Understanding the Drivers and Outcomes of Healthcare Organizational Privacy Responses

Completed Research Paper

Rachida Parks
Pennsylvania State University
University Park, PA, USA
rfp127@ist.psu.edu

Chao-Hsien Chu
Pennsylvania State University
University Park, PA, USA
chu@ist.psu.edu

Heng Xu
Pennsylvania State University
University Park, PA, USA
hxu@ist.psu.edu

Lascelles Adams
Bethune-Cookman University
Daytona Beach, FL, USA
adamsl@cookman.edu

Abstract

This research adopts a grounded theory approach to examine the drivers, safeguards and operational outcomes of organizational information privacy responses in the healthcare context. Semi-structured interviews with key healthcare stakeholders were conducted. The findings are sobering. First, privacy safeguards are driven by legal compliance, competitive advantages, available resources and best practices. However, organizations have to balance conflicting risks associated with these drivers. Second, this study identifies the operational and behavioral outcomes which results in major balance issues. Third, the adoption of a privacy impact assessment (PIA) allows the integration of a risk management approach to effectively assess the different types of privacy risks. The findings provide evidence for: (1) a gap between privacy responses and their outcomes on healthcare practice and delivery; (2) the importance of the privacy impact assessment as a risk management tool; and (3) the challenging context of the healthcare environment of how privacy responses are unfolding.

Keywords: Healthcare IT, Organizational Information Privacy Responses, Electronic Health Records (EHRs), Grounded Theory, Privacy Impact Assessment (PIA)

Introduction

With the integration of electronic health records (EHRs) into healthcare organizations, information privacy issues and threats have drawn considerable attention from researchers and practitioners. Privacy breaches associated with these threats continue to make headlines in the media (Hodgkinson et al. 2010). These breaches may have dire consequences on the organization's reputation, monetary fines, along with potential civil and criminal liabilities (Culnan et al. 2009). As a result, organizations are now exceedingly focusing on developing privacy programs and safeguards to mitigate these privacy threats. However, the evidence indicates that these initiatives are failing since "breaches continue to occur, suggesting that existing compliance programs are not effective" (Culnan et al. 2009, p.678).

Previous studies examined information privacy concerns primarily at the individual level of analysis (Angst et al. 2009; Chen et al. 2009; Son et al. 2008; Xu et al. 2008). Furthermore, several research studies investigated information privacy by focusing on specific contexts, such as e-commerce (Cranor et al. 2007; Van Slyke et al. 2006), and online social networks (Bulgurcu et al. 2010b; Chen et al. 2009). While these studies provided rich perspectives into the information privacy literature, we still know little about how organizations handle these information privacy threats. Thus, understanding the theoretical explanations and the outcomes of organizational information privacy remains a major issue (Appari et al. 2010; Culnan et al. 2009; Greenaway et al. 2005; Smith et al. 2011). To date, no comprehensive framework has been developed to empirically explore the different theoretical explanations as well as to identify the outcomes while assessing the privacy impacts associated with each step.

This study aims to address this gap and contribute to information privacy literature by focusing on the context of healthcare and explaining the drivers, responses, and outcomes of how healthcare organizations respond to privacy threats. This research facilitates the interactions among the major drivers influencing healthcare organizational privacy responses and discusses the impact of these responses on practice while integrating a privacy impact assessment model. From a theoretical perspective, this study offers the most comprehensive framework that integrates the context of healthcare to organizational privacy responses. From a practical perspective, it provides insights on how practitioners develop their own privacy impact assessment models given external pressures, available resources and impact on practice.

Literature Review

The notion of privacy issues and threats varies depending on several factors such as industry sectors, regulatory laws and cultures (Malhotra et al. 2004; Milberg et al. 1995; Xu et al. 2008). In the United States, privacy laws are sectoral with industry specific regulatory rules (Culnan et al. 2009). Thus, information privacy as a concept holds different definitions or expectations across industries. Consequently, privacy issues and threats will be better understood when they are bounded by a specific context (e.g., healthcare industry) (Bansal et al. 2008; Johns 2006). Therefore, in this literature review section, we will integrate research studies from both the IS and the health informatics communities in order to gain in-depth and context specific insights about information privacy in the healthcare context.

Our interdisciplinary literature review revealed three major themes with regards to the factors explaining organizational responses regarding privacy issues and threats: institutional pressures (Agrawal et al. 2007; Greenaway et al. 2005; Neubauer et al. 2011), competitive advantage (Greenaway et al. 2005; Smith 2000); and moral and ethical considerations (Culnan et al. 2009; Kluge 2007; Mohan et al. 2004).

Institutional Pressures: Research on Institutional theory has generated extensive insights on how organizations respond to external pressures (Oliver 1991). Institutional theory posits that organizations respond to institutional pressures and adopt behavioral and structural changes in order to achieve legitimacy and conformity (DiMaggio et al. 1983; Meyer et al. 1977). Institutional pressures can be imposed by the state, interest groups, and the general public (Oliver 1991). Healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH) define the federal regulatory requirements for handling patients' protected health information (PHI). Healthcare organizations must adhere to these regulations (Appari et al. 2010; Neubauer et al. 2011). Institutional theory has received significant attention from IS and organizational researchers (Goodstein 1994; Mignerat et al. 2009; Orlikowski et al. 2001; Teo et al.

2003). Thus, the theory seems to offer an appropriate lens to examine the regulatory effects on organizational information privacy responses.

Competitive Advantage: In a conceptual paper, Greenaway et al (2005) argued about the lack of theories to be used in investigating information privacy at the organizational level. The authors also argued that the Institutional Theory, with its social approach is not sufficient to explain organizational behaviors. Integrating it with an economic approach, the Resource Based View (RBV) theory provided much richer insights into organizational information privacy. RBV posits that organizations possess resources that can be a source of sustained competitive advantage (Barney 1986; Rumelt 1984; Wernerfelt 1984).

Ethical Responsibility: Organizations recognize the importance of moral responsibility and ethical considerations in their practices (Culnan et al. 2009; Mohan et al. 2004). Organizations that recognize moral and ethical responsibilities will gain more buy-in from their employees and customers. Using two privacy breach case studies, Culnan at al. (2009) offered a set of best practices to help organizations transcend their reactive approach to a more proactive one. These best practices include fostering a culture of privacy, governance processes and avoiding decoupling. These ethics translates into having best business practices that accounts for fair information practices (FIPs). FIPs are a set of global standards, which were originally developed by the US Department of Health, Education and Welfare (HEW 1973). In the context of information privacy, FIPs serve as guidance to organizations about responsible privacy behaviors (Smith 1993).

