2012

Imbalance Challenge of Enacting Information Privacy Safeguards in Healthcare: A Grounded Theory Approach

Rachida Parks
Pennsylvania State University

Heng XU
Pennsylvania State University

Chao-Hsien CHU
Pennsylvania State University, chchu@smu.edu.sg

Imbalance Challenge of Enacting Information Privacy Safeguards in Healthcare: A Grounded Theory Approach

Rachida Parks
University of Arkansas at Little Rock
Little Rock, AR, USA
rfparks@ualr.edu

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

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

ABSTRACT

Healthcare organizations face significant challenges in designing and implementing the appropriate safeguards to mitigate information privacy threats. While many studies examined various technical and behavioral safeguards to protect the confidentiality and privacy of patient information, very little is known about the actual outcomes and implications of the privacy practices in which organizations engage. There is little research theoretically explaining the outcomes of enacting privacy safeguards and subsequent effects on privacy compliance. This paper reports the results of a grounded theory study investigating the intended consequences (positive impacts) and unintended (negative impacts) consequences of enacting privacy safeguards in healthcare organizations. An imbalance challenge occurs when the negative impacts outweigh the positive ones. To address the imbalance challenge, organizations need to achieve a balance between privacy and utility, meeting privacy requirements without impeding the workflow in medical practices. Findings are presented within an emerging theoretical framework of the imbalance challenge identified in this work. This study is one of the first systematic attempts to identify the opposing impacts of privacy safeguard enactments and examine its implications for privacy compliance in the healthcare domain.

Keywords: Information privacy, privacy safeguards, healthcare, imbalance challenge, and grounded theory

1. INTRODUCTION

Ensuring patient information privacy remains one of the most pressing problems in the modern healthcare industry. Situations where personal health information is stolen or disclosed without authorization have been widely discussed in the media and have raised awareness about digitization and the use of personal health information. For example, the Privacy Rights Clearinghouse has been tracking breaches since 2005 and published a chronology including over 22 million healthcare-related breaches (PRC 2012). Since 2009, the Office of Civil Rights has identified privacy breaches affecting over 19 million individuals (HHS 2011a). Information privacy breaches endanger the privacy and confidentiality of patient information (Angst and Agarwal 2009; Bourgeois et al. 2008; Fernando and Dawson 2009), resulting in problems such as adverse effects on medical insurance and unemployment (Benitez and Malin 2010). In addition, these breaches may also affect organizations' reputations and lead to dire consequences such as monetary penalties and civil and criminal liabilities (Bulgurcu et al. 2010).

Previous research advocated implementing privacy safeguards in organizational privacy management,[1] i.e., preventative measures to reduce privacy threats and protect sensitive health information, such as policies, privacy-enhancing technologies, and administrative processes, (Aberdeen et al. 2010; Agrawal and Johnson 2007; Croll 2010; Culnan and Williams 2009; Mohan and Razali Raja Yaacob 2004). These safeguards do not seem effective, because privacy breaches continue to occur (Culnan and Williams 2009). Empirical evidence suggests that

[1] In this research, we focus on privacy management problems resulting from as organizational information practices in terms of collection, use, security, and distribution of personal information (Culnan and Williams 2009). Consistent with Culnan and Williams (2009), we define security as one aspect of privacy and argue that privacy includes more than security. According to Culnan and Williams (2009, p.675), "privacy is broader and encompasses permission and use of personal information. Privacy is difficult to achieve without security. However, organizations can successfully secure the personal information in their databases but still make bad decisions about subsequent use and distribution of personal information, resulting in a privacy problem."

effective privacy safeguards should account for business impact (Choi et al. 2006; Parks et al. 2011b; Stahl et al. 2011). However, very little is known about the impacts of privacy safeguard enactments on clinicians' needs for information and organizational workflow. Moreover, there is little research theoretically explaining the outcomes of enacting privacy safeguards and the subsequent effects on privacy compliance.[2] As Belanger and Crossler (2011, p. 1022) pointed out, "there are many behavioral questions to be explored with respect to not only use of potential privacy protection tools but also effectiveness and consequences of use." Similarly, this void in extant privacy literature has also been identified by an interdisciplinary literature review (Smith et al. 2011) that highlights the need for more privacy research to consider actual outcomes. Following these calls for research on examining impacts and outcomes of privacy safeguards, we aim to investigate the conditions under which the negative impacts[3] of privacy safeguard enactments outweigh the positive ones (i.e., the imbalance challenge occurs). Specifically, we aim to address the following two research questions in this work:

Research Question 1: What are the positive and negative business impacts in implementing information privacy safeguards, and how are these safeguards integrated into medical practices?

Research Question 2: Under what conditions will the negative impacts of privacy safeguard enactments outweigh the positive ones? What are the outcomes of the imbalance challenge?

The current study contributes to existing privacy research in several important ways. First, following the call by Belanger and Crossler (2011), we have studied the outcome of enacting privacy safeguards and their subsequent effects on privacy compliance; specifically, the

[2] Privacy compliance is defined as complying with HIPPA privacy rules in order to assure the confidentiality of electronically protected health information.

[3] In this study, the term "impact" is used to describe the challenges organizational leaders identified from their operational processes and work practices after the enactment of privacy safeguards.

imbalance challenge emerged as an analytical construct to capture unintended consequences caused by the situation where the negative impacts of privacy safeguards outweigh the positive ones. Second, Smith et al. (2011) have shown a lack of organizational level privacy research in extant literature, and the challenge is that studies at the organizational levels "are necessarily more complex and less conducive to 'quick' data collection techniques such as written and online surveys" (p. 1006). This research provides new theoretical insights into understanding privacy management by targeting this under-researched level of analysis through a grounded theory approach. Third, this study was designed to gain an in-depth understanding of the actual outcomes and implications of privacy practices in healthcare organizations. Therefore, using a grounded theory methodology provides a rich lens to understand the consequences of privacy safeguards enactments and their implications for privacy compliance. Fourth, this study contributes to the recent need for interdisciplinary research by converging the research streams of IS and health informatics.

2. LITERATURE REVIEW

We review literature from both the fields of IS and health informatics in order to describe the current level of knowledge associated with the impacts in implementing information privacy safeguards. The literature in health informatics was sought because this study focuses on healthcare organizations. Following this review, we briefly outline the different types of information privacy safeguards, identify the gaps in literature, and then discuss how negative impacts of enacting privacy safeguards contribute to the imbalance challenge.

There is a growing, yet limited, body of research targeting organizational responses to privacy threats and issues (Culnan and Williams 2009; Greenaway and Chan 2005, Smith et al.

2011). One recent study suggests that organizations respond to the increasing list of privacy threats through a combination of technical and human controls, as well as processes (Parks et al. 2011a). In terms of technical safeguards, health informatics literature is saturated with research that employs various technologies to address health information privacy threats, including the application of access control mechanisms to limit access to authorized users (Blobel et al. 2006; Chen et al. 2010; Lovis et al. 2007; Mohan and Razali Raja Yaacob 2004; Peleg et al. 2008; Reni et al. 2004; Sujansky et al. 2010; van der Linden et al. 2009), use of anonymization and pseudonymization to remove the identifier from medical data (Aberdeen et al. 2010; Boyd et al. 2007; Chiang et al. 2003; Li and Sarkar 2010; Mohan and Razali Raja Yaacob 2004; Neubauer and Heurix 2011; Ohno-Machado et al. 2004; Quantin et al. 2000), and adoption of encryption and cryptographic methods to make the data unreadable to anyone except those who hold the keys (Kluge 2007; Quantin et al. 2000).

One of the biggest challenges in implementing the aforementioned technical safeguards is to develop systems or technologies that do not impede the operational activities of healthcare providers (Lovis et al. 2007). In terms of healthcare delivery processes, both IS and health informatics research discuss policies that were developed to govern such processes and ensure information privacy. It has been almost two decades since Smith (1993) published the findings based on a study of organizational privacy policies, which drew attention to such problems as a lack of policies and gaps between different policies and practices. While organizations in the U.S. are more likely to have a privacy policy (Liu and Arnett 2002; Peslak 2006), the gap between policies and clinical uses is still significant (Croll 2010), and research on policy violations is growing (Siponen and Vance 2010). In term of human safeguards, several studies investigated the impact of training and education and thus contributed to the current scholarly knowledge

(D'Arcy et al. 2009; Fernando and Dawson 2009; Ishikawa 2000; Mohan and Razali Raja Yaacob 2004; Patel et al. 2000; Yeh and Chang 2007). The positive impact of these safeguards is questionable, especially with more recent research on employees' misbehaviors, lack of adherence, and compliance problems (Bulgurcu et al. 2010; Siponen and Vance 2010; Vroom and Von Solms 2004).

As discussed above, various types of information privacy safeguards have been identified as the mechanisms for organizations to respond to privacy threats and achieve compliance. However, establishing safeguards in harmony with the "actual day-to-day procedures" remains one of the major challenges for healthcare organizations (Choi et al. 2006). In this study, we identified four facets of negative impacts on enacting information privacy safeguards: (1) unavailability of information, (2) workflow disruptions, (3) usability issues, and (4) operational feasibility issues.

Unavailability of Information. Healthcare professionals, such as doctors and nurses, are increasingly dependent on the availability and accuracy of patient information to provide adequate treatment and make other healthcare-related decisions. Information availability is very important in the healthcare sector, where it is often needed on a continuous, 24/7 basis. Traditionally, non-availability of information is linked with computer failures, program or human errors, and environmental conditions (Bakker 1998). However, existing privacy research in the field of health informatics highlights the dilemma of ensuring availability and access to patient information for authorized healthcare providers without breaching the confidentiality and privacy of medical information (Salomon et al. 2010; Smith and Eloff 1999). If the information needed by healthcare professionals to reach critical clinical decisions was unavailable due to

tight access controls, patients may be incorrectly treated. Therefore, unavailability of information may have dire consequences for the quality for patient care.

Workflow Disruptions. In the pursuit of privacy compliance, organizations implement processes that change their operational workflows. These changes may involve encrypting documents network transmission, pulling staff out for training, or instating time-out features. As a result, users may not always positively react to implemented changes, especially when these changes disrupt their work routines. Bulgurcu et al. (2010) reported push backs and resistance from users. According to Choi (2006), before HIPAA, workflow was much smoother and more efficient than the newer workflow that involves locking doors and limiting computer access to avoid regulatory incompliance and/or penalties. Another example of how implementing privacy safeguards triggers workflow disruptions is documented by Coiera et al. (2004), in which managing patients' e-consent privacy preferences may impede clinicians' workflow. Failure to address these workflow disruptions could potentially lead employees to embrace workarounds to bypass features that make accomplishing their work difficult (Ash et al. 2004).

Usability Issues. Usability has been defined as the degree of efficiency and effectiveness of use (Bennett 1984; Shackel 1984), and this concept has been applied within a range of users, tasks, tools, and environments. With the design and implementation of privacy protective technologies, usability has become an extremely important, albeit poorly understood, element of privacy. The end results are user dissatisfaction and unusable systems (Johnson et al. 2005). In the healthcare industry, understanding the interplay between usability and privacy is essential. Privacy safeguard technologies, such as biometrics, have been introduced to control access to medical facilities and protect the privacy and confidentiality of patient information (Marohn 2006). However, using biometrics also poses several usability issues due to the impact of

temperature, humidity, and dirt (Flores Zuniga et al. 2010). The usability issues of biometrics can also stem from the user's age, skin color, or certain health conditions where the use of hygienic gloves is required (Flores Zuniga et al. 2010). This study pertains to the impacts of privacy safeguard enactments on workflow and work practices; therefore, we will focus on usability issues perceived by healthcare workers.

