privacy calculus and CLT-based model to determine PHI disclosure intentions. In doing so, we contribute to privacy research by examining how psychological distance influences an individual's cost-benefit analysis for PHI disclosure. Kokolakis (2017) argued empirical models should take into account the diversity of privacy harms, diversity of personal information and privacy concerns. This study contributes to this call by addressing 1) the negative consequences of PHI disclosure based on the risk of data breach and 2) antecedents of the privacy calculus based on CLT.

References