Integrating the Three Theoretical Perspectives: The need for generating a new theory rises when significant gaps in the literature on organizational privacy responses and their outcomes are considered together. Existing organizational research has used a limited repertoire of theories to explicate how organizations respond to privacy issues and threats (Greenaway et al. 2005). Greenaway considered the Institutional and Resource Based View theories to account for social external forces as well as sustainable competitive advantage. Prior organizational research on privacy has also considered moral responsibility into how organizations respond to privacy threats (Culnan et al. 2009). Each theory points to a need to understand the processes by which organizational privacy responses unfold. Yet, absent from the literature is how organizations assess the dynamics of these theories taken together. This paper argues for a risk assessment of these theories and how the implementation of privacy responses is impacting healthcare delivery practices, thus the notion of privacy impact assessment (PIA). Previous studies had defined PIA as a risk management tool used to assess the use of privacy safeguards (Culnan et al. 2009). PIA uses the fair information practices to assess any impact on patients' privacy. The US Department of Homeland Security defines PIA as a decision-making tool used to identify and mitigate privacy risks at the beginning and throughout the development life cycle of a program (DHS 2010). In accordance with the guidelines of the e-Government act of 2002, the Department of Health and Human Services (HHS) started promoting PIA as a mechanism of assessing that patient information is adequately protected (HHS 2011b). While the proposed PIA serves the interest of different health agencies (e.g. Food and Drug administration, Center for Disease Control and Prevention), we argue that they can also serve the interest of healthcare organizations such as hospitals. Thus, it is essential to assess the privacy risks of different drivers under which organizational privacy responses might be impacted. It is also essential to assess the privacy risks associated with the practical impact. We believe that a better understanding of how to assess these privacy risks will further enhance the theoretical understanding of privacy in healthcare and the impact of healthcare practices.

Once a privacy impact assessment has been conducted, a variety of privacy responses are implemented to reduce the impact of a given risk. Previous studies focused more on the safeguards themselves rather than a privacy approach that takes into consideration the drivers as well as the outcomes. These safeguards fall into a technical (Aberdeen et al. 2010; Chiang et al. 2003; Kluge 2007; Ohno-Machado et al. 2004; Quantin et al. 2000; Tsai et al. 2011), and a human equation (D'Arcy et al. 2009; Fernando et al. 2009; Herath et al. 2009; Ishikawa 2000; Straub et al. 1990; Yeh et al. 2007). Thus, we argue that the existing frameworks are not cohesive enough (Smith et al. 2011) to explain how and why organizations are responding to privacy issues and threats.

We believe a better understanding of organizational responses, their drivers and their operational impact would allow us to develop a better information privacy operational model where privacy impact

assessment can be an integrative part of the model. Therefore, this paper aims to (1) explore the safeguards developed by healthcare organizations with regards to healthcare privacy threats stemming from the use of e-health technologies such as EHRs; (2) understand the major drivers influencing these privacy responses in healthcare; (3) identify the outcomes of these responses on healthcare practice and delivery; and (4) identify the privacy impact assessment variables to be assessed.

Research Method

To achieve our research objectives, we adopted a grounded theory methodology that accounts for and uncovers organizational activities and behaviors with regards to healthcare information (Strauss and Corbin, 2008). Grounded theory approach is becoming increasingly common in the IS research literature because the method is extremely useful in developing context-based descriptions and explanations of the phenomenon (Orlikowski 1993). This methodology also enables us to "produce theoretical accounts which are understandable to those in the area studied and which are useful in giving them a superior understanding of the nature of their own situation" (Turner 1983, p. 348). Further, this particular form of qualitative approach has its origin in healthcare settings (Glaser and Strauss, 1967) and, thus well suited for understanding responses to information privacy issues within healthcare organizations.

Research Context

The context for our study is the healthcare industry; we have selected this industry because of its uniqueness. We focused on hospitals using electronic health records. Hospitals are categorized by ownership (for profit, not for profit), by bed size (small, medium and large), by location (rural, urban, suburban), and by activities (community, research, critical care). Although our original objective was to interview several informants equally across different categories, we were faced with the challenges associated with the sensitivity of our research questions about information privacy. Challenges that were already commented on in previous research (Kotulic et al. 2004). Our target participants included key leaders and managers who are directly involved in the decision-making concerning privacy and/or security within their organization.

Data Collection

In this study, we gathered data through semi-structured interviews with consenting key informants with expert knowledge in privacy and holding key positions in healthcare organizations such as: Chief Information Officer (CIO), Chief Privacy Officer (CPO), Chief Medical Information Officer (CMIO), Chief Executive Officer (CEO), and HIPAA privacy compliance officers (Table 1). We used a "snowball" technique (Lincoln et al. 1985) to identify more informants as well as through the first author's affiliation with the university center of integrated healthcare delivery system.

A total of 17 informants were interviewed (16 interviews) and three workshops/round tables were attended. The interviews addressed three major questions: (1) the privacy threats the organization is facing, (2) the countermeasures undertaken; and (3) the drivers behind these responses. Further elaborations were obtained during the interviews based on the informants' position(s) and background (e.g. an informant with a computer science background had a different perspective than an informant with a medical or a law background). Interviews lasted between 35 and 90 minutes, the workshops lasted eight and eleven hours, and the round table lasted one hour. The first interviews were conducted mainly face to face (seven out of 10) at the informants' location. Due to sensitivity of the subject of privacy that translate into data breaches for practitioners, a face–to–face approach created a more personal approach and kept the interviews deeply grounded in their contextual settings (Schultze et al. 2010). Therefore only informants located within a 200 mile radius from the authors' location were considered for a face-to-face interview. Subsequent interviews expanded to other geographic locations across the United States to include in no particular order, the states of Florida, Pennsylvania, Illinois, Ohio, California, and Connecticut as well as Washington, D.C. Although our original objective was to interview more than 17 informants, we were faced with the difficulty of getting participants because of the critical sensitivity of privacy and security topics (Kotulic and Clark, 2004), as well as the scheduling challenges of healthcare executives.

Table 1. Data Sources						
#	**Informants Position(Background)**	**Organization Type**	**Size**	**Location**	**#Beds**	**Teaching Hospital**
1	CMIO (Medical)	Hospital	Medium	Suburban	484	Yes
2	CIO (IT)	Hospital	Medium	Rural	207	No
3	CPO	Hospital	Medium	Rural	207	No
4	CMIO (Medical)	Hospital	Large	Suburban	818	Yes
5	Ex-President (HPA)	Healthcare Association	-	-	-	-
6	CPO (Law)	Government	-	-	-	-
7	Security Officer (IT)	Hospital	Medium	Suburban	250	No
8	CPO (Law)	Hospital	Large	Urban	4200	Yes
9	CPO(Law)/Security Officer (IT)	Hospital	Medium	Rural	228	No
10	VP Implementations (HPA)	EHRs Solutions	-	-	-	-
11	CEO (IT)	Hospital	Small	Rural	25	No
12	Privacy Officer (Law)	Large Hospital	Large	Urban	4200	Yes
13	IS Director (IT)	Hospital	Medium	Suburban	204	No
14	Security officer (Engineering)	Hospital	Medium	Urban	1267	Yes
15	Privacy Officer (Health Management)	Hospital	Medium	Suburban	275	No
16	CPO (Law)	Global Research Firm/Consulting	-	-	-	-
Workshops and Round Tables						
1	Consultant/Faculty/ Government	Privacy & Security workshop	-	-	-	-
2	Consultants, Lawyers, CIOs, CPOs	Privacy Round table	-	-	-	-
3	Faculty, EHRs Developers, Hospital Administrators	Healthcare Workshop	-	-	-	-

According to Martin and Turner (1986), grounded theory suggests that there should be a continuous interplay between data collection and analysis. Though not by design, informants from entities other than hospitals were interviewed. Our preliminary data collection targeted only hospitals; however through this interplay, we revisited our target to include healthcare government entities, healthcare professional associations, EHRs solution providers, and healthcare privacy consultants that were recommended as important stakeholders by earlier informants. Interviews were conducted between Fall 2010 and Spring 2011. All interviews were audio-recorded and transcribed. Based on informants' recommendations, the first author attended a week-long healthcare IT conference with an attendance close to 31,000 representing healthcare government entities, academia, consultants and developers. The first authors attended several education sessions as well as a privacy and security workshop and a round table.

