The current unpublished reference for this work is as follows:

> Rachida Parks, Heng Xu, Chao-Hsien Chu, and Paul Benjamin Lowry (2016). "Examining the intended and unintended consequences of organisational privacy safeguards enactment in healthcare: A grounded theory investigation," ***European Journal of Information Systems* (*EJIS*)** (accepted 07-May-2016).

If you have any questions, would like a copy of the final version of the article, or would like copies of other articles we've published, please contact any of us directly, as follows:

- **Rachida Parks**:
  - Email: rfparks@ualr.edu
  - Website: http://ualr.edu/management/dr-rachida-f-parks/
- **Heng Xu:**
  - Email: heng.xu.dr@gmail.com
  - Website: https://faculty.ist.psu.edu/xu/
- **Chao-Hsien Chu:**
  - Email: chu@ist.psu.edu
  - Website: http://ist.psu.edu/directory/faculty/chc4
- **Paul Benjamin Lowry:**
  - Email: Paul.Lowry.PhD@gmail.com
  - Website: http://www.cb.cityu.edu.hk/staff/pblowry
  - System to request Paul's articles: https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx

Examining the Intended and Unintended Consequences of Organisational Privacy Safeguard Enactment in Healthcare: A Grounded Theory Investigation

Abstract

Research shows that despite organisational efforts to achieve privacy compliance, privacy breaches continue to rise. The extant studies on organisational privacy compliance concentrate on the extent to which privacy threats can be alleviated through a combination of technical and human controls and the positive (and often intended) influences of these controls. This focus inadvertently neglects unintended consequences such as impeded workflow in medical practices. To address this research conflict, this study uses an interpretive grounded theory research approach to investigate the consequences of privacy safeguard enactment in medical practices, including whether it influences their ability to meet privacy requirements and whether workflows are impeded. Our central contribution is a theoretical framework, the unintended consequences of privacy safeguard enactment (UCPSE) framework, which explicates the process by which privacy safeguards are evaluated and subsequently bypassed and the resulting influence on organisational compliance. The UCPSE highlights the importance of the *imbalance challenge*, which is the result of unintended consequences outweighing the intended consequences of privacy safeguard enactment. Failure to address the imbalance challenge leads to the adoption of workarounds that may ultimately harm the organisation's privacy compliance. Despite several research calls, the consequences and effectiveness of organisational privacy efforts are largely missing from both information systems and health informatics research. This study is one of the first attempts to both systematically identify the impacts of privacy safeguard enactment and to examine its implications for privacy compliance in the healthcare domain. The findings also have practical implications for healthcare executives on the unintended consequences of privacy safeguard enactment and how they could alleviate the imbalance challenge to thwart workarounds and the subsequent negative effects on privacy compliance.

Keywords

Information privacy, privacy safeguards, healthcare, imbalance challenge, grounded theory, interpretive research, unintended consequences, intended consequences, the unintended consequences of privacy safeguard enactment (UCPSE) framework

Introduction

Organisational governance of the information privacy of patient healthcare records has grown into a serious problem, and the U.S. requires healthcare providers to adhere to the strong information privacy protections outlined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

(Choi *et al.*, 2006; Wall *et al.*, 2015). Despite the strong privacy information protections of HIPAA, over 134 million patients' information have been breached since 2009 (HHS, 2016). These breaches endanger the confidentiality of patient records and result in dire organisational consequences, such as reputation damage, monetary penalties, and civil and criminal liabilities (Wall *et al.*, 2015). To protect patients' information from further breaches and to adhere to HIPAA without facing severe sanctions, healthcare organisations face major challenges in designing and implementing appropriate safeguards to mitigate information privacy threats (Choi *et al.*, 2006).

Information privacy refers to the degree to which individuals and organisations control when, how and to what extent information about them is released (Claerhout & DeMoor, 2005). Greenaway & Chan (2005) explain that organisational information privacy refers to how firms treat their customers' personally identifiable information. Our focus is on organisational-level privacy violations and protection. Notably, Wall *et al.* (2015) outline four kinds of organisational privacy contexts, depending on whether organisational privacy procedures are internally generated (usually because of ethical and professional considerations) or externally generated (usually because of legal requirements, such as HIPAA) and on whether they are focused on protecting consumer privacy (such as HIPAA) or employees.