Operational Feasibility Issues. Operational feasibility is an important factor for the deployment of new technologies or processes in the real world. Privacy safeguards include a variety of measures that range from technologies to policies and processes. In the case of technologies, several research papers reported negative impacts of the implementation of protective technologies on operational feasibility resulting in the degradation of performance. Zhao et al. (2005), in a technical study on security protocols, found that such security protocols led to a tradeoff between privacy measures and performance. Implementing privacy safeguards includes putting into place formal privacy education and training programs, as well as monitoring compliance through the use of technology and human processes. Prior studies investigated the impact of training on employees and their employees' compliance (Whitman and Mattord 2004). However, there is little insight into how these safeguards impact the operational feasibilities of healthcare practices. We are unaware of any studies, other than technology-oriented ones, analyzing the operational impact of training, audits and investigation, and facility access.

3. RESEARCH METHODS

This study adopts a qualitative research method to answer our research questions about the outcomes of enacting privacy safeguards. Specifically, the study uses a qualitative research approach based on the grounded theory (Strauss and Corbin 2008). Grounded theory aims to

develop inductive theory from data through incremental and systematic progression in knowledge, deriving conceptual deduction and hypotheses (Urquhart et al. 2010). Furthermore, the grounded theory method is particularly appropriate for studies of dynamic environments, such as healthcare (Glaser and Strauss 1967). It offers a rigorous approach that assists in the understanding of organizational privacy safeguards at the organizational level, through testable theories tightly connected to their data and their context (Eisenhardt 1989).

3.1 Data Collection

After clearance of the Institutional Review Board (IRB), informants were contacted to participate in this study. Informants from U.S. hospitals as well as other healthcare organizations (consulting and healthcare research firms, government, and professional healthcare organizations) agreed to participate in this study as part of a dissertation project. All informants held executive and decision-making positions within their respective organizations. Table 1 summarizes the informants' titles and types of organizations.

Data were gathered through semi-structured interviews with thirty key consenting informants who could offer expert knowledge in privacy practices and were holding key positions in hospitals, such as Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Privacy Officer (CPO), Chief Medical Information Officer (CMIO), Information Technology directors and privacy officers (Table 1). Interviews lasted between 40 and 90 minutes and were carried out by the first author between fall 2010 and spring 2012. The interviews explored the types of safeguards being used by healthcare organizations to mitigate privacy threats and their impacts on healthcare activities and practices. Further details about the interview items are provided in Appendix A and B.

Hospital size	***Informants***	***Title***
Small (less than 200 beds)	*1*	*Chief Executive Officer*
	2	*Privacy Officer*
	3	*IT Director*
	4	*Chief Information Officer*
	5	*IT Director*
	6	*Vice President*
	7	*Executive Director*
	8	*Director of HIM*
	9	*Privacy Officer*
	10	*IT Director*
Medium (between 200 and 500 beds)	*11*	*Chief Information Officer*
	12	*Chief Privacy Officer*
	13	*Vice President of IT*
	14	*Chief Privacy Officer*
	15	*Security Officer*
	16	*IS Director*
	17	*Privacy Officer*
	18	*Chief Information Officer*
Large (more than 500 beds)	*19*	*Chief Medical Information Officer*
	20	*Chief Medical Information Officer*
	21	*Chief Privacy Officer*
	22	*Privacy Officer*
	23	*HIPAA Security Officer*
	24	*Chief Security Officer*
	25	*HIPAA Officer*
Other healthcare organizations	*26*	*President*
	27	*Chief Privacy Officer*
	28	*Vice President*
	29	*Chief Privacy Officer*
	30	*Chief Executive Officer*

Table 1: Summary of Data Sources

In grounded theory, sampling is driven by conceptual emergence and limited by theoretical saturation (Glaser and Strauss 1967). Consequently, the selection of data sources is neither a random selection nor a totally a priori determination. For example, we decided a priori

that a combination of different hospital sizes was most appropriate for this study; however, the specific details depended on the emerging themes. Strauss and Corbin note that the researcher must be flexible to handle the turns and twists as they arise during data collection and analysis. In this study, theoretical sampling is evident through the following statements:

- Interviewing was initiated with informants from hospitals. However, after initial data analysis, this target was revisited to include other healthcare organizations and entities (e.g., the U.S. Department of Health and Human Services, healthcare professional associations, healthcare IT providers, and healthcare privacy consultants).
- The interview questions were also revisited after the analysis of the first interviews, in order to include more specific questions about the operational impacts as a result of implementing privacy safeguards. This is consistent with Strauss and Corbin's approach to theoretical sampling, where the researcher "adjusts the interviews and observations on the basis of emergent and relevant concepts" (1998, p. 207).

Although 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, data collection and analysis were conducted until the point of saturation, when redundancy in the data was reached and no new concepts were found (Corbin and Strauss, 2008).

3.2 Data Analysis

In this section, we provide a summarized overview of the steps undertaken using the grounded theory approach. These steps are depicted in Figure 1.

All interviews were audio recorded and transcribed verbatim. Transcribed interviews were imported to a computer aided qualitative data analysis software tool called Nvivo (v.9). It is worth noting that Nvivo is not a software that automatically code the transcribed interviews but rather was used to organize the different codes and categories that were identified during the first and second order analysis. NVivo supported conducting different stages of analysis including setting up concepts within themes called nodes, and providing some data analysis capabilities for searching, grouping, and relating nodes. Interviews were coded in several steps. First, we used open coding techniques to inductively identify preliminary categories. No a priori coding or categorization was used. The next step used was axial coding, which helped to develop the categories further into themes (Strauss and Corbin 2008). Finally, we implemented selective coding, where we related the categories together into a coherent theoretical framework. During the process of data collection and analysis, we 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.

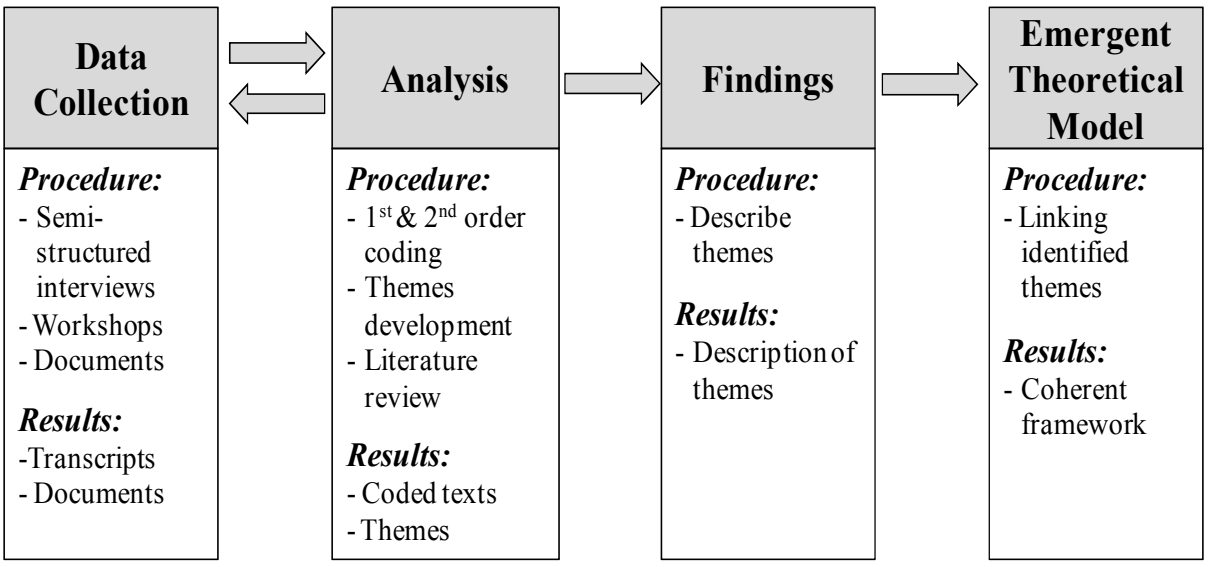

Figure 1: Grounded Theory Analysis Process

During the coding process, every piece of data was contrasted against other pieces through constant comparison. The process of constant comparison was an iterative one to assure the allocation of the appropriate codes to informants' views. The constant comparison determines the relevance or otherwise the assumptions to the emergent theory. For example, the initial perception of the importance of the hospital's size did not sustain into the theory.

Having embracing constant comparison, we needed to know when to stop coding and categorizing data. We continued looking for information until the categories were saturated and no additional data was found.

3.3 Evaluative and Trustworthiness Criteria

Every research must be evaluated by the appropriate criteria. Positivist researchers employ the criteria of internal validity, external validity, reliability, and objectivity. These criteria are not appropriate for interpretive studies. In what follows, two approaches for judging interpretive research are presented: (1) ensuring trustworthiness (Lincoln et al. 1985) and (2) ensuring the adequacy of the research process and the empirical grounding (Strauss et al., 1998; Corbin et al., 2008).

The aim of trustworthiness is to support the premise that the study's findings are "worth paying attention to" (Lincoln et al., 1985, p. 290). Lincoln and Guba (1985) offered a set of four trustworthiness criteria appropriate for interpretive research and analogous to positivist research: credibility, transferability, dependability, and confirmability. To address credibility, the study used multiple methods and sources to ensure triangulation of the findings, such as single interviews, group interviews, and data collection across different sources (e.g., hospitals,

government, consultants, and IT designers). Triangulation was also achieved by supplementing workshops, round tables, and documentation. Moreover, the first author had several years of industry experience in healthcare IT, in addition to being an active member of a healthcare research center and a national healthcare professional association. To ensure transferability, the study provided a detailed first-order analysis of the phenomenon and context, which is supposed to provide enough background for the readers to judge the plausibility of the findings and their applicability beyond the bounds of this project (Van Maanen 1979). Rather than conducting an inter-rater reliability, an inquiry audit was conducted. This is because interpretive research assumes each researcher will have a unique interpretation of the findings, therefore inter-rater reliability cannot be applied (Lincoln and Guba, 1985). An inquiry audit was performed by one professor of organizational behavior and a senior graduate student (trained in qualitative research) to examine and assess the process of inquiry and review the interview transcripts, coding sheets, and data analysis. Finally, to measure how the findings are supported by the data collected; the study was shared with professors, two graduate students, and two healthcare professionals, in order to get critical feedback. Consensus suggests that this research analysis and theoretical model accurately reflect the data.

Corbin and Strauss (2008) identified several criteria for evaluating the empirical grounding and the research process of the study. Each criterion was evaluated for applicability and documented in Appendix F and Appendix G.

4. FINDINGS

In this section, findings about positive impacts and negative impacts are reported. Negative impacts are identified as information unavailability, disruptions of workflows, usability issues, and operational feasibilities issues. Positive impacts are identified as deterrence effects,

controlled access, and tracking mechanisms. Figure 2 depicts the first-order concepts that led to the second-order themes and overarching dimensions.

In this study, privacy leaders reported intended consequences (positive impacts) and unintended consequences (negative impacts) of implementing privacy safeguards. No concerns were noted when there was a dominance of positive impacts. However, the data analysis revealed a tension when negative impacts outweighed positive impacts, causing a state of imbalance between maintaining patient privacy and not inhibiting work practices. Thus the notion of *imbalance challenge* emerged when the equilibrium between positive and negative impacts is shifted because the negative impacts outweigh positive impacts.