The study included all common positions held by healthcare privacy experts. These positions were recommended by healthcare professionals. We listed these informants based on their associations with hospitals, government entities, consultants or vendors. Despite several interactions with the workshops

and the round table attendees, we did not include them in our interviews' count. Attendees included healthcare IT consultants, faculty researchers, EHRs vendors, and hospital administrators. The second workshop was used as a confirmation and validation of our findings.

Data collected consisted of (1) audio recordings of 16 interviews; (2) notes taken during the interviews, privacy workshops and round tables; and (3) documentation provided by informants and/or downloaded from their websites.

Grounded Theory Analysis Process

In this section, for the purpose of clarity, we provide a brief overview of the tasks undertaken using the grounded theory approach:

1) Data Collection and Transcription: We audio recorded the interviews with each informant. We then transcribed them into word text documents.

2) Data Analysis using NVivo: Each transcribed interview was imported to a computer aided qualitative data analysis software tool called Vvivo (v.9). Transcripts were then coded. This involved taking pieces of raw data and using codes to describe events, and characteristics. These codes were initially as close to the data as possible. We used an inductive approach, which does not use a predefined set of codes, but rather identifies 'in vivo' codes that arise from the data. For the first order analysis, we embraced an open coding approach in order to brainstorm and open up the data to all potentials and possibilities.

3) Second Order Analysis: Using our first order analysis results from the step above, there was the emergence of certain categories but not all relationships were defined. Strauss and Corbin (2008) refer to this step as axial coding, which is the act of relating concepts and categories to each other and constructing a second order model at a higher theoretical level of abstraction. This step involved an iterative process of collapsing our first order codes into theoretically distinct themes (Eisenhardt 1989). We first grouped the safeguards to mitigate privacy issues into technical, human, physical safeguards and organizational processes. We labeled these safeguards healthcare organizational privacy responses (OPRs). The drivers influencing theses responses were grouped into external pressures and internal context. The external environment included pressures exercised by healthcare regulations and competitive advantage while the internal context included resources and best practices. Finally, the operational and behavioral outcomes formed the overall OPRs outcomes.

4) Literature Review: We have thoroughly reviewed the literature from both the IS and health informatics communities to identify potential contributions of our findings to the privacy literature in the healthcare context. Our review consisted of information privacy related work with a special focus on existing theories and frameworks at the organizational level. We integrated the context of healthcare by reviewing health informatics research. Upon this review of the strengths and weaknesses of the existing literature, we decided to: (1) focus on the drivers influencing OPRs and assess the privacy impact associated with each in order to strengthen the lack of theories explaining how organizations handles privacy responses (Greenaway et al. 2005); and (2) break out of the box of drivers and responses (Hodgkinson et al. 2010) to include the outcomes of privacy responses that were not part of our original research questions though captured through the data collected. Capturing the outcomes allows a better integration of a privacy impact assessment into our model.

5) Theoretical Framework: Our final stage of the analysis consisted of determining how the various themes we have identified could be linked into a coherent framework explaining organizational privacy responses, their drivers and their impact on healthcare practices.

Ensuring Trustworthiness and Validity

To ensure that our analysis met Lincoln and Guba's (1985) four criteria for trustworthiness: credibility, transferability, dependability, and confirmability, we employed the following steps: (1) we used multiple methods and different sources to ensure triangulation of our findings such as single interviews, group interviews, round tables and workshops across different sources such as hospitals, government entities, consultants and IT designers; (2) the first author has a long term industry experience in healthcare IT and

attended a week long Healthcare IT conference with several sessions on privacy and security; and (3) the first author generated a "thick description" or detailed first order analysis that was reviewed by all authors, which provides enough background to the readers to generalize the findings (Van Maanen 1979).

More evaluative criteria for interpretive IS research were used (Klein et al. 1999; Walsham et al. 1999) to include triangulation, member checking and authenticity. Triangulation was achieved by supplementing workshops, round tables and documentations to the interviews' data. Member checking was achieved by inviting informants to provide feedback on the interpretation of the data. Finally, authenticity was achieved through an annual workshop organized by a multidisciplinary center that involved leaders from healthcare industry, healthcare IT solution providers and faculties. Preliminary findings of this study were shared to get critical feedback about constructs and relationships. Consensus suggests a reasonable degree of validity of the findings and constructs.

Findings

In this section, we present our findings by interweaving both first order codes along with second order themes to provide an overarching structure of our grounded theory approach through a thick description from our data (Kreiner et al. 2006). These themes serve as a foundation for our grounded theoretical model for organizational privacy responses presented in Figure 1.

Privacy Response Drivers

Our data analysis revealed a categorization of drivers, based on internal and external considerations, that impact how privacy responses might be developed. These drivers include regulations, competitive advantage, resources and best practices. The analysis also unveiled the adoption of PIA by healthcare organization, in order to assess the privacy impact associated with each driver.

> *"Everyone is constantly in the back of their minds measuring risk all the time. So, I think that's why you always do what the law says. That's a risk that's not worth taking. But then you have to look at other kinds of risks too for what you may do or may not do and what is the risk of reputational harm or financial harm or all those other kinds of things, how that comes into play."*

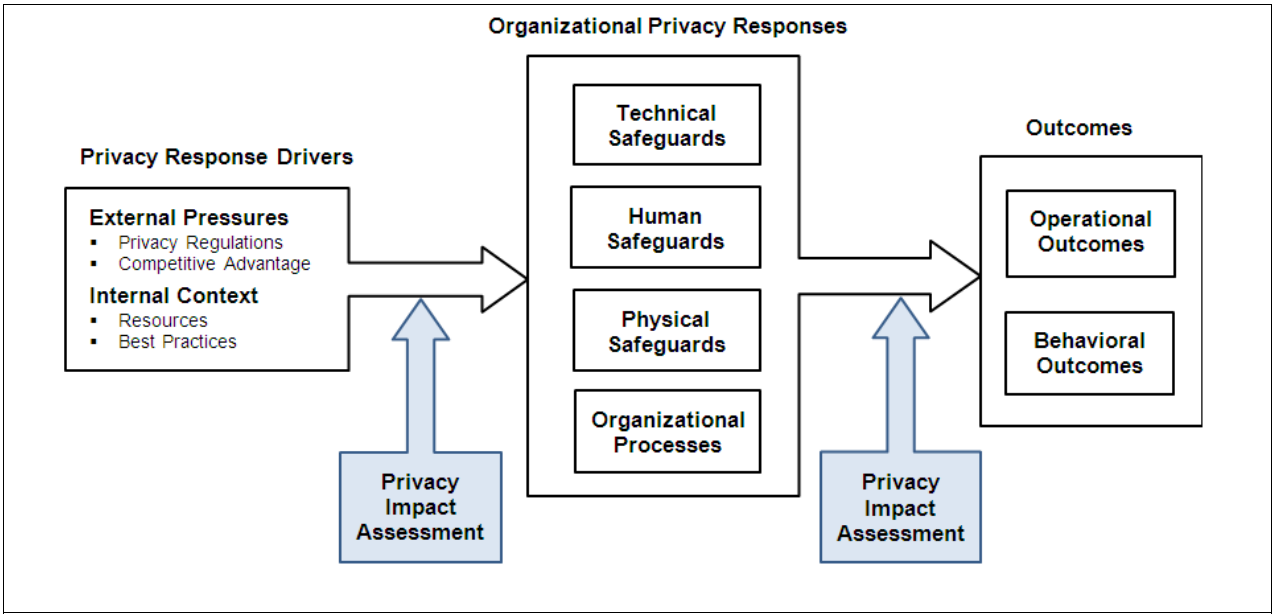

Figure 1. Data Structure

External Pressures refer to the pressures exercised by entities other than a healthcare organization itself. These entities can represent the government and its regulations but can also represent other hospitals that are competing for the same patients.