Our privacy context is compliance to externally governed privacy regulations that protect healthcare consumers. The selection of the healthcare domain is not arbitrary. According to the privacy rights clearinghouse, a non-profit organization that keeps up-to-date information about data breaches across all industries within the U.S, the healthcare industry has the highest number of breaches (PRC, 2016). This presents major challenges for healthcare organizations as they are trying to minimise these data breaches while not impeding the practice of medicine. The presence of increasing healthcare penalties for non-compliance and privacy operational demands (Croll, 2011), is adding further complexity. Accordingly, in our context, *privacy compliance* is defined on the organisation level (not the individual level) as the organisation complying with regulatory privacy rules to ensure the confidentiality of patients' electronically protected health information (Wall *et al.*, 2015). Previous researchers advocate for implementing privacy safeguards as part of organisational privacy management strategies. *Privacy safeguards* refer to technical protections, human defences, physical precautions and organisational processes to protect privacy (Parks *et al.*, 2011b). However, these safeguards are only partially effective, because privacy breaches continue to occur (Culnan & Williams, 2009; Wall *et al.*, 2015). Despite the acknowledged importance of privacy safeguard enactment on overall privacy compliance, the consequences of these enactments remain comparatively understudied (Belanger & Crossler, 2011; Smith *et al.*, 2011). Notably, when referring to enacting privacy safeguards in this study, we focus on the act of implementing safeguards, not only decision to do so. This enactment, or implementation, can take many forms, including implementing the technical measures of encryption or passwords, adapting employment

sanctions for looking up records that do not pertain to one's line of work and enforcing physical security through the use of badges to restrict access to certain areas. Importantly, most privacy and security studies, whether consumer- or employee-centric, focus primarily on internal rather than external compliance to privacy protection measures. As Wall *et al.* (2015) explain, studies focusing on externally governed privacy and security rules are primarily exploratory and descriptive in nature, probably because organisation-centric data collection is difficult in this research area (Dhillon & Moores, 2001; Walczuch & Steeghs, 2001; Milne & Culnan, 2002; Nord & McCubbins, 2006; Crossler *et al.*, 2013). Moreover, much research in this area uses surveys or hypothetical scenarios (e.g., D'Arcy *et al.*, 2009; Siponen & Vance, 2010), both of which may be difficult to apply to an organisation-level analysis of compliance to external privacy regulations.

Moreover, to date, studies of organisational privacy compliance concentrate on the extent to which privacy threats can be alleviated through a combination of technical and human controls and the positive (and often intended) impacts of these privacy controls. However, this focus overlooks the unintended impacts of privacy safeguards, such as those that undermine medical processes or patient care. This is no minor oversight. Recent empirical studies raise concerns regarding the unintended consequences of privacy safeguards that impede employees' needed access to information access and overall workflow (cf., Chen & Xu, 2013), as well as induce employees to engage in workarounds to bypass privacy procedures or features (cf., Murphy *et al.*, 2014). Given the centrality of privacy compliance and the pivotal nature of engaging in proper processes in healthcare, it is imperative that privacy researchers in the healthcare domain identify both the intended and unintended consequences of enacting privacy safeguards and their subsequent effects on privacy compliance on an organisation level.

The current study makes several contributions. First, it introduces a theoretical framework that explicates the process by which the individual privacy safeguards are evaluated and their intended and unintended impacts on the organisation's privacy compliance are examined. Second, in response to the call by Belanger & Crossler (2011), we study the actual outcomes and implications of privacy safeguards in healthcare organisations. Specifically, we use a grounded theory approach to provide a rich lens to understand both intended and unintended consequences of privacy safeguard enactment and their implications for privacy compliance in medical practice. Third, this research contributes to the recent call for interdisciplinary research (Smith *et al.*, 2011) by converging the research streams of both information systems (IS) and health informatics. Fourth, because Smith *et al.* (2011) show a lack of organisation-level privacy research in the extant literature, noting studies at the organisation level 'are necessarily more complex and less conducive to 'quick' data collection techniques such as written and online surveys' (p. 1006), our research targets this under-researched level of analysis through a grounded theory approach, thus providing new theoretical insights on organisational privacy management.