In summary, healthcare organizations face significant challenges in designing and implementing the appropriate safeguards to mitigate information privacy threats. These challenges continue with the sequel of privacy safeguards post implementation. For example, enacting privacy safeguards such as time out features has a positive impact by protecting unattended computers. However, the same feature can stand in the way of optimum healthcare delivery for an emergency physician, as noted by a Chief Security Officer:

> *"We have twenty minutes time out feature . . . If I am a doctor in the emergency room and my system times out on me while I'm critically working on a patient . . . I have to [enter] my password, that's not a good thing. "*

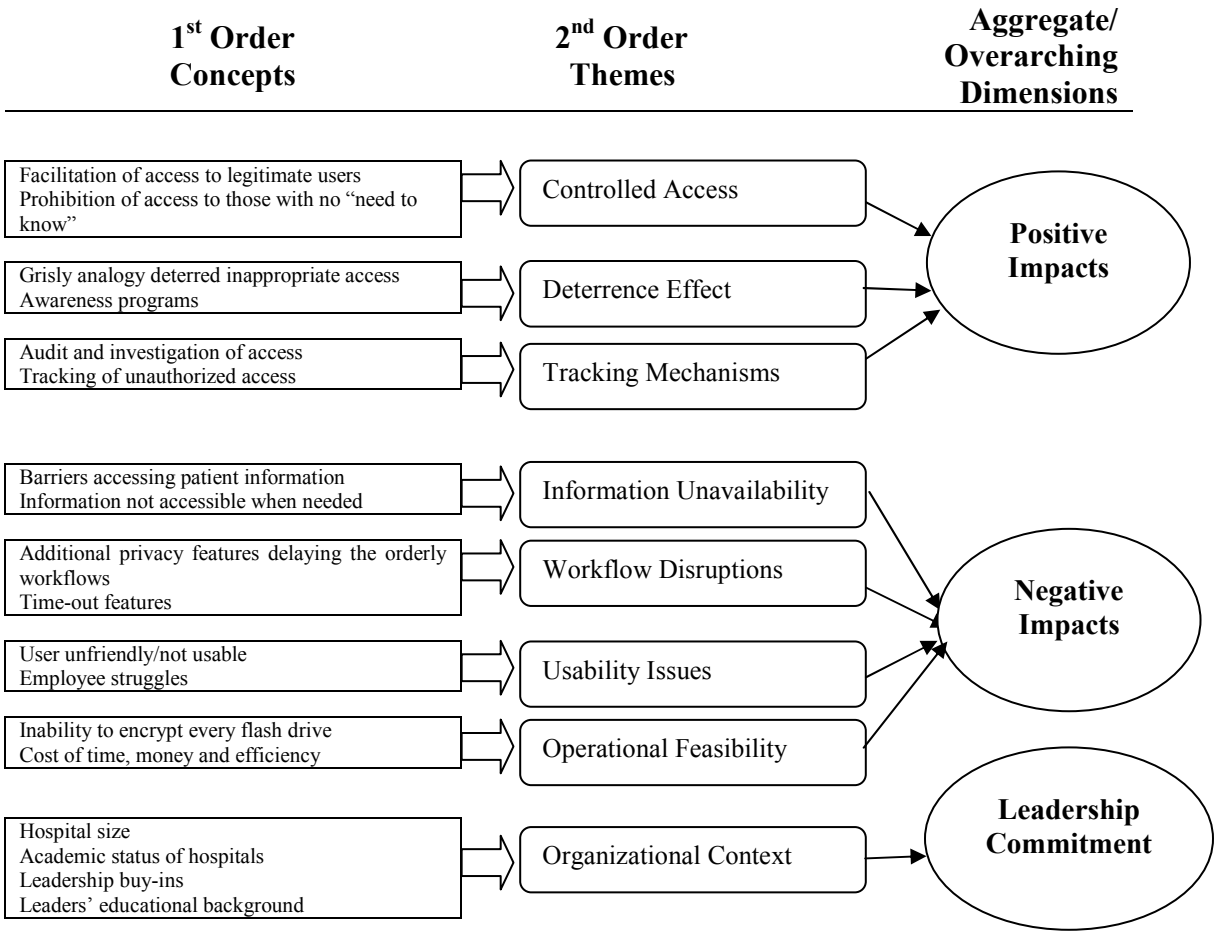

Figure 2: Emergent Concepts, Themes, and Dimensions

4.1 Negative Impacts

Throughout this research project, healthcare leaders stated on numerous occasions that privacy threats do not end with the implementation of controls. They uniformly emphasized the need for better understanding and handling of the conflicting challenges that arose. Hence a thorough understanding of these factors and their impacts on business practices is fundamental for explaining and possibly addressing the imbalance challenge. One Chief Privacy Officer

commented: *"There is a lot of indirect impact that you have to be careful of its operational efficiency . . . It's got to be costing us money or it's got to be costing us efficiency."* The impact of privacy safeguards brings out a balance issue that is of high concern to healthcare leaders. This section includes the analysis of the influence of four facets of negative impacts: (1) unavailability of information, (2) workflow disruptions, (3) usability issues, and (4) operational feasibility.

Information Unavailability: It should be noted that a question about the impact of privacy safeguards on availability of information was not explicitly asked during the interviews. Rather, the informants themselves introduced this challenge into the course of explaining the impact of implementation of privacy safeguards. This challenge was described by one Chief of Information Security Officer as having two directives:

> *"Our role is to protect it [patient information], make sure that confidentiality, integrity and availability is there for us but that we can also get it [patient information] into the hands of the patient. And, to be honest with you, it's going to be a challenge. It's almost like having two directives. A lot of healthcare facilities concentrate on trying to keep everything tight to the chest . . . but at the same time we now have mandates that say we have to make it available in a variety of formats to our patients. "*

Several healthcare leaders discussed the ways in which implementing privacy safeguards influenced the availability or accessibility of patient information. Lacking access to the information needed to perform his or her job is a big hurdle for any healthcare professional. For example, doctors need to see a patient's medications list or their lab tests, but may not need to see a progress note on a psychiatric condition or a psychotherapy note. The desire to balance the implementation of privacy programs and the healthcare delivery appeared to have created a

serious issue for clinicians trying to provide care for their patients, which ended up opening doors for potential unauthorized access and impacting their privacy compliance. As was noted by one of the healthcare executives:

> *"The biggest challenge with respect to privacy and healthcare, in my mind, is this notion that you have to err on the side of providing additional information access. You can't afford to put a barrier in front of a physician or a clinician when they need to have access to the information. So you have to sometimes err on providing broader access than you might think you need, because you don't necessarily know what you need about those people who need to have access to. That does raise challenges, because that then allows those individuals [to access] information that they don't need to see."*

Another healthcare executive noted that*:*

> *"One of the challenges with my area is when we try to secure the information but, yet, our healthcare providers need quick access to it. So there's always kind of a fine line there. We try to make it as accessible as possible but, yet, have security measures in place to protect those assets."*

Such an imbalance challenge is potentially impacting privacy compliance. Indeed, when healthcare leaders described the challenges of information availability and data accessibility, they connected it to their compliance with healthcare regulations. There is a worrisome aspect of compliance concerning the law and its impact on privacy compliance. It is well described in a following statement made by one of the study participants:

"We have lots of policies and everybody else has lots of policies, but we can't meet the regulations in the strictest letter of the law and offer clinicians the ability to practice in an efficient, cost-effective manner."

Workflow Disruptions: As part of the interview protocol (Appendix A), the first author explored the impact of privacy and security safeguards on healthcare workflows. Comments about workflow disruptions issues came up during the semi-structured interviewing. The data analysis shows that these workflow disruptions were reflected through conflicts and push-backs from employees: "*If the security is too hard, people wouldn't do it. If it is beyond their workflow much, they won't do it*." In addition, another informant stated: *"I tell people all the time that security flies in the face of convenience; that's just the way . . . so a lot of push-backs or complaints"* and *"do you want me not to administer that medication because everything didn't line up in the security behind the scenes?"*

The enactment of certain privacy technologies resulted in conflicts and push-backs. For example, timeout features are supposed to log off employees whose sessions are inactive in order to prevent unauthorized access by other employees. While this feature theoretically seems to be a great privacy initiative, it is not always positively received by certain healthcare professionals, especially by doctors in emergency departments. One privacy leader stated:

"Once I log in, I don't want the system to log me out automatically. I don't like it and timeout features. There's timeout in all our systems. This is something we have to work around."

Another example of workflow disruptions is password management. Healthcare is swamped with different applications, and employees have to log on into different systems to

access information about their patients. One informant commented on the difficulty in managing different passwords: "*I am using application A, application B, and you get all these passwords you got to remember. Guess what? I am going to start writing them down*." Employees start writing down their passwords, which potentially makes the organizational network easily accessible to hackers or unethical co-workers. This ultimately hinders privacy compliance instead of facilitating it as first intended by instating a password.

Organizations tend to consider these impacts in order to avoid push-backs and workarounds: "*We try to take that into account, the workflow issues, when you are looking at a policy because there is no sense in establishing a policy that people will not adhere to*." Although mitigation tools were put in place to bring the hospitals into compliance, in some cases, they end up negatively impacting the hospitals' adherence to regulations. In the case of workflow disruptions issues, employees found ways around these mitigations tools to accomplish their duties. This disruption is illustrated by the nurses' work practices that one of the study informants shared:

> *"40% of the work that a nurse does is to administer medication. 40% of her day, she is looking for pills and administering them . . . She is logging in and waiting, waiting, waiting, waiting. That is a problem; she is not going to get her job done. It's hard enough to do the charting, administering medicine without the waiting, waiting, waiting, waiting. So what most hospitals do is they have these computers-on-wheels, and they wheel [such a computer] into the patient's room and they leave it logged on and they administer the medicine and they wheel it out and they leave it logged on, and then they go into the next room and then leave it logged on. But when they go back to the medicine room it's logged on and that's a security risk.*"

In the case of password management, employees are writing down their passwords, which means they become easily accessible to hackers or unethical co-workers. This ultimately hinders privacy compliance instead of facilitating it as first intended by instating a password.

Usability Issues: The usability challenges that were found during data analysis include current applications or systems of electronic health records (EHRs). The challenges arise from dealing with inherent difficulties associated with the task of using certain applications. Over the course of this study, healthcare executives explained that they had to take into consideration the usability of the privacy safeguards they put in place or embedded in their IT applications:

> *"It comes from EHRs' usability and access to information. I mean, in certain scenarios, I would like to walk in with a purely clinician's hat on. I like to walk into a room and see the patient's information, talk with that patient, and provide the care. But somehow I have to be acknowledged as being allowed to see that information. So, that is one of the conflicts. I have to log in or else I have to use an RFID tag or swipe something to get into that record."*

If a new privacy or security feature is hard to use or difficult to navigate, users will abandon it, as was clearly stated by an informant: "*If it is not usable to them, they won't use it. And the things that are very usable to them, they are used to them, they can; I've seen this all the time.*" Therefore, not accounting for the usability issues causes employees not to use privacy protocols or to find ways around them to accomplish their tasks, which could negatively impact the organizational privacy compliance.

Operational Feasibility Issues: Many of the informants commented on the operational feasibility of the privacy safeguards implemented in their hospitals, which usually involves resources, time, and efficiency. As stated by one of the informants:

> *"So it does have an impact on resources and operation. You're going to get to a point where people are going to have to have staff in place to just deal with that one situation, just to keep up with what they're going to have to do to make sure they protect themselves. It's got to be costing us money or it's got to be costing us efficiency."*

For example, implementing automated analytics that trigger an alert whenever a doctor accesses a patient's record that has the same last name as the doctor's can involve so many people and processes that it could impact the overall performance of healthcare delivery. With regard to healthcare regulations, hospitals are facing major operational issues due to how healthcare policies are crafted. The challenges that healthcare leaders face regarding operational feasibility are weighed against the patient's best interests and, therefore, the impact privacy compliance. One privacy compliance officer stated:

> *"My biggest concern time again comes down to operational feasibility and whether what's being asked is either can be operationalized, or is it going to be detrimental to the patient's best interest, and there is balance, it really is."*

The above categories, and representative data for each of them, are presented in Appendix C.