Healthcare Regulations: Our analysis revealed that federal (e.g. HIPAA and HITECH) and state regulations are amongst the most cited drivers into why organizations are responding to privacy issues and threats. Organizations are abiding by the law because they have to. With the latest healthcare federal regulations (e.g. HITECH), the threats of higher penalties and imprisonment are forcing organizations to make efforts to comply with the law and develop the appropriate privacy safeguards.

> *"There are hefty fines and penalties out there for organizations. You can be fined up to 1.5 million dollars by the federal government if you have an egregious breach."*

With regards to healthcare regulations, we have identified two PIA elements that should be accounted for when developing privacy responses: (1) the risks associated with following the law and negatively impacting healthcare processes creating a tension between the law and practices; and (2) risks associated with the fines and penalties for not abiding by the regulations.

> *"I would much rather happen to explain to the office of civil rights why some body inappropriately accessed information than explain to a family why their loved one is dead and they wouldn't have been dead had information we had in our possession wasn't accessible to the people treating that patient."*

Competitive Advantage: Protecting patients' information from external and internal unauthorized access and other threats is considered a competitive advantage. Healthcare organizations, not only have to report their breaches to the US Department of Health and Human Services, which maintains a website of privacy breaches by organizations (HHS 2011a), but also publish in a news media following a breach of 500 or more patients. This negative exposure impacts their market share and, thus as a part of their PIA, organizations have to account for (1) the risk of loss of reputation when inappropriate or no safeguards are taken and (2) the impact on patients' trustworthiness.

> *"When they go to a hospital they expect that that hospital can be trusted with both their money, their data and their body. I think the difference though is healthcare for some individuals anyway, is such a personal kind of thing, maybe more so than the amount of money in their bank account."*

Internal Context refers to the internal factors associated with a particular organization. Our data analysis revealed several internal factors impacting how healthcare organizations are going by their privacy responses such as their payer mix (e.g. Medicaid, Medicare, Blue Cross Blue Shield), hospital size, IT infrastructure. However, due to their low frequency, we focused on resources and best practices with much higher frequencies.

Resources: The availability of human and capital resources impact how much organizations can invest into their privacy responses. From hiring the appropriate workforce, to buying and maintaining technical solutions, the amount of resources to handle these initiatives is not insignificant. Most of the time organizations have to make a call between what is primarily needed for healthcare delivery and what is needed to respond to privacy issues.

> *"It's actually very expensive to do, and if you think about it, a work force of 60,000 people, let's just say on average, it takes half hour to complete the training that's 30,000 man hours, let's put a labor rate of $50 an hour, it's a $1,500,000 just in lost labor time. I understand that we need to do it, but it is cost. There is a lot of training that we do in this organization, and you have to balance all of that against what the disruption is going to be on services."*

PIA at this level, primarily consist of assessing the privacy impacts associated with investing in privacy responses versus investing in direct healthcare delivery expenses such as hiring a surgeon or purchasing imaging equipments.

> *"Do you add another level of security that may make a difference or do you hire another surgeon and add another operating room? Those are real capital decisions that get made every year and you have to do your best based upon the information that you have to make those decisions."*

Best Practice is a very hard term to define and capture but frequently used implicitly or explicitly by our informants. In some organizations, it even takes precedence over regulations, because it sets higher standards than simply meeting the regulatory requirements.

> *"It is not like we did not care about information before, now all of the sudden the legislation makes you compliant with this, that is a poor assumption. So we clearly value patients, health information security at the highest level … eight years ago, before HITECH, even before HIPAA stuff, all those considerations of who need to see what information, where is it secured, where are the displays for the screens, things like that, were all inherent to what we are doing."*

> *"I believe that most organizations now are much more aware of privacy and security than they were before that law came into place. And just seeing this as just a good business practice instead of something we have to do, make all the difference in the world. They may call it; I have heard some of the techy people call it hygienic environment or something like that you know."*

Within best practices, we identified the following PIA elements: (1) high performance through a culture of being the best, and (2) proactive attitudes by embedding privacy in the organizational culture.

> *"You know that's one of the things that characterizes really high performance organizations, I think when you do develop that culture of we are the best, and if we are not a lot better by next year, we are going to be down the toilet kind of feeling."*

Organizational Privacy Responses (OPRs)

With the goal of developing a taxonomy of organizational privacy responses, we sought to document the variations in responses to privacy issues, in the complex and challenging environment of healthcare. We therefore asked a broad question about privacy safeguards being used. We found evidence of four major OPRs types to mitigate privacy issues in healthcare: technical safeguards, human safeguards, physical safeguards and organizational processes.

> *"We would identify something internally where we had a risk. We would address that whether it is a technological fix, or education or process fix."*

> *"What I try to do is listen to both the clinicians and physicians, and patients and through my exposure on the national committees that I have been on, to listen and try to understand what the perspectives are and try to develop systems that, in processes and policies, are reasonable based upon our needs to access information as well as to allow our patients to feel comfortable that their information is being protected."*

Technical Safeguards: Healthcare organizations are developing a wide range of technical safeguards to handle the threats of accessing patients' data from unauthorized users. Though the frequency of technical measures was the highest, the details around it were not always very granular. This was either due to the fact that technical safeguards were handled by a different department than the informant's or the background of the privacy officer (i.e. law, medical) did not allow him/her to provide thorough details of their technical safeguards. The purpose of this study was not mainly focused on technical safeguards, so while they were given their fair share during the interviews, no further questions were pushed by the researcher.

> *"The electronic security of it is a whole another ball game in regards to firewalls and remote access to the information, redundancy of that information, who has the sign in security to see pieces of information."*

> *"You have put things in place technically to make sure that privacy is maintained."*

Our findings revealed three major types of technical safeguards: Access control, encryption and audit controls. With access being a major privacy issue, it was obvious that a lot of technology efforts were centered on this area, especially role based access and monitoring its use.

> *"Well we do have role based security, but if we decided that you should have rights to getting at certain class of data, we can give it you, and then we have a logging system that will log and consolidate all that logging information."*

Despite their already high commitments to technology to mitigate their privacy issues, informants were still looking for more technological capabilities to handle data monitoring and audits.

> *"I think, even though we have incredibly sophisticated log tools, I would love to see better analytics, associated with log ins to catch more people that are doing things wrong because our alerting, you know we would not necessarily know if you are my next door neighbor. I would love to have some analytics that says something John Doe and Mary Smith have the same street address, and their numbers are separated by four digits, maybe I should look at this. The analytics side is something I would really like to try do; I think that would be really powerful."*

Human Safeguards: Experts clearly distinguish technical versus human safeguards. In this section, we categorized the findings into education which includes training and awareness efforts; disciplinary actions; creating privacy positions; and creating a culture of privacy.