Background

This study's literature review was based on defining three criteria: domain, sources and search strategy (Cooper, 1998). The domain is interdisciplinary and includes IS and health informatics. The literature on health informatics was reviewed, as it is contextually relevant. Our sources include the top five outlets identified by Lyytinen *et al.* (2007)for the IS field and we use Le Rouge & De Leo (2010) ranking to select our sources from the leading journals on health informatics. Importantly, our literature review focuses on two main themes that define our qualitative research: (1) privacy safeguards that are used in the healthcare industry and (2) the intended versus unintended consequences of enacting privacy safeguards in organisations.

Privacy Safeguards in Healthcare

There is a growing, yet still limited, body of research targeting organisational responses to privacy threats and issues (e.g., Greenaway & Chan, 2005; Culnan & Williams, 2009; Smith *et al.*, 2011; Wall *et al.*, 2015). One recent study suggests that organisations 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, the health informatics literature is replete with research that proposes various technologies to address health information privacy threats, including the application of access control mechanisms to limit access to authorised users (Mohan & Yaacob, 2004; Blobel *et al.*, 2006; Lovis *et al.*, 2007; Chen *et al.*, 2010), the use of anonymisation and pseudo-anonymisation to remove the identifiers from medical data (Quantin *et al.*, 2000; Mohan & Yaacob, 2004; Aberdeen *et al.*, 2010) and the adoption of encryption and cryptographic methods to make the data unreadable to anyone except those who hold the keys (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 the fields of IS and health informatics, the extant research studies the procedures that govern healthcare delivery processes and ensure information privacy. However, it has been more than two decades since Smith (1993) published findings based on a study of organisational privacy policies, which drew attention to such problems as a lack of policy and gaps between different policies and practices. Although organisations in the U.S. are more likely to enact privacy protection measures due to HIPAA compliance requirements (Peslak, 2006), the gap between organisationally desired privacy behaviours and actual privacy behaviours is still momentous (Croll, 2011; Wall *et al.*, 2015).

In term of human safeguards, several studies investigate the impact of training and education on increasing compliance (Mohan & Yaacob, 2004; Yeh & Chang, 2007; D'Arcy *et al.*, 2009; Fernando & Dawson, 2009). However, the positive influence of these safeguards is mixed, especially in light of

research on employee misbehaviour and general compliance problems (Bulgurcu *et al.*, 2010; Siponen & Vance, 2010; Hu *et al.*, 2011; Hsu *et al.*, 2015; Lowry & Moody, 2015; Lowry *et al.*, 2015).

The Consequences of Enacting Privacy Safeguards

Much of the literature on information privacy rests on the assumption that the enactment of privacy safeguards and mechanisms leads to better protected information and to better compliance (see Table 1), both of which are intended consequences. However, the enactment of privacy safeguards can bring some unintended consequences as well. We posit in our study that there may often be an imbalance between these intended and unintended consequences.

Table 1 Mapping the Consequences of Enacting Privacy Safeguards

	Intended Consequences	**Unintended Consequences**
Positive	(Quantin *et al.*, 2000; Ohno-Machado *et al.*, 2004; Ravera *et al.*, 2004; Gritzalis *et al.*, 2005; Blobel *et al.*, 2006; Boyd *et al.*, 2007; Choe & Yoo, 2008; Kantarcioglu *et al.*, 2008; Lee & Lee, 2008; Blanquer *et al.*, 2009; Aberdeen *et al.*, 2010; Chen *et al.*, 2010; Croll, 2011; Haas *et al.*, 2011; Canim *et al.*, 2012; Li *et al.*, 2014)	n/a
Negative	(Ohno-Machado *et al.*, 2004; Kantarcioglu *et al.*, 2008; Canim *et al.*, 2012)	(Ash *et al.*, 2004; Coiera & Clarke, 2004; Choi *et al.*, 2006; Posey *et al.*, 2011; Lowry & Moody, 2015; Lowry *et al.*, 2015)