4.2 Positive Impacts

We have identified three factors with regard to the positive impact of privacy safeguards: controlled access, deterrence effect, and tracking mechanisms.

Controlled Access: The enactment of technical privacy safeguards, such as role-based access control mechanisms, allowed for better control over who could access the system. Filtering out users who have no business looking at patients' data was a positive impact of privacy safeguard enactments, as commented by a healthcare executive: *"We have a role-based access, and that's very important, because you don't want to give employees any more access than what they need . . . So basically, what we do is we look at the information system and the duties of the employee and we base their access on that"*

Deterrence Effect: Informants emphasized the ability of a deterrence approach to create an environment of fear when rules are not followed. This fear was perceived as a positive impact, because it sets an example and deters other employees from inappropriately handling patients' information. A Chief Privacy Officer of a large hospital used an analogy to refer to how his organization benefits from a deterrence approach:

> *"It is sort of user grisly analogy. Back in medieval England when they chopped people's heads off, they would put [that] 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."*

Tracking Mechanisms: The ability to track the identity of the users who accessed what information along with when it was accessed was perceived by organizational leaders as a major positive impact of privacy safeguard enactments. One Chief Medical Information Officer stated:

> *"One of the nice things about EHRs is when somebody signs in, you know who signed in and what time where they are at [a record] . . . We have tracking mechanisms to be able to determine if I log into a chart and I go look at a nurse I work with it. Well the system really knows who I am looking at here. So if I am taking care of her [the nurse] as a patient in the emergency department. That would be clinically appropriate. If I have never seen her as a physician-patient relationship and I am looking at her chart, well that is completely inappropriate."*

The above categories and representative data for each of them are presented in Appendix D.

4.3 Imbalance Challenge

Capturing the imbalance challenge was a major finding in this study. The imbalance challenge is an analytical construct that was created to make sense of what organizations reported they are faced with as a result of enacting information privacy safeguards. As shown in Figure 3, an imbalance challenge occurs when the negative impacts of enacting privacy safeguards outweigh the positive ones. The challenge resides in the organizations' struggles in maintaining patient privacy and without inhibiting business processes. One privacy officer illustrated this imbalance challenge by stating:

> *"The biggest challenge with respect to privacy and health care in my mind is this notion that you have to err on the side of providing additional information access. You can't*

afford to put a barrier in front of a physician or clinician when they need to have access to the information."

The imbalance challenge is of great concern to healthcare privacy leaders, especially in light of upcoming regulations. This concern is illustrated by a chief privacy officer:

"*The federal law is toying with the idea of making sure that data at rest is encrypted. Not the movement of the data. In other words, if one of my hard drives would be encrypted and if somebody needs to get data unencrypted and pass it forward, that's going to be almost impossible to put in place. This is because none of the environments, none of the vendors have built their systems that way.*"

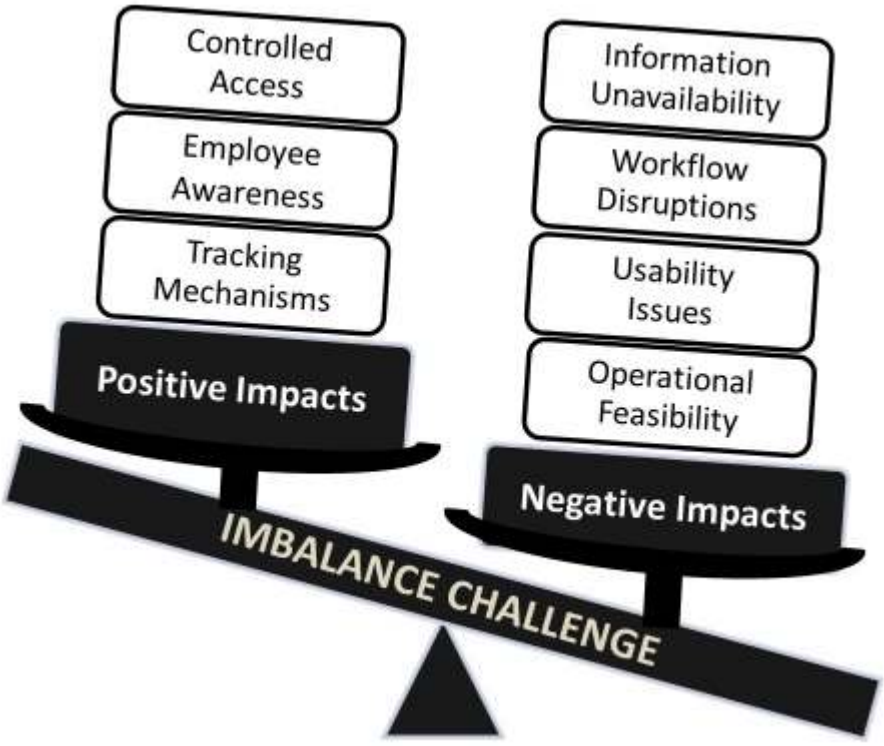

Figure 3 –The Imbalance Challenge

4.4 Organizational Context

The primary dimensions of organizational context that emerged from this study include hospital size, academic status, leader's educational background, and leadership commitment.

Hospital Size: Based on initial data gathering and analysis, large healthcare organizations are more likely to better respond to privacy issues than small ones, because they can afford to hire consultants to provide comprehensive assessments. Organization size has been positively related to adoption behaviors (Rogers 1995) and negatively related to regulatory compliance (Baron and Baron 1980). Large hospitals' perspectives on the effect of the hospital size was captured and illustrated by a Chief Privacy Officer from a large hospital:

> *"If you ask me if I think that the medium-to small-sized institutions did everything. I think they did what they thought they needed to do. I think their intentions were good, but I don't believe that they are as sophisticated. So it's probably the difference between when you hand your bank card to the local hair stylist, and you hope that they do a pretty good job with not losing your credit card information, versus handing your credit card to Citibank that has much more sophisticated systems and so on and so forth. You know there's some of that human error thing that comes into it, and a different mindset that comes into it."*

For large hospitals, the ability to properly respond to privacy threats is closely linked to available resources, which could be a major constraint for smaller hospitals. This argument translates into cutting corners and not hiring the appropriate entities to assist in interpreting the law. A privacy officer of a large hospital illustrated this viewpoint as follows:

"What many of the smaller and medium-sized institutions did was try to skimp and rather than hire a consultant or an attorney to help them where they didn't have the resources to allow them to (a) interpret the law, interpret HIPAA; (b) implement, operationalize it. What they did rather than hiring the appropriate people because they didn't have the resources to do so, was they tried to figure it out on their own and the one complaint that I have seen many times and I think HHS has gotten many complaints about this is companies misinterpreting HIPAA."

Interviewing informants from smaller hospitals helped to reveal a significant difference in opinion, since their responses clearly challenged the previous statement made by an informant based in a large hospital. This opposing view can be succinctly illustrated by statement made by a CEO of a small hospital: "*Because we're smaller and more contained, we may be able to control it a little better.*" Smaller hospitals look at the issues in terms of proportions: "*I'm thinking of Hospital X and you've been in that hospital probably. I mean there are so many points of access there, so many people and so many workstations and so much [is] happening and paper is everywhere. It may be more of a challenge for them to adhere to the standards than here at this little hospital*." Or in terms of HIPAA officers, "*I have one (HIPAA officer) person to worry about 120 employees. If you had 12,000 employees, to get that same ratio you'd have to have 100 HIPAA officers*."

Organization's Academic Status. Among the healthcare organizations interviewed, academic hospitals are associated with large hospitals and tied to medical schools and ongoing research about protected health information (PHI). These organizations have very well-established rules and IRBs with regard to PHI. Therefore, institutions with teaching hospitals have an existing culture of privacy practices. Healthcare organizations with academic affiliations showed

evidence of more awareness of privacy through stricter guidelines for medical students, resulting in expulsion from medical programs when patient's privacy guidelines were not observed properly. Teaching and research hospitals are also more aware of the secondary use of patient data.

Professional Background of Privacy Officers. Under the Health Insurance Portability and Accountability Act of 1996, every healthcare organization must designate a privacy officer. The data revealed that healthcare organizations comply with this provision mainly by adding this function to the list of duties performed by an existing employee. As one IT director stated: "*We have privacy officers . . . none of our privacy officers are full time, meaning they have other jobs*." The privacy informants, though they performed similar functions as privacy leaders, had different business and/or educational backgrounds, which could have affected their business vision of how privacy responses should be handled. It is worth noting that while the educational background could have impacted the weight of one type of safeguards versus another, in the end, what mattered was how much they were involved in protecting patients' information.

Leadership Commitment. The aforementioned findings triggered a theoretical sampling for the purpose of pursuing a potential pattern related to the hospital's size and its academic status (teaching, non-teaching). The findings showed that regardless of a hospital's size, culture seems to determine the attitude toward information privacy safeguards and the organizations' actions, regardless of its resources. Furthermore, the commitment from the top management appeared to transcend the limited resources in small hospitals. For example, while large hospitals hire consultants to assess and review their processes and technologies, smaller hospitals can be very creative in accomplishing the same objective with much smaller budgets. One Chief Privacy Officer commented on leadership commitment:

"*If you don't have that [buy-in from leadership], no matter what you implement, you are not going to have the resources in the first place.*"

The above categories and representative data for each item in the organizational context are presented in detail in Appendix E.

5. EMERGING THEORETICAL FRAMEWORK

This section presents the theoretical framework grounded by the findings from the empirical study with support from the relevant extant literature. This study led to the emergence of major categories: the enactment of privacy safeguards, negative and positive impacts, the imbalance challenge, and privacy compliance. Close analysis of the data revealed interrelations among these categories and allowed for their integration into a theoretical framework (Strauss et al. 1998). These major categories are found within both the IS and health informatics communities, yet they are very seldom interconnected in the literature. We present a theoretical framework that unifies these concepts and thereby contributes to the explanation of the consequences of privacy safeguards' enactment and the cause of the imbalance challenge.

In using grounded theory, Urquhart (2010) emphasized leveraging a systematic and iterative approach to theory conceptualization. Embracing this approach enabled further analysis of the negative impacts. We pursued a theoretical sampling in an attempt to increase our knowledge of the intended and unintended consequences of privacy safeguards' enactment, their impact on business practices, and their implications for privacy compliance.

Further analysis allowed us to distinguish between: (1) organizations where leaders were not aware of the negative impacts, and (2) organizations that were aware of the negative impacts and accounted for the imbalance challenge in how they responded to privacy threats. In fact,

when asked how they measured the effectiveness of their safeguards, former organizations indicated that there were no formal metrics in place to assess the impacts, positive or negative, of their privacy safeguards' implementation. Instead, they relied on the number of complaints, or reported breaches, as an indication of the effectiveness of their safeguards. Once these organizations became aware of the negative impacts, they considered revisiting their safeguards to account for the imbalance challenge. In these instances, awareness only happened when privacy compliance became an issue. If the organizations' privacy compliances were not in jeopardy, would they ever become aware of any negative impacts? Additional analysis revealed that organizations that were aware of the negative impacts had performed some sort of risk assessment. Such initiatives allowed organizations to look out for these impacts and sometimes to prevent or minimize them. Ultimately, a proactive assessment versus a reactive approach seems to distinguish these two types of organizations and further explains the imbalance challenge. Indeed, organizations with a proactive approach are trying to develop their metrics to assess negative impacts. Relationships between the imbalance challenge, privacy safeguards, impacts, and privacy compliance are depicted using propositions in Figure 4.