Education, training and awareness programs are receiving high attention from healthcare organization leaders. However these educational efforts are faced with a couple of challenges related to the cost and the amount of information retained by employees.

> *"On the human side, there will probably be more discussions. You know what, you can't discuss it enough and educate enough so there will probably be some more education."*

> *"Your typical employee is going to retain three or four or maybe five concepts at most. People have done studies about what people retain. So what we try to do is, we periodically do articles in our employee new letter, just to let people know what's going on."*

Disciplinary actions, including termination from employment, were undertaken when employees failed to follow the privacy guidelines and principles outlined in their education, training and awareness programs.

> *"We have actually terminated people for accessing family you know, particularly say if there is a messy relationship and one spouse complains and it is found to be true."*

Another interesting aspect of abiding by the law is hiring privacy personnel or more exactly appointing existing personnel to a position of privacy officer. The workload of these new assignments takes about 25% of their time, and up to 100% during investigations. Across organizations, these assignments were quite intriguing as the backgrounds of the privacy officers were completely disparate, from clinicians, to lawyers, to managers of medical records, and CIOs.

> *"We have privacy officers, part of their day job, you know they, none of our privacy officers are officers full time meaning they have other jobs."*

Finally, cultivating a culture of privacy starts with a support from the organization's top executives and survives through the employees' buy-in.

> *"Culture can make or break a privacy officer. It absolutely can. If you've got support at the very top from your CEO, that makes your job a whole lot easier because people will pay attention. If you have others promoting you and your program, that helps a lot. If your company hired a chief privacy office just because they had to because HIPAA said we did or just because they want to pretend like they care, but they don't really care, you're not going to be successful. Ultimately you're just going to continue to beat your head against a wall and you won't get the resources that you need, your budget won't be what you need it to be, you won't have the staffing, and it's you know you're standing in quick sand hoping for the best and then it's not working."*

Physical Safeguards: These measures receive the least amount of attention as far as frequency. However, they seem to represent an important safeguard, the lack of which can be an open invitation for potential breaches. Physical measures included simple tools such as one-way glass or simply asking for a physical badge before allowing access to an area.

> *"We do rounding to look at the computers to see if a screen is visible. We have put in nurse stations, one way glass in certain area so the public cannot walk by and look in and see a computer, we've taken steps like that."*

Organizational Processes: This section includes (1) policies based on healthcare regulations such as training policies, investigation policies, treatment policies and (2) processes to handle particular tasks that impact PHI privacy.

> *"Privacy of health information is a priority and we have policies and procedures and infrastructure that support that approach to patient information."*

> *"Our whole current administration process, first of all making sure that those people who need access to the system they requested, they are audited, and we can know who they are, process in place when someone leaves, whether it is a termination, transfer to whatever, we have a process in place that we make sure that they get out to the system and no longer have access."*

Operational and Behavioral Outcomes

Our findings identify two groups of outcomes: Operational and behavioral. Operational outcomes are defined as disruptions of workflows, impact on information availability, and balance challenges of actual privacy practices. Behavioral outcomes are identified through a deterrence approach, compliance monitoring, and lobbying. These outcomes led to including PIA at the outcome level of our model.

Operational Outcomes

The impact of OPRs brings out a balance issue that is of high concern to healthcare leaders. This balance involves a tension between ensuring the privacy of patients' information and the operational convenience. One informant stated that in some situations, his organization would rather face audits from and explanations to the office of civil rights than having to justify to a dead patient's family that he/she could have been saved if role based access was defined differently. We identified the following PIA elements to be accounted by healthcare organizations:

1) Availability of information in order to provide adequate care

> *"The fact of the matters a lot of difficulties goes back to this idea of access; we can't overly restrict access, because when you do so, what you end up doing in getting in the way of delivering care. So how do you allow people access knowing that the biggest exposure will probably remain to be people looking at information they shouldn't when they have right to getting that information. I think that is a huge challenge."*

2) Disruptions of existing workflow processes that create a push back from users

> *"There is a lot of training that we do in this organization, and you have to balance all of that against what the disruption is going to be on services."*

> *"There is a constant push for people coming in to want to vary the type of smart phones they can access information and that is the sort of conflict."*

3) Balance challenges and operational feasibility

> *"It's a balance, you need to have role based access, but you've gotta be careful about being too prescriptive in terms of limits. You gotta error on the side of more access, understanding that people very well may you know, look at something that they shouldn't be, but hopefully you catch it on the back end by log in and monitoring."*

Behavioral Outcomes

We have identified three behavioral outcomes with regards to healthcare OPRs. To our surprise, a great deal of focus was on a deterrence approach to create an environment of *fear* when rules are not followed. The goal was to set an example and deter other employees from inappropriately handling patients' information:

> *"It is sort of user grisly analogy. Back in medieval England when they chop people's heads off, they would put the head on a pike, and they stick it on the London bridge, and the idea was that it would allow you to see who had their head chopped off. It was a very public hanging. And so, it's the same thing here, we can't necessarily say who we fire, but you hope the word gets out,*

> *you hope the employee that gets fired almost says, I can't believe they fired me for looking at that. Well okay fine, I want you to tell your co workers, because I want your coworkers to say, I am not going to do this again because I don't want to have the same thing happen to me, or I don't want to be suspended."*

In addition to a deterrence approach, organizations embrace a compliance monitoring behavior to determine how their privacy program is doing. Compliance monitoring is assessed by considering the number of complaints received and through audits.

> *"We monitor our complaints, we monitor any time we have a violation. So we actually have a log in system whereby we make sure all privacy officers log in any type of event that might be privacy related. That is one measure but that is also hard to say. How do you measure compliance? I mean we go through and we do audits, our auditors come in and check for complaint."*

Not having a set of guidelines is weighing heavily on organizations who are trying to be compliant and even much heavier on the ones that want to be proactive.

> *"There were going to be audits that were going to be performed by HHS and they were going to be random audits. Nobody has ever come back out and I have asked on numerous occasions I will like to see the audit plan, what would an auditor if they came into our office what will they be looking for. The reason I ask for that is that I, as an organization will like to take that audit plan and I will like to do my own audit, based upon the audit criteria that that auditor will be using, so that I can see if I have any gaps."*

Finally, lobbying was undertaken by organizations to handle those legal requirements that were hard to implement. In these instances, assistance by healthcare professional associations, laws firms or their state representative was sought.

> *"We can also help legislate, because we have lobbyists. Some of the legislation we may like, or may not like, or may want to have happen"*

Within the behavioral outcomes, we identified the following PIA variables that include an assessment of the deterrence effect, the compliance monitoring processes, and finally the behaviors toward external regulatory entities through lobbying.

Discussion

A major contribution of this study is the emergence of the privacy impact assessment concept and explication of its role in helping healthcare organizations assess the drivers and the outcomes of their privacy responses. How organizations assess the impact of regulations, loss of reputation or the use of best practices, appear to be critical to understanding and developing the appropriate organizational privacy responses. PIA allows organizations to assess the dynamics between different drivers, and identify the impact of OPRs on practices. Another contribution of this study is the emergence of our grounded model on organizational privacy responses, which allows us to lay a foundation for future research by proposing research questions and propositions.