In the literature, unintended consequences refer to the unforeseen or unpredicted results of a specific action (Campbell *et al.*, 2006). Organisational theorists study the impacts of unintended consequences in the domains of economic performance (Lal, 2001), project management (Brown, 2000) and organisational decision-making (Magasin & Gehlen, 1999). Recently, in the IS policy compliance literature, unintended consequences include negative employee reactions to policies, such as pushing back, doing the opposite of what is required, workarounds, malicious compliance and anger (Posey *et al.*, 2011; Lowry & Moody, 2015; Lowry *et al.*, 2015). This literature indicates that such unintended consequences can occur because of employees' perceived threats to freedom, unfairness or privacy invasion.

The discussion of unintended consequences is relatively new in the privacy management literature. However, in the IS field, unintended consequences originated from the diffusion of innovations (DOI) theory (Rogers, 1998), which posits that the consequences of adopting innovations can be intended or unintended and desirable or undesirable. Although our research focuses on the unintended negative consequences of organisational privacy safeguards in the healthcare domain, prior studies on DOI identify various unintended desirable and beneficial consequences of innovation adoption (Ash *et al.*, 2004). Campbell *et al.* (2006) point out that 'unintended consequences are not uniformly errors or mistakes: they are simply surprises that can span a spectrum from lucky to unfortunate' (p. 548).

In health informatics, many studies recognise the importance of the unintended consequences of adopting healthcare information technologies (HIT). For instance, both Ash *et al.* (2004) and Campbell *et al.* (2006) highlight the importance of the unexpected adverse consequences surrounding the implementation and maintenance of computerised provider order entry systems. Similarly, Harrison *et al.* (2007) analyse the emergent and recursive processes in HIT implementation and their unintended consequences. Collectively, these studies lead to a general consensus that introducing and implementing HIT is likely to incur a range of unanticipated adverse consequences, including higher clinician workloads, interrupted workflow, untoward changes in communications and practices, negative emotional responses, error generation and unexpected changes in power structures (Campbell *et al.*, 2006).

Given the recognised importance of unintended adverse consequences in both IS and health informatics, it is somewhat surprising to find limited studies on the unintended adverse consequences of privacy safeguards. One of the few exceptions is the study by Choi *et al.* (2006), which suggests that before the enactment of HIPAA, secure-lock doors remained open and passwords were shared to increase ease and efficiency. Work practices have changed after HIPAA to 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 & Clarke (2004), who show that managing patients' e-consent privacy preferences may impede clinicians' workflows. Failure to address these workflows' disruptions could potentially lead employees to embrace workarounds to bypass the features that make accomplishing their work difficult (Ash *et al.*, 2004).

In summary, the privacy literature identifies various types of information privacy safeguards; that is, the mechanisms by which organisations respond to privacy threats and achieve compliance. Although unintended consequences are highlighted as an important issue within privacy management in the healthcare domain, little empirical research explicitly examines them in relation to privacy safeguards, or the struggles that organisation may face in balancing intended and unintended consequences. This research is designed to fill in the gap in the literature by exploring and describing how privacy safeguards

result in both intended and unintended consequences and to examine their effects on organisational privacy compliance.

Research Method

We adopt a qualitative research method in this study to answer our research question on the outcomes of enacting privacy safeguards. Specifically, we use a qualitative research approach based on grounded theory (Strauss & Corbin, 1998; Corbin & Strauss, 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 (Glaser & Strauss, 1967), such as healthcare. It offers a rigorous approach that assists in understanding organisational privacy safeguards at the organisation level through testable theories tightly connected to data and context (Eisenhardt, 1989).

Data Collection

After clearance by the institutional review board, informants were contacted to participate in this study. Informants from 21 U.S. hospitals as well as other healthcare organisations (consulting and healthcare research firms, the government and professional healthcare organisations) agreed to participate in this study, which is part of a larger project. Data were gathered through semi-structured interviews with 30 consenting informants who had expert knowledge in privacy practices and were holding key positions in hospitals