When considering the relationship between privacy safeguards and the imbalance challenge, the study revealed that the implementation of privacy safeguards does not necessarily lead to positive impacts. We draw attention to the negative impacts that were not unnoticed to healthcare leaders. On the contrary, organizations face major challenges when they became aware of negative impacts. This study allowed for distinctions between: (1) organizations where leaders were not aware of the negative impacts and (2) organizations where leaders were aware of the negative impacts and accounted for the imbalance challenge in their responses to privacy threats. In fact, when asked how they measured the effectiveness of their safeguards, these

organizations indicated that there were no formal metrics in place to assess the impacts, positive or negative, of their privacy safeguards' implementation. Instead, they relied on the number of complaints, or reported breaches, as an indication of the effectiveness of their safeguards. Once these organizations became aware of the negative impacts, they considered revisiting their safeguards to account for the imbalance challenge. In these instances, awareness only happened when privacy compliance became an issue. If their privacy compliance were not in jeopardy, would they ever become aware of other negative impacts? A further analysis revealed that organizations that were aware of the negative impacts had performed some sort of risk assessment. Such initiative allowed organizations to look out for the negative impacts, sometimes to prevent them or at least to minimize them. Ultimately, a proactive assessment versus a reactive approach seems to distinguish these two types of organizations, and further explains the imbalance challenge.

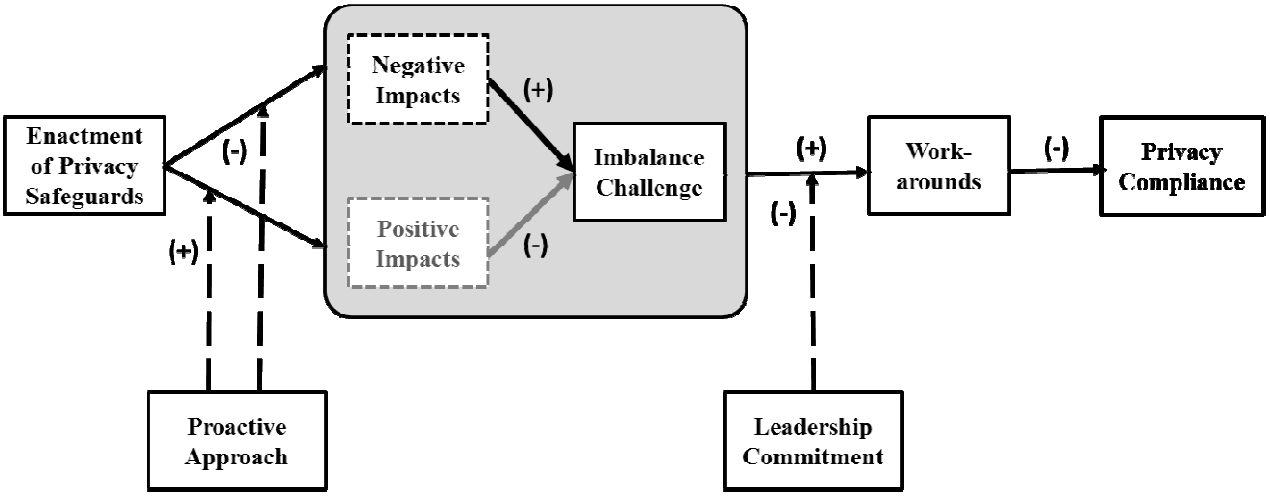

Figure 4 –Emerging Theoretical Framework of the Imbalance Challenge

Note: *An imbalance challenge results ONLY if the negative impacts outweigh the positive ones. Ideally, an organization would want to minimize the negative impacts and enhance the positive ones.*

Recognizing the state of imbalance in which negative impacts overpower positive impacts constitutes a strong conceptual foundation of the upshot of a privacy safeguard in healthcare organizations.

In this study, awareness is linked with how proactive a hospital is in handling the threats and the controls. Whereas proactive organizations are capable of identifying and acting upon the negative impacts of enacting privacy safeguards, reactive organizations become aware much later (i.e. when privacy complaints or breaches are reported). A priori awareness of potential negative impacts allows for the implementation of the appropriate safeguards, to minimize the negative impacts and maximize the positive impacts. Therefore, we propose:

> **Proposition 1:** In the absence of a proactive approach, the implementation of privacy safeguards is more likely to lead to: a) a higher degree of negative impacts and b) a lower degree of positive impacts.

With regard to the first research question on the positive and negative business impacts in implementing information privacy safeguards, the findings identified more factors than those exhibited by the literature. Healthcare leaders provided many examples in terms of how they implemented privacy protective safeguards and how they were mindful of the negative impacts associated with these safeguards. But in discussing the negative impacts on practices, factors that were positively impacting healthcare practices were also identified.

5.1 Effect of Positive and Negative Impacts on the Imbalance Challenge

Organizations implement privacy safeguards for the purposes of mitigating information privacy threats and ensuring legal compliance. However, much of the research on privacy

safeguards assumes a positive impact where the sequels of post implementation (negative impact) are often overlooked. In this research, the emergence of negative impacts was an important concept. These types of impacts tend to negatively shift the organizations' desired balance. For example, we expect the unavailability of information needed to treat a patient to create an environment of an imbalance challenge between protecting patient information and treating the patient. Similarly, disruptions in workflow, usability, and operational issues are slowing down healthcare delivery. Ideally, an organization will want to minimize the negative impacts and enhance the positive ones. This is because healthcare organizations seek to achieve both protection of patients' information and regulatory compliance. In doing so, they implement privacy safeguards in order to minimize privacy breaches and abide by regulatory pressures.

Based on these findings, we suggest that although a higher degree of negative impacts of adopting privacy safeguards lead to a higher degree of imbalance, organizations leverage the positive impacts of adopting privacy safeguards to further minimize the negative impacts. Therefore, the following proposition and its sub-propositions are suggested:

Proposition 2: An imbalance challenge will result if the negative impacts outweigh the positive ones. After an imbalance challenge occurs:

Proposition 2a: A higher degree of negative impacts leads to a higher degree of imbalance challenge.

Proposition 2b: A higher degree of positive impacts leads to a lower degree of the imbalance challenge.

The data revealed that the implementation of information privacy protective safeguards is impacting healthcare work practices through positive and negative impacts and thus creating the imbalance challenge. Achieving a balance in privacy and utility by maximally reducing negative impacts was challenging because of the dynamic environment surrounding healthcare delivery. The dynamics inherent in medical practices, such as scheduled and unscheduled patient visits, clinicians' unscheduled shifts, and workforce needed at unexpected times and locations, often conflicted with privacy role-based access safeguards (Boxwala et al. 2011) and therefore made the imbalance challenge even more important. The positive impact of privacy protective safeguards may function as a facilitator to privacy compliance, while negative impacts may function as inhibitors. Identifying these impacts is not enough. Healthcare leaders must also address the imbalance challenge that ultimately defines the level of their privacy compliance. In the section below, we will address the second research question on the outcomes of the imbalance challenge.

5.2 Effect of the Imbalance Challenge on Privacy Compliance

The findings suggest that the issues surrounding the organizational struggles to meet the ever-increasing privacy constraints and to comply with regulatory requirements have become a central concern to healthcare leaders. In particular, the imbalance challenge emerged as the key concept with regard to these struggles. An unattended imbalance challenge can potentially be harmful to the organization's privacy compliance. This study provides evidence that healthcare professionals may see a need to improvise or work around privacy safeguards. Existing health informatics literature describes workarounds as clever alternative methods developed by the users to accomplish what the system does not easily allow them to do (Ash et. al., 2004). Morath and Turnbull (2005) define workarounds as ‘‘work patterns an individual or a group of

individuals create to accomplish a crucial work goal within a system of dysfunctional work processes that prohibits the accomplishment of that goal or makes it difficult'' (p. 52). Workaround has been recognized in both IS and health informatics literature (Pollock 2005), however limited studies theorize this concept (Halbesleben et al. 2008), especially with regard to information privacy.

This study provides three themes with regard to workarounds: conditions leading to workarounds, evidence of these workarounds, and concerns and potential consequences of these workarounds. These themes are summarized in Figure 5.

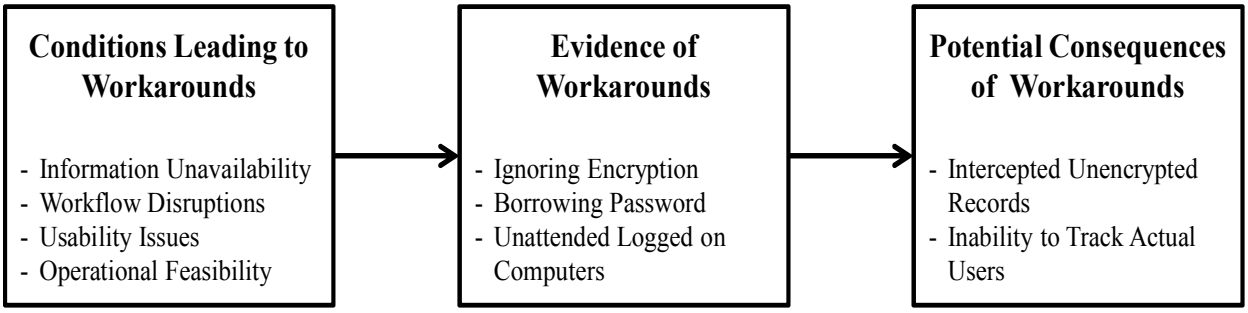

Figure 5 – Model of Workarounds

Healthcare professionals seek to balance privacy demands with the need to provide care for their patients, all in an efficient manner. This study provides evidence of the struggles that privacy leaders face as the effects of the imbalance challenge. A striking example was provided by a Chief Privacy Officer who stated that clinicians sometimes bypass privacy safeguards to do their job, which involves saving lives. He emphasized that he would rather explain the office of civil rights why one of the hospital's employee inappropriately accessed information (e.g., used someone else's log in credentials) rather than explain to a family that he could not save their loved one because of privacy safeguard enactments. The concern surrounding such action is the

possibility that the same access that saved lives could hinder privacy compliance. The same Chief Privacy Officer referred to the case of the Arizona Representative who was admitted to a hospital after being shot, and how several employees lost their jobs for inappropriately looking up her medical records.

This study provides evidence, with support from the literature, that when negative impacts outweigh positive impacts, healthcare professionals may see a need to improvise or workaround their work practices. For example, information unavailability can be circumvented by users borrowing passwords or smart cards to access records that they are not authorized to access (France 1998). They may also ignore required encryption mechanisms because of their impact on job performance. The potential harm resides in the subsequent use of patients' information (e.g., copying, transmitting) under different users' log-ins. In light of these struggles and the imbalance challenge, organizations will continue to face breaches, because their programs are not effective and are not accounting for these tensions (Culnan and Williams 2009). Thus, we propose that workarounds act as mediators between the imbalance challenge and privacy compliance. This leads to the following propositions:

Proposition 4: The stronger the imbalance challenge, the higher the frequency of workarounds will occur.

Proposition 5: The higher the frequency of workarounds, the lower the degree of organizational privacy compliance.