The Privacy Impact Assessment Concept

Our findings provide evidence that the issues surrounding the appropriate OPRs and their impact on practice was of a high priority to healthcare privacy leaders. The concept of privacy impact assessment emerged as a key when assessing the impact of privacy both at the drivers and the outcome levels of OPRs.

We consider the concept of PIA as both simple and profound. Assessing each driver (institutional, competitive and best practices), while simultaneously accounting for the dynamics of how complying with one driver may impact another driver or outcome, constitute a strong conceptual foundation for organizational privacy responses.

The emergence of the privacy impact assessment concept prompts us to question whether this concept is simply an extension of security risk management. PIA is different. First the concepts of information

privacy and information security hold different meanings. Security has been associated with a technical connotation while technology is just a subset of privacy as suggested by Ackerman (2004) "security mechanisms provide some privacy capabilities. It must be noted that security is necessary but not sufficient for privacy" (p.432). Security risk management was traditionally a technology driven approach using different computing technology assets to handle known threats (Gerber et al. 2005), however current research have embraced a more business driven approach to account for employees' awareness, participation and behaviors (Bulgurcu et al. 2010a; Siponen et al. 2010; Spears et al. 2010). PIA is different in that it serves as an assessment bridge between OPRs, their drivers and their outcomes. As such, PIA is to ensure that the organizations' practices are consistent with FIPs regarding the collection, use and dissemination of information while using the appropriate safeguards and embracing a sense of moral responsibility through a privacy culture and use of best practices (Culnan et al. 2009).

Another important difference between security risk management and PIA is that security risk management decisions have been associated with the return on investment and information governance (Cavusoglu et al. 2004; Gordon et al. 2002; Khansa et al. 2009; Zhao et al. 2008). PIA prioritizes patients' privacy beyond its investment decisions. One implication of these differences is that organizations are willing to be subject to regulatory fines penalties if it means saving patients' lives.

A Process Model of Organizational Privacy Responses

Findings from this study suggest that the effectiveness of privacy responses is unveiled through its operational and behavioral outcomes. Although our model captures the different outcomes, the extent to which such outcomes change in smaller/rural healthcare organizations was not fully captured. As such, an important future research question is how OPRs outcomes differ in large/urban healthcare organizations from small/rural organizations.

We speculate further research into the impact of PIA on outcomes, because these outcomes impact the effectiveness of work practices, which might have profound implications on healthcare delivery. Our data could not directly measure the impact associated with the presence of PIA with the outcomes' effectiveness, but our finding about the benefits of PIA leads us to suggest the following proposition:

> Proposition 1 (P1): Outcomes of OPRs are more likely to be effective into healthcare practices if a privacy impact assessment has been integrated a priori.

Our findings suggest that PIA was effective because it impacted what safeguards organizations developed to mitigate privacy threats in the light of institutional pressures, competitive advantage and best practices. On paper, a combination of technical safeguards, physical safeguards, human safeguards and organizational processes makes sense, and yet organizations continue to face breaches suggesting that existing compliance programs are not effective (Culnan et al. 2009, p.678). Our data shows evidence of a strong dominance of technical safeguards used among informants, with close match with training and education safeguards. Thus, an obvious question for future inquiries is whether the presence (or absence) of PIA is associated with the right combination of safeguards employed by an organization. This leads us to suggest the following proposition:

> Proposition 2 (P2): The integration of PIA will lead to a greater balance of the appropriate OPRs.

Our findings suggest three key drivers explaining why organizations respond to privacy issues: (1) institutional pressures, (2) competitive advantage via reputation and image, and (3) ethical responsibility via best practices. Through PIA, each driver is represented as an enabler or inhibitor in developing OPRs. We expect further research to confirm that the enabling drivers are likely to facilitate and explain privacy responses, while inhibiting drivers are likely to stand in the way. Thus, we suggest the following propositions:

> Proposition 3a (P3a): The stronger the regulatory pressures (penalties and otherwise), the more likely to be considered in the organization's PIA.

> Proposition 3b (P3b): The stronger the impact of negative image and loss of reputation, the more likely to be considered in the organization's PIA.

Proposition 3c (P3c): The greater the level of commitment to business best practices, the more likely to be considered in the organization's PIA.

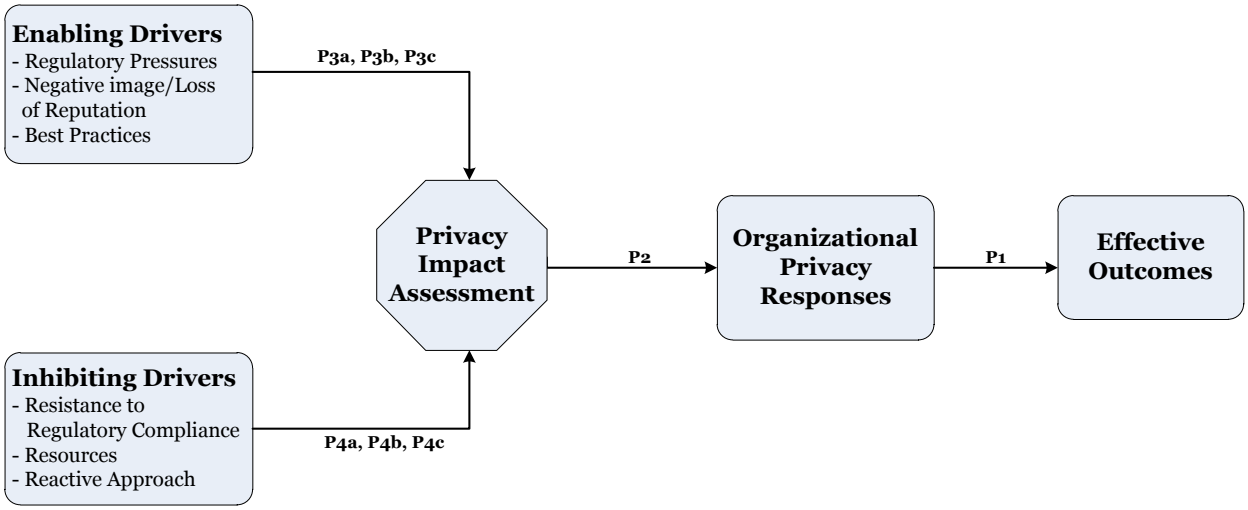

Figure 2. A Framework for Testing Propositions about PIA

Similarly, the inhibiting drivers lead to the following propositions:

Proposition 4a (P4a): The greater degree of resistance to regulatory compliance, the less likely to embrace a PIA.

Proposition 4b (P4b): The greater degree of resources limitations, the less likely to embrace a PIA.

Proposition 4c (P4c): The more reactive (and less proactive), the less likely to embrace a PIA.

Figure 2 depicts graphically the propositions derived from our grounded theory model about privacy impact assessment. The research propositions developed based on our findings should be considered in the light of this study's limitations depicted in the last section.

Conclusion and Strategic Implications

This study introduced the privacy impact assessment concept to examine the ways in which healthcare organizations respond to privacy threats and issues. The analysis of our data led to understanding the different drivers and their interactions as well as the operational and behavioral outcomes of these information privacy responses.

This study is not without limitations. In particular, our study suffered from some methodological shortcomings. First, our sampling was mainly drawn from one particular state primarily due to convenience; however, later interviews were conducted with informants from other states. Second, our informants, though they perform similar functions as privacy leaders, had different business and/or educational backgrounds, which could have affected how the privacy responses unfolded. Finally, though our sampling was diverse, we were not able to fully investigate the effect of small size hospitals and how their information privacy responses are unfolding despite their resources' constraints. Future research could explore these limitations by expanding the geographic locations with a good representation of different hospital sizes and geographic locations. Further research, could also investigate more deeply the impact of privacy leaders' backgrounds (e.g. medical, law, computer science) into their organizational privacy approaches.

Despite these limitations, this study responds (1) to current research and industry calls for better understanding of information privacy responses (Blumenthal 2011; Smith et al. 2011), (2) to the lack of theoretical explanations (Greenaway et al. 2005), and (3) to a better understanding of operational outcomes in the healthcare context (Appari et al. 2010). This study also makes important theoretical and practical implications.

From a theoretical perspective, to the best of our knowledge, this is the first study that empirically investigated organizational privacy responses in the context of healthcare. This environment showed different dynamics that resulted in unique challenges. The study addresses some important theoretical gaps in information privacy literature by considering the dynamics of these theories taken together. For example, under current regulations, healthcare organizations have to abide by the privacy rules to avoid hefty penalties. However organizations are willing to submit to theses penalties if it means saving patients' lives. Thus, a dilemma exists between what organizations have to do (organizational pressures) and the right things to do (best practices) with regards to healthcare delivery. Perhaps the major contribution of this study is the emergence of PIA where we identified several key elements that should be accounted for when handling the dynamics of the drivers of OPRs and their outcomes. This study is also the first to propose a model of OPRs using a grounded theory approach. The proposed theory attempts to reflect the actual context of healthcare.

This study offers important practical implications for healthcare practitioners. First, it offers a taxonomy of different OPRs being implemented in healthcare organizations. Second, this study offers a PIA model of assessing the influences of different drivers, while simultaneously accounting for the impact of the operational outcomes on healthcare delivery such as the impact on workflow processes, the availability of information for patients' treatment, and balance challenges. Finally, this research holds practical implications related to a deterrence approach to gain employees' adherence and several ways to monitor the overall organizational privacy compliance.

Appendix A: Semi-Structured Interview Protocol for Information Privacy Experts

1. **General Information**
    a. Interviewee background
        i. Title(s)
        ii. Education background
        iii. Years in profession
        iv. How did you end up in this position
    b. Definition/scope of information privacy
        i. Definition of information privacy
        ii. Is it similar to information security? Why? Why not?
    c. Privacy issues facing healthcare organizations in general
        i. Different Types, levels
        ii. Challenges

2. **Privacy Measures**
    a. What types of measures does your organization have in place to handle the threat of privacy issues? Were you subject to ant data breach?
    b. How long have you had these programs in place?
    c. Would your hospital consider adding other privacy measures in the future? Why or why not?
    d. What might these new measures address?
    e. Do you have privacy impact assessment tools that help you determine if you are meeting your legal, technical and policies obligations toward EHRs privacy?
    f. How do you measure your privacy compliance?

3. **Influencing Factors and Values**
    a. Why do you respond to privacy threats?
    b. What factors would influence your organization to initiate these particular measures? (What prompted your hospital to initiate these measures?)
    c. Are your organization's privacy measures designed to comply mainly with HIPAA and HITECH?
    d. Are there other regulations that you have to comply with?
    e. Are there any other internal and external factors that dictate how you design your privacy programs?
    f. What type of resources (human/financial) does the organization invest in to develop privacy policies and programs?
    g. Are there different degrees of compliance (reactive/proactive/other)? Where are you situated and why?
    h. What type of resources would you need to further your commitment to privacy?
    i. Which type of measure would you invest more on if you have extra resources?

4. **Privacy Controls Enactment/ Implementation Issues**
    a. How is privacy practiced? Is it different from one setting (clinical) to others?
    b. What type of business conflicts (workflow conflicts) does you organization face in developing and enacting these privacy programs?

c. What do you do when there is a conflict between your medical clinical work flow and mandates from regulations?
d. How does your organization balance between its day-to-day operations and privacy policies' implementation?
e. How does training and education align with routing activities? Does it support actual practices or it is informational (awareness)?
f. Are you a part of any HIMSS or CHIME chapters? Do you ever use your associations with these chapters to raise privacy mandates that are in conflict with your workflow processes? Has it ever been lobbied?
g. Under what scenario, would an organization not comply with regulations?
h. How do you balance privacy with convenience (for employees and for patients)

5. Privacy Design

a. What are the inputs of users into the design and development of privacy programs?
b. Is patients' feedback sought at any point in time with these privacy programs?
c. Is there a particular relationship with your vendors, what is the impact of vendors into embedding security and privacy features into the software?

References

Aberdeen, J., Bayer, S., Yeniterzi, R., Wellner, B., Clark, C., Hanauer, D., Malin, B., and Hirschman, L. 2010."The MITRE Identification Scrubber Toolkit: Design, Training, and Assessment," *International Journal of Medical Informatics* (79:12), pp. 849-859.

Ackerman, M.S. 2004."Privacy in Pervasive Environments: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing* (8:6), pp. 430-439.

Agrawal, R., and Johnson, C. 2007. "Securing Electronic Health Records without Impeding the Flow of Information," *International Journal of Medical Informatics* (76:5-6), pp. 471-479.

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.

Appari, A., and Johnson, M.E. 2010. "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management* (6:4), pp. 279-314.

Bansal, G., Zahedi, F., and Gefen, D. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," Proceedings of the 29th Annual International Conference on Information Systems (ICIS), Paris, France, Paper 6.

Barney, J.B. 1986. "Types of competition and the theory of strategy: Toward an integrative framework," *The Academy of Management Review* (11:4), pp. 791-800.

Blumenthal, D. 2011."Federal Health Information Technology Strategic Plan 2011 – 2015," *http://www.healthit.gov/buzz-blog/from-the-onc-desk/hit-strat-plan/*).

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010a. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010b."Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook," Proceedings of the 31st Annual International Conference on Information Systems (ICIS), Saint Louis, MO, Paper 230.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7), pp. 87-92.

Chen, J., Ping, W., Xu, Y., and Tan, B.C.Y. 2009. "Am I Afraid of my Peers? Understanding the Antecedents of Information Privacy concerns in the Online Social Context.," Proceedings of the 30th Annual International Conference on Information Systems (ICIS), Phoenix, AZ, Paper 174.

Chiang, Y.C., Hsu, T., Kuo, S., Liau, C.J., and Wang, D.W. 2003. "Preserving Confidentiality When Sharing Medical Database with the Cellsecu System," *International Journal of Medical Informatics* (71:1), pp. 17-23.

Cranor, L., Egelman, S., Tsai, J., and Acquisti, A. 2007. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," Proceedings of the 28th Annual International Conference on Information Systems (ICIS), Montreal, Canada, Paper 20.

Culnan, M., and Williams, C. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly* (33:4) 2009, pp 673-687.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: a Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

DHS. 2010. "Privacy Office- Privacy Impact Assessments (PIA). http://www.dhs.gov/files/publications/editorial_0511.shtm,".