5.3 Effect of Leadership Commitment on the Imbalance Challenge

This study has unveiled how organizations differently handle the imbalance challenge through the amount of support they receive from their top management. At an early stage of our analysis, we expected the hospital size to dictate the degree of commitment to compliance. In other words, we expected to find that larger hospitals with more resources would strive to achieve a higher degree of privacy compliance and better address imbalances issues. We further analyzed that pattern to discover that, while the hospital size matters because it is often closely linked with resources, it is the commitment of top managers that prevails. Prior research found that top executives' values and commitments influence organizational outcomes and impacts, because these executives hold the powers to influence organizational actions (Finkelstein and Hambrick 1990). As a result, top management would invest in privacy programs to demonstrate their commitments to the impact of these programs. Top management support emerged as an essential element impacting the level of privacy compliance. In this study, when clinicians could not access the records they needed, policies were reviewed by the healthcare leaders and a "break-the-glass" feature was created to allow clinicians to bypass access controls. The absence of leadership commitment to privacy posed ethical conflicts for employees in charge of day-to-day privacy behaviors (Smith 1993). Therefore, a commitment from the leadership is important to the success and more positive impact of privacy safeguards (Culnan and Williams 2009). Therefore:

> **Proposition 6:** With stronger leadership commitment, the proposed positive association between the degree of the imbalance challenge and the frequency of workarounds will be weaker.

5.4 Relating the Imbalance Challenge to the Literature

This section attempts to compare the categories and relationships of the theoretical framework of the imbalance challenge with those from related literature.

When relating the imbalance challenge to the literature, we applied the lens of balance theory to seek an explanation for the contradictory positive and negative impacts and the imbalance challenge. According to Heider (1946) and Lewin (1951), Balance Theory is viewed as a structural arrangement between social actors and affective ties. If these arrangements create an imbalance (tension or strain), actors will take actions to reduce this imbalance. For example, as a result of discomfort in a relationship, an actor may take a detachment action. Contrary to the balance theory's expectation of detachment, our data found that once healthcare leaders became aware of negative impacts, they worked on resolving those negative impacts rather than distancing themselves. In situations where privacy safeguards were in the way of healthcare delivery, healthcare leaders increased their involvement rather than reduced it. For example, when needed information was not available to clinicians, policies were reviewed by leaders and a "break-the-glass" feature was created to allow clinicians to bypass access controls. Also, because of the penalties associated with breaches, organizations could not afford to avoid taking actions.

The opposing concepts of negative and positive impacts of the imbalance challenge led us to consider the privacy calculus theory in the privacy literature (see Culnan and Bies 2003 for a review). This theoretical framework has been applied at the individual level (e.g., Dinev and Hart 2006; Xu et al. 2010) and provides insights that are worth taking into account at the organizational level. Privacy calculus considers two sets of opposing factors: inhibitors and facilitators to behavioral intentions (such as willingness to conduct online transaction or intention to disclose information). A user's decision to transact online is based on the outcome of

weighing both sets of factors: if the effects of the facilitating factors (i.e., trust and control) are greater than those of inhibiting factors (i.e., privacy concerns and perceived risk), the user is more likely to engage in an eCommerce transaction. While the individual user has to make a priori decisions, the theoretical model of the imbalance challenge pertains to consequences of these decisions at the organizational level. Moreover, the privacy calculus allows the individual user to "calculate" if it is beneficial or not to engage in an online transaction, whereas in the theoretical model of the imbalance challenge, organizations do not "calculate," but rather deal with the consequences, which is the imbalance challenge. The imbalance challenge results from negative impacts outweighing positive impacts.

Theoretically speaking, we view the imbalance challenge as an important addition to the theoretical framework. Recognizing the state of imbalance in which negative impacts overwhelm positive impact constitutes a strong conceptual foundation of the impact of privacy safeguards' implementation.

The two research questions investigated in this study directed our attention to the importance of negative impacts that cause the imbalance challenge when it comes to organizational privacy compliance. In considering potential solutions for the complex issue of the imbalance challenge, it is imperative to consider these challenges in light of risk management. Consequently, we argue for a proactive approach that could prevent or at least lessen the negative impacts – a Privacy Impact Assessment (PIA). Previous studies defined the PIA as a risk management tool used to assess the use of privacy safeguards (Culnan and Williams 2009). The PIA is advocated by several federal agencies. The U.S. Department of Homeland Security utilizes the PIA as a decision-making tool designed 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 to promote the PIA as an assessment mechanism for evaluating the level of the patients' information protection (HHS 2011b). Therefore, we believe that there is a reasonable potential for transferability of the PIA approach from the federal level to other levels, such as the organizational level (i.e., hospitals). And it is essential to simultaneously assess the privacy risks and potential business impacts (Parks et al. 2011b). We believe that a better understanding of the PIA will further enhance the theoretical and practical understanding of privacy safeguards and, more importantly, their potential negative impacts on healthcare delivery processes.

6. DISCUSSION AND IMPLICATION

This study aims to contribute to existing privacy research in several ways. First, our primary contribution is to respond to the compelling call for research investigating the effectiveness and consequences of enacting privacy safeguards (Belanger and Crossler, 2011). To date, most studies on privacy focus on designing and implementing the appropriate safeguards to mitigate information privacy threats, and there has been a notable lack of research on the outcomes of privacy safeguards enactments. Our emerging theoretical framework highlights the importance of the analytical construct we developed–the Imbalance Challenge–to capture the unintended consequences caused by the situation where the negative impacts of privacy safeguards outweigh the positive ones. Analyzing these opposing impacts is important, because it enables us to assess and account for their implications for work practices and for privacy compliance.

Second, this research provides new theoretical insights into understanding privacy management by targeting the organizational level of analysis through a grounded theory

approach. In the IS field, Smith et al. (2011, p. 1006) have made an explicit call for research on studying information privacy at the organization level:

> *"Indeed, most rigorous studies of organizational privacy policies and practices would likely include a set of exhaustive interviews with an organization's members and stakeholders, and some amount of deep process tracing would also likely be involved. Such studies are the best approach to uncovering the somewhat subtle organizational dynamics that drive privacy policies and practices."*

Methodologically, using a grounded theory provides a rich lens through which to understand the consequences of privacy safeguards enactments and their implications for privacy compliance. Grounded theory methodology was selected because of the lack of existing theory to explain how organizations interpret the implications of privacy safeguard enactments, the contextualization of the healthcare domain, practical relevance, and suitability to study healthcare processes. Based on a grounded theory study spanning over 16 months in which we were able to interview thirty privacy leaders from several healthcare organizations, including the government, the study uncovered subtle organizational dynamics that would not have emerged through quick data collection techniques such as online surveys. The ability to revisit the interview questions and the target population to include more pertinent questions and participants was crucial for reaching saturation, where all concepts are well defined and no new concepts emerge (Corbin and Strauss, 2008).

The findings of this study have useful practical implications for healthcare organizations in general and hospitals in particular. The emergence of the imbalance challenge provides a clearer understanding of the unintended consequences of privacy safeguard enactments and their implications for the organization's overall privacy compliance.

This study is evaluated through Strauss and Corbin (1998) and Corbin and Strauss (2008) eight evaluative criteria for the empirical grounding (Appendix F) and seven criteria for judging a grounded theory research process (Appendix G).

There are several limitations of the study. With regard to the validity of the emerging theory, it is worth referring to generalizability, which is "the validity of a theory in a setting different from the one where it was empirically tested and confirmed" (Lee et al. 2003, p. 221). Lee and Baskerville clarified that the appropriate type of generalizability (not just statistical) should be applied to this particular type of study. The purpose of this study was not to achieve statistical validation, but rather to discover patterns for the purpose of theory building and gaining a better understanding of the main issues in its context. It is reasonable to assume that the insights of the emerging framework would guide future research to a more formal theory (Orlikowski 1993).

This work creates numerous future research opportunities. First, our study was conducted with the objectives of examining and identifying the factors that impact the imbalance challenge at the organizational level. Hence, there is an opportunity to research this imbalance impact from an individual level of analysis. Indeed, employees have different stakes in the organization based on their employment status (full-time/part-time, contract/permanent, staff/management) that could impact how receptive they are to privacy safeguards. Second, the findings show that hospitals are taking different attitudes toward the imbalance challenge, based on their top management commitment. Therefore, a second research opportunity is to further examine the correlations among leadership style and negative impacts. Doing so could facilitate the development of programs supported by executive to effectively act on the imbalance challenge. Finally, the findings are based on the U.S. hospitals, and some IS researchers demonstrated that

there were differences in information privacy issues across countries and cultures (Bellman et al. 2004; Milberg et al. 2000). Therefore, a third research opportunity could be a comparative study of the factors impacting this imbalance, while taking into consideration the cultural influences.

7. CONCLUSION

Recent literature suggests that the most existing information privacy research focuses on the enactment of privacy safeguards and neglects the actual outcomes of the practices in which organizations engage. This study focuses on understanding the imbalance challenge between privacy requirements and healthcare business practices by identifying the positive and negative impacts. This research responds to a theoretical challenge that was overlooked in prior research, and it makes the following essential contributions: 1) it introduces a theoretical model of the imbalance challenge that accounts for negative impacts of privacy safeguards, 2) it identifies the opposing impacts of privacy safeguards and the importance of the imbalance challenge, 3) it explores the imbalance implications for privacy compliance, and 4) it discovers an important correlation between how effectively organizations handle the imbalance challenge and how much support they receive from top management. Finally, the study argues for a privacy impact assessment (PIA) as a proactive solution to handle the imbalance challenge. The PIA allows organizations to simultaneously assess privacy risks and practical impacts. As a result, organizations will be able to better understand and handle the imbalance challenge and ultimately achieve a better compliance without impeding their healthcare practices.

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.

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.
Ash, J.S., Berg., and M., C., E. "Some Unintended Consequences of Information Technology in Health care: The Nature of Patient Care Information System-Related Errors," *Journal of the American Medical Informatics Association* (11) 2004, pp 104–112.
Bakker, A. 1998. "Security in Perspective; Luxury or Must?," *International Journal of Medical Informatics* (49:1), pp 31-37.
Belanger, F., and Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *Management Information Systems Quarterly* (35:4), pp 1017-1041.
Bellman, S., Johnson, E.J., Kobrin, S.J., and Lohse, G.L. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *The Information Society* (20:5), pp 313-324.
Benitez, K., and Malin, B. 2010. "Evaluating Re-Identification Risks with Respect to the Hipaa Privacy Rule," *Journal of the American Medical Informatics Association* (17:2), pp 169-177.
Bennett, J.L. 1984. "Managing to Meet Usability Requirements: Establishing and Meeting Software Development Goals," in: *Bennet, J., Case, D., Sandelin, J., Smith, M. (Eds.), Visual Display Terminals.* . Prentice-Hall, Englewood Cliffs, NJ, pp. 161-184.
Blobel, B., Nordberg, R., Davis, J.M., and Pharow, P. 2006. "Modeling Privilege Management and Access Control," *International Journal of Medical Informatics* (75:8), pp 597-623.
Bourgeois, F.C., Taylor, P.L., Emans, S.J., Nigrin, D.J., and Mandl, K.D. 2008. "Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients," *Journal of the American Medical Informatics Association* (15:6), pp 737-743.
Boxwala, A.A., Kim, J., Grillo, J.M., and Ohno-Machado, L. 2011. "Using Statistical and Machine Learning to Help Institutions Detect Suspicious Access to Electronic Health Records," *Journal of the American Medical Informatics Association* (18:4), pp 498-505.
Boyd, A.D., Hosner, C., Hunscher, D.A., Athey, B.D., Clauw, D.J., and Green, L.A. 2007. "An 'Honest Broker' Mechanism to Maintain Privacy for Patient Care and Academic Medical Research " *International Journal of Medical Informatics* (76:5-6), pp 407-411.
Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *Management Information Systems Quarterly* (34:3), pp 523-548.
Chen, K., Chang, Y.C., and Wang, D.W. 2010. "Aspect-Oriented Design and Implementation of Adaptable Access Control for Electronic Medical Records," *International Journal of Medical Informatics* (79:3), pp 181-203.
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.
Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. 2006. "Challenges Associated with Privacy in Health Care Industry: Implementation of Hipaa and the Security Rules," *Journal of Medical Systems* (30:1), pp 57-64.

Coiera, E., and Clarke, R. 2004. "E-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment," *Journal of the American Medical Informatics Association* (11:2), pp 129-140.
Croll, P.R. 2010. "Determining the Privacy Policy Deficiencies of Health Ict Applications through Semi-Formal Modelling," *International Journal of Medical Informatics*).
Culnan, M., and Williams, C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and Tjx Data Breaches," *MIS Quarterly* (33:4), pp 673-687.
Culnan, M.J., and Bies, R.J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Contemporary Perspectives on Privacy: Social, Psychological, Political* (59:2), pp 323-342.
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."
Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp 61-80.
Eisenhardt, K.M. 1989. "Building Theories from Case Study Research," *The 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.
Finkelstein, S., and Hambrick, D.C. 1990. "Top-Management-Team Tenure and Organizational Outcomes: The Moderating Role of Managerial Discretion," *Administrative Science Quarterly* (35:3), pp 484-503.
Flores Zuniga, A.E., Win, K.T., and Susilo, W. 2010. "Biometrics for Electronic Health Records," *Journal of Medical Systems* (34:5), pp 975-983.
France, Francis H.R.,1998."Ethics and biomedical information" *International Journal of Medical Informatics* (49:1)pp 111-115
Glaser, B.G., and Strauss, A.L. 1967. "The Discovery of Grounded Theory: Strategies for Qualitative Research," *New York: Aldine de Gruyter*).
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.
Halbesleben, J.R.B., Wakefield, D.S., and Wakefield, B.J. 2008. "Work-Arounds in Health Care Settings: Literature Review and Research Agenda," *Health Care Management Review* (33:1), p 2.
Heider, F. 1946. "Attitudes and Cognitive Organization," *The Journal of Psychology* (21:1), pp 107-112.
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/,").
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.

Johnson, C.M., Johnson, T.R., and Zhang, J. 2005. "A User-Centered Framework for Redesigning Health Care Interfaces," *Journal of Biomedical Informatics* (38:1), pp 75-87.
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.
Lee, A.S., and Baskerville, R.L. "Generalizing Generalizability in Information Systems Research," *Information Systems Research* (14:3) 2003, pp 221-243.
Lewin, K. 1951. "Field Theory in Social Science: Selected Theoretical Papers (Edited by Dorwin Cartwright.),").
Li, X.B., and Sarkar, S. 2010. "Data Clustering and Micro-Perturbation for Privacy-Preserving Data Sharing and Analysis," *ICIS 2010 Proceedings.* .
Liu, C., and Arnett, K.P. 2002. "Raising a Red Flag on Global Www Privacy Policies," *Journal of Computer Information Systems* (43:1), pp 117-127.
Lovis, C., Spahni, S., Cassoni, N., and Geissbuhler, A. 2007. "Comprehensive Management of the Access to the Electronic Patient Record: Towards Trans-Institutional Networks," *International Journal of Medical Informatics* (76:5-6), pp 466-470.
Marohn, D. 2006. "Biometrics in Healthcare," *Biometric Technology Today* (14:9), pp 9-11.
Milberg, S.J., Smith, H.J., and Burke, S.J. 2000. "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), pp 35-57.
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.
Morath, J.M., and Turnbull, J.E. "To Do No Harm: Ensuring Patient Safety in Health Care Organizations," Jossey-Bass Inc Pub, 2005.
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.
Orlikowski, W.J. "CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development," *MIS Quarterly* (17:3) 1993, pp 309-340.
Parks, R., Chu, C., and Xu, H. 2011a. "Healthcare Information Privacy Research: Issues, Gaps and What Next," *Proceedings of the 17th Americas Conference on Information Systems (AMCIS)*, Detroit, MI.
Parks, R., Chu, C., Xu, H., and Adams, L. 2011b. "Understanding the Drivers and Outcomes of Healthcare Organizational Privacy Responses," *Proceedings of the 32nd Annual International Conference on Information Systems (ICIS)*, Shanghai, China
Patel, V.L., Arocha, J.F., and Shortliffe, E.H. 2000. "Cognitive Models in Training Health Professionals to Protect Patients' Confidential Information," *International Journal of Medical Informatics* (60:2), pp 143-150.
Peleg, M., Beimel, D., Dori, D., and Denekamp, Y. 2008. "Situation-Based Access Control: Privacy Management Via Modeling of Patient Data Access Scenarios," *Journal of Biomedical Informatics* (41:6), pp 1028-1040.
Peslak, A.R. 2006. "Internet Privacy Policies of the Largest International Companies," *Journal of Electronic Commerce in Organizations* (4:3), pp 46-62.
Pollock, N. 2005. "When Is a Work-Around? Conflict and Negotiation in Computer Systems Development," *Science, Technology & Human Values* (30:4), pp 496-514.

PRC. 2012. "Http://Www.Privacyrights.Org/Data-Breach." Privacy Rights Clearinghouse.
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.
Reni, G., Molteni, M., Arlotti, S., and Pinciroli, F. 2004. "Chief Medical Officer Actions on Information Security in an Italian Rehabilitation Centre," *International Journal of Medical Informatics* (73:3), pp 271-279.
Salomon, R.M., Blackford, J.U., Rosenbloom, S.T., Seidel, S., Clayton, E.W., Dilts, D.M., and Finder, S.G. 2010. "Openness of Patients' Reporting with Use of Electronic Records: Psychiatric Clinicians' Views," *Journal of the American Medical Informatics Association* (17:1), pp 54-60.
Shackel, B. 1984. "The Concept of Usability. ," in: *Bennet, J., Case,D., Sandelin, J., Smith, M. (Eds). Visual Display Terminals.* . Prentice-Hall, Englewood Cliffs, NJ, pp. 45-87.
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, E., and Eloff, J.H.P. 1999. "Security in Health-Care Information Systems--Current Trends," *International Journal of Medical Informatics* (54:1), pp 39-54.
Smith, H.J. 1993. "Privacy Policies and Practices: Inside the Organizational Maze," *Communications of the ACM* (36:12), pp 104-122.
Smith, J.H., Dinev, T., and Xu, H. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4) 2011, pp 989-1015.
Stahl, B.C., Doherty, N.F., and Shaw, M. 2011. "Information Security Policies in the Uk Healthcare Sector: A Critical Evaluation," *Information Systems Journal* (22:1), pp 77-94.
Strauss, A.L., and Corbin, J.M. 2008. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* 3rd Ed. Newbury Park, CA: Sage.:
Sujansky, W.V., Faus, S.A., Stone, E., and Brennan, P.F. 2010. "A Method to Implement Fine-Grained Access Control for Personal Health Records through Standard Relational Database Queries," *Journal of Biomedical Informatics* (43:5), pp S46–S50.
Tjora, A., Tran, T., and Faxvaag, A. 2005. "Privacy Vs Usability: A Qualitative Exploration of Patients' Experiences with Secure Internet Communication with Their General Practitioner," *Journal of medical internet research* (7:2), p e15.
Urquhart, C., Lehmann, H., and Myers, M.D. 2010. "Putting the 'Theory' Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information Systems Journal* (20:4), pp 357-381.
van der Linden, H., Kalra, D., Hasman, A., and Talmon, J. 2009. "Inter-Organizational Future Proof Ehr Systems: A Review of the Security and Privacy Related Issues," *International Journal of Medical Informatics* (78:3), pp 141-160.
Vroom, C., and Von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23:3), pp 191-198.
Whitman, M.E., and Mattord, H.J. 2004. "Making Users Mindful of It Security," *Security Management* (48:11), pp 32-35.
Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp 135-174.

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, M., Smith, S.W., and Nicol, D.M. 2005. "The Performance Impact of Bgp Security," *IEEE Network* (19:6), pp 42-48.

Appendix A

Interview Protocol

The protocol for interviewing information privacy informants followed the following five steps:
Step1: The first author explained in detail the purpose of the study, confidentiality of the data collected and the option to opt out and/or not respond to questions they judged sensitive.
Step 2: We use semi-structured interviews format. Sample questions related to this particular study are listed below:

- What types of measures does your organization have in place to handle the threat of privacy issues? Were you subject to ant data breach?
- Are there any implementation/impact issues of these measures?
- What type of business conflicts (workflow conflicts) does you organization face in developing and enacting these privacy programs?
- How does your organization balance between its day-to-day operations and privacy policies' implementation?

Step 3: The first author recorded and transcribed all interviews
Steps 4: Following each interview, we documented impressions and patterns
Steps 5: We reviewed recordings and transcripts which led to more detailed questions with subsequent interviews

Appendix B

Semi –Structured Interview Questions

This study is part of a dissertation work completed by the first author. Questions have been expanded as new categories emerged. Not all questions pertain to this study.

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 Implementation Issues/ Practices/Enactment

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 is 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?

6. Concluding Questions

a. Are there other issues related to privacy programs that we haven't discussed but that would be important for me to know?

Appendix C

Illustrative Supporting Data for Negative Impacts

2nd Order Themes	Illustrative 1st Order Data
Information Unavailability	"We don't want to keep information out of the hands of people who need it. So if we develop something that is too stringent…they can't do their job the right way." "One of the challenges with my area is when we try to secure the information but yet our healthcare providers need quick access to it. So there's always kind of a fine line there. We try to make it as accessible as possible but yet have security measures in place to protect those assets." "We have lots of policies and everybody else has lots of policies but we can't meet the regulations in the strictest letter of the law and offer clinicians their ability to practice in an efficient cost effective manner." "I would much rather happen to explain to the office of civil rights why some body inappropriately access information than explain to a family why their loved one is dead and they wouldn't have been dead had the information we had in our possession wasn't accessible to the people treating that patient"
Workflow Disruption	"If the security is too hard, people wouldn't do it. If it is beyond their work flow much, they won't do it." "I tell people all the time that security flies in the face of convenience that's just the way it's always is… so a lot of push back or complain." "Do you want me not to administer that medication because everything didn't line up in the security behind the scenes?" "Once I log in, I don't want the system to log me out automatically. I don't like it. " "Time out features. There's times out in all our system end this is something we have to work around. You know we have some key systems in the emergency department and what they're saying … We have a twenty minute time out feature … if I'm a doctor in the emergency room and my system times out on me while I am critically working on a patient … I have to [enter] my password, that's not a good thing." "I'm using application A, application B and you get all these passwords you got to remember. Guess what? I'm going to start writing them down. " "40% of the work that a nurse does is to administer medication. 40% of her day, she is looking at pills and administering them. … she is logging in and