DiMaggio, P.J., and Powell, W.W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *Rationality in Organizational Fields* (48), pp. 147-160.

Eisenhardt, K.M. 1989. "Building theories from case study research," *Academy of Management Review* (14:4), pp. 532-550.

Fernando, J.I., and Dawson, L.L. 2009. "The Health Information System Security Threat Lifecycle: An Informatics Theory," *International Journal of Medical Informatics* (78:12), pp. 815-826.

Gerber, M., and von Solms, R. 2005. "Management of Risk in the Information Age," *Computers & Security* (24:1), pp. 16-30.

Goodstein, J.D. 1994. "Institutional Pressures and Strategic Responsiveness: Employer Involvement in Work-Family Issues," *The Academy of Management Journal* (37:2), pp. 350-382.

Gordon, L.A., and Loeb, M.P. 2002. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security (TISSEC)* (5:4), pp. 438-457.
Greenaway, K.E., and Chan, Y.E. 2005. "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6:6), pp. 171-198.
Herath, T., and Rao, H.R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp 154-165.
HEW. 1973. "Fair Information Practices. U.S. Dept. of Health, Education and Welfare. http://www.privacyrights.org/ar/fairinfo.htm,").
HHS. 2011a."Breaches Affecting 500 or More Individuals. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html,"
HHS. 2011b. "Privacy Impact Assessments. http://www.hhs.gov/pia/,").
Hodgkinson, R., Branz, L., Culnan, M., Dhillon, G., MacWillson, A., and Ponemon, L. 2010. "Information Security and Privacy: Rethinking Governance Models," Proceedings of the 31st Annual International Conference on Information Systems (ICIS), Saint Louis, MO, Paper 38.
Ishikawa, K. 2000. "Health Data Use and Protection Policy; Based on Differences by Cultural and Social Environment," *International Journal of Medical Informatics* (60:2), pp. 119-125.
Johns, G. 2006. "The Essential Impact of Context on Organizational Behavior," *Academy of management review* (31:2), pp. 386-408.
Khansa, L., and Liginlal, D. 2009. "Valuing the Flexibility of Investing in Security Process Innovations," *European Journal of Operational Research* (192:1), pp. 216-235.
Klein, H.K., and Myers, M.D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), pp. 67-93.
Kluge, E.H.W. 2007. "Secure e-Health: Managing Risks to Patient Health Data," *International Journal of Medical Informatics* (76:5-6), pp. 402-406.
Kotulic, A.G., and Clark, J.G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp. 597-607.
Kreiner, G.E., Hollensbe, E.C., and Sheep, M.L. 2006. "Where is the" me" among the" we"? Identity Work and the Search for Optimal Balance," *The Academy of Management Journal* (49:5), pp. 1031-1057.
Lincoln, Y.S., and Guba, E.G. 1985. *Naturalistic inquiry* Sage Publications, Inc,.
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.
Martin, P.Y., and Turner, B.A. 1986. "Grounded Theory and Organizational Research," *The Journal of Applied Behavioral Science* (22:2), pp. 141-157.
Meyer, J.W., and Rowan, B. 1977. "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), pp. 340-363.
Mignerat, M., and Rivard, S. 2009. "Positioning the institutional perspective in information systems research," *Journal of Information Technology* (24:4), pp. 369-391.
Milberg, S.J., Burke, S.J., Smith, H.J., and Kallman, E.A. 1995. "Values, personal information privacy, and regulatory approaches," *Communications of the ACM* (38:12), pp. 65-74.
Mohan, J., and Razali Raja Yaacob, R. 2004. "The Malaysian Telehealth Flagship Application: a National Approach to Health Data Protection and Utilisation and Consumer Rights," *International Journal of Medical Informatics* (73:3), pp. 217-227.
Neubauer, T., and Heurix, J. 2011. "A Methodology for the Pseudonymization of Medical Data," *International Journal of Medical Informatics* (80:3), pp. 190-204.
Ohno-Machado, L., Silveira, P.S.P., and Vinterbo, S. 2004. "Protecting Patient Privacy by Quantifiable Control of Disclosures in Disseminated Databases," *International Journal of Medical Informatics* (73:7-8), pp. 599-606.
Oliver, C. 1991. "Strategic Responses to Institutional Processes," *Academy of management review* (16:1), pp. 145-179.
Orlikowski, W.J. 1993. "CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development," *MIS Quarterly* (17:3), pp. 309-340.
Orlikowski, W.J., and Barley, S.R. 2001. "Technology and Institutions: What can Research on Information Technology and Research on Organizations Learn from Each Other?," *MIS Quarterly* (25:2), pp. 145-165.
Quantin, C., Allaert, F.A., and Dusserre, L. 2000. "Anonymous Statistical Methods Versus Cryptographic Methods in Epidemiology," *International Journal of Medical Informatics* (60:2), pp. 177-183.

Rumelt, R.P. 1984. *Towards a Strategic Theory of the Firm*. Prentice-Hall, Englewood Cliffs, NJ, pp. 556-570.
Schultze, U., and Avital, M. 2010. "Designing Interviews to Generate Rich Data for Information Systems Research," *Information and Organization* (21:1), pp. 1-16.
Siponen, M., and Vance, A.O. 2010. "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *Management Information Systems Quarterly* (34:3), pp. 487-502.
Smith, H.J. 1993. "Privacy Policies and Practices: Inside the Organizational Maze," *Communications of the ACM* (36:12), pp. 104-122.
Smith, J. 2000. "Towards a Secure EPR: Cultural and Educational Issues," *International Journal of Medical Informatics* (60:2), pp. 137-142.
Smith, J.H., Dinev, T., and Xu, H. (forthcoming). "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*.
Son, J.Y., and Kim, S.S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.
Spears, J.L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.
Straub, D.W., and Straub, W. 1990. "Effective IS Security," *Information Systems Research* (1:3), pp. 255-276.
Strauss, A.L., and Corbin, J. 2008. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques. 3rd Ed. Newbury Park, CA: Sage*.
Teo, H.H., Wei, K.K., and Benbasat, I. 2003. "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective," *MIS Quarterly* (27:1), pp. 19-49.
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268.
Turner, B.A. 1983. "The Use of Grounded Theory for the Qualitative Analysis of Organizational Behaviour," *Journal of Management Studies* (20:3), pp. 333-348.
Van Maanen, J. 1979. "The Fact of Fiction in Organizational Ethnography," *Administrative Science Quarterly* (24:4), pp. 539-550.
Van Slyke, C., Shim, J.T., Johnson, R., and Jiang, J.J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:6), pp. 415-444.
Walsham, G., and Sahay, S. 1999. "GIS for District-Level Administration in India: Problems and Opportunities," *MIS Quarterly* (23:1), pp. 39-65.
Wernerfelt, B. 1984. "A Resource-Based View of the Firm," *Strategic Management Journal* (5), pp 171-180.
Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," Proceedings of the 29th Annual International Conference on Information Systems (ICIS), Paris, France, Paper 6.
Yeh, Q.J., and Chang, A.J.T. 2007. "Threats and Countermeasures for Information System Security: A Cross-Industry Study," *Information & Management* (44:5), pp. 480-491.
Zhao, X., and Johnson, M.E. 2008. "Information Governance: Flexibility and Control through Escalation and Incentives," in: *Workshop on the Economics of Information Security*, Hanover, NH, pp. 26-27.