	waiting, waiting, waiting, waiting, that's a problem she is not going to get her job done. It's hard enough to do the charting, administering medicine without the waiting, waiting, waiting, waiting, waiting. So what most hospitals do is there have these computers on wheels, they wheel it into the patient room and they leave it logged on and they administer the medicine and they wheel it out and they leave it logged on and then they go into the next room and then leave it logged on but when they go back to the med room it's logged on and that's a security risk."
Usability Issues	"It comes from EHR usability and access to information. I mean in certain scenarios, I would like to walk in from purely a clinician hat on, I like to walk into to room and see that patient' information , talk with that patient and provide the care .but somehow I have to be acknowledge as being allowed to see that information. So, that one of the conflicts. I have to log in or else I have to use an RFID tag or swipe something to get into that record. " "With the privacy and security in healthcare it's the need for speed. I don't want to log in twice. I don't want to log in this, I don't want to that." "If it is not usable to them, they won't use it. and the things that are very usable to them, that they are used to, they can, I've seen this all the time."
Operational Feasibility	"My biggest concern time again comes down to operational feasibility and weather what's being asked is either can be operationalized or is it going to be detrimental to the patient best interest." "It really comes down to practice." "There is a lot of indirect impact that you have to be careful of its operational efficiency you know you have to really look at, you will never get a number you look and say oh my God. It's got to be costing us money or it's got to be costing us efficiency." "So it does have an impact on resources and operation. You're going to get to a point where people are going to have to have staff in place to just deal with that one situation, just to keep up with what they're going to have to do to make sure they protect themselves.. It's got to be costing us money or it's got to be costing us efficiency." "Let's just say for example, your brother is Don Parks and you are a physician, and you are looking up Don Parks records for no reason what so ever. An alert is triggered and will be sent to someone who actually sponsors your account. It is going to say Rachida Parks looked at Don Parks' record. The person that sponsors you will need to get with you and say who is that? You might say that is my brother, and one might say, why did you look at that record? You would say he was not looking good at the family dinner last week, so I looked up his record, which will be totally inappropriate. Or you could say, Don parks is not related to me, but is a patient of mine. The alerting provokes the next level of inquiry. If you were to say the former where you

	were looking up at your brother's record and you didn't really have a reason to, then that gets referred to the human resources for discipline." "We got to make sure the things are operationally supportable and I have to say that there are aspects of HIPAA that are very difficult to operationalize and they really often don't have a lot of meaning either." "We have lots of policies and everybody else has lots of policies but we can't meet the regulations in the strictest letter of the law and offer clinicians their ability to practice in an efficient cost effective manner." "My biggest concern time again comes down to operational feasibility and weather what's being asked is either can be operationalized or is it going to be detrimental to the patient best interest and there is balance, it really is."

Appendix D

Illustrative Supporting Data for Positive Impacts

2nd Order Themes	Illustrative 1st Order Data
Controlled Access	"We do have role based security, if we decided that you should have rights to getting at certain class of data, we can give it you.. .That's very important because you don't want to give employees any more access than what they need." "Basically what we do is we look at the information system and based on the security capabilities and the information system and the duties, or the responsibilities or the duties of the employee, we, we give, we base their access on that." "we go through our due diligence in regard to what different provider groups are allowed to see or should be able to see for their job , they don't want to stop them from providing care for patients obviously and you want to facilitate their care for patients but do you really have a true clinic need to be able to do that." "So do you want the environmental health worker to be able to log in to your record and see that? Well no, but there may be component of your records that are important to the environmental health workers to do their job."
Positive Impact (Deterrence Effect)	"I hate to say this, a certain amount of people get caught, you know people deciding to look at stuff that they shouldn't. Because you also want to make an example out of them, you know it's sad to say, what really helps if no one looks at it, and if no one looks at things that they shouldn't, that's the ideal. You know that's not going to happen. So what you do hope is that when people do look at things they shouldn't, they get caught, we work very hard on that, and when they get caught, people find out about them. It's the deterrent effect." "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." "We need to discipline them, we need to make sure that people understand that we take this seriously, and hopefully, there is a deterrent effect that occurs from other people seeing the fact that people have lost their jobs over. Now the fact that only three people in that hospital lost their jobs over it, probably it says to me only good thing, because it says to me only three people were dumb enough to look at the record."

Positive Impact (Tracking Mechanisms)	"We have alerts built in to things, there are alerts for certain people when there is a perceived attack or perceived breach so to speak." "We have software which goes through every PC in the house every day looking for things on PCs . so we have software in place on emails that look for certain patterns of information of people are trying to send out here it will block it." "Our system is all doing very advanced logging, and if I decided that I wanted to see who looked at your record, I would know everybody who looked at your record." "So anybody who goes in and looks at a record of same, the same last name that's, that's a flag. It doesn't mean it's inappropriate. It just means that we need to look at those a little bit closer." "A system behind the scenes looking at these audit models that are being generated continuously and let's look for patterns or let's look for, let's look for trends or patterns that you know doesn't appear to be right and they need to be investigated on."

Appendix E

Illustrative Supporting Data for Organizational context

2nd Order Themes	Illustrative 1st Order Data
Hospital Size	"They [small hospitals] will be out of business and will not be compliant with HIPAA or HITECH, because they cannot afford to" "I have one (HIPAA officer) person to worry about 120 employees. If you had 12,000 employees, to get that same ratio you'd have to have 100 HIPAA officers." "I'm thinking of Hospital X and you've been in that hospital probably. I mean there's so many points of access there, so many people and so many work stations and so much happening and paper everywhere. It may be more of a challenge for them to adhere to the standards than here at this little hospital." "I'd imagine in a big organization trying to control that is a daunting task so while we may not have the, the, the resources for the IT and the sophisticated systems and all that, from a HIPPA privacy standpoint we probably could do better than the big places." "I think if you were a little hospital, you couldn't afford all these utilities."
Academic Status	"We have a large teaching hospital which is actually in the heart of Columbus, Ohio." "[We are] medical school and a major research institution." "we have teaching hospitals"
Educational Background	"I have an undergraduate degree in computer science, and I also have a degree in history, and then i have my JD, jurist doctor, I am an attorney" " I have an associate's degree in biomedical engineering and a bachelor's degree in electronic engineering and a master's in business administration and business." "I have a medical degree." "I went to medical school and became an internist. I became convinced that we will never be able to provide high quality efficient care without using computers effectively … so started to get interested at the end of my residency and became one way and another involved [the hospital] implementation of EHRs. "

	"I have a diploma in professional nursing, a bachelor's of business and finance and a Master's in organizational development."
Leadership	"I think organizations really are a mirror who is leading them and I don't think it's any different on this subject [privacy] than it is on other key subjects whether it's patient safety or anything else." "Organizations that have great leadership at the top are generally proactive whether it's HIPAA and privacy or electronics health records in general. They are generally the trend setters and you have others that are the laggards that will comply, but they'll do it in the 11th hour on the last day." "That is the type of organization, the type of leader [CEO] that will take the intent of something i.e. privacy, HIPAA, data security, and they will be trend setters, and will not negotiate on those points. So that's you know it comes from the top. "

Appendix F

Empirical Grounding of the Study

Evaluative Criteria	Description	Goal	What to look for in this study
Criterion 1	Are concepts generated?	Assess if the concepts used in the research are grounded in the data.	The concepts used in the research are grounded in the data. Therefore, the study could be viewed as fitting with the first criterion.
Criterion 2	Are the concepts systematically related?	Check if there is a linkage between concept	The study shows how the concepts have been interwoven into more coherent themes and categories.
Criterion 3	Are there many conceptual linkages and are the categories well developed? Do they have conceptual density?	Check if categories and subcategories are tightly linked.	Open coding was followed by axial coding, which allowed dense categories to emerge. The linkage between categories was implemented and extension of those categories to themes and overarching dimensions was pursued to achieve conceptual density.
Criterion 4	Is much variation built into the theory?	Check for variations in the theoretical model and different conditions and consequences.	This research presents a hybrid of process and variance in the theoretical framework (Figure 4) that aims to depict the processes as a result of enacting privacy safeguards. The variance component derives from the organizational proactive approach which positively or negatively influences the outcomes.
Criterion 5	Are the broader conditions that affect the study built into its explanation?	Incorporate the micro and macro conditions.	This study incorporates micro conditions that were relevant to the study. The incorporation of the leadership commitment is a good example of integrating micro conditions.
Criterion 6	Has process been taken into	Check if process has been	This study focuses on understanding the outcomes of enacting privacy safeguards and

	account?	considered.	their impact om privacy compliance.This translates into the processes undertaken to handle these outcomes. Therefore, the criterion of identifying process in research has been achieved.
Criterion 7	Do the theoretical findings seem significant and to what extent?	Check for imagination and insights.	The preliminary findings and a theoretical model have been published and well received (Parks et al., 2011a; Parks et al., 2011b); thus, I would regard this as evidence in support of their significance.
Criterion 8	Does the theory stand the test of time and become part of the discussions and ideas exchanged among relevant social and professional groups?	Check if the theoretical framework is able to withstand future testing and research.	Given that this study has been developed based on a specific context (i.e., healthcare), it is our hope that the insights of the emerging theory can make it withstand future applications and research.

Appendix G

Research Process Evaluation Criteria

Evaluative Criteria	Description	What to look for in this study
Criterion 1	How was the original sample selected? On what grounds?	Interviewing informants has been initiated in the hospitals. However, after initial data analysis, this target was revisited to include other healthcare organizations and entities (e.g., the U.S. Department of Health and Human Services, healthcare professional associations, healthcare IT providers, and healthcare privacy consultants). This sample was originally based on privacy leaders only in hospitals and ultimately included privacy leaders from other healthcare-organizations who impact the process by which hospitals respond to information privacy threats.
Criterion 2	What major categories emerged?	The study led to the emergence of major categories – Enactment of Privacy safeguards, Negative Impacts, Positive Impacts, Imbalance Challenge, Workarounds, and Privacy Compliance.
Criterion 3	What were some of the events, incidents, or actions (indicators) that pointed to some of these categories?	Categories emerged as a result of first and second order analysis. For example workarounds emerged when leaders mentioned their lack of compliance, and when healthcare employees embraced activities to bypass privacy safeguards.
Criterion 4	On the basis of what categories did theoretical sampling proceed? That is, how did theoretical formulations guide some of the data collection? After the theoretical sampling was done, how representative did the	Theoretical sampling was driven by the concepts that emerged. The categories of hospitals' size, Workarounds and the Imbalance Challenge created a need to collect further data. Ultimately, some categories sustained (e.g.,

	categories prove to be?	Workarounds and the Imbalance Challenge) and others did not hold up (e.g., hospital size)
Criterion 5	What were some of the hypotheses pertaining to conceptual relations (i.e., among categories), and on what grounds were they formulated and validated?	As a qualitative researcher, I came up with hypotheses in their initial form in early analysis. These hypotheses were formulated and based on the interpretations of the data collected. Examples of these hypotheses include proactive type organizations who exhibited very distinct behaviors regarding their approaches to responding to privacy threats, while reactive type organizations' behaviors were opposite to the ones described above.
Criterion 6	Were there instances in which hypotheses did not explain what was happening in the data? How were these discrepancies accounted for? Were hypotheses modified?	As the coding continued, I improved categories and themes. Some did not hold up. For instance, at early stages of data analysis, I formulated the hypothesis that larger hospitals with more resources would thrive to achieve higher degree of privacy compliance and better address the imbalance issues. I further analyzed this pattern to discover that, while the hospital size matters because it is often closely linked with resources, it is the commitment of top managers that prevails. This hypothesis eventually was modified to account for the role of leadership commitment.
Criterion 7	How and why was the core category selected? Was this collection sudden or gradual, and was it difficult or easy? On what grounds were the final analytics decisions made?	The Imbalance Challenge gradually emerged as the core theme of this study. While other categories emerged first, the Imbalance Challenge theme emerged as further analysis was undertaken. The final analytics decisions were made and validated with the empirical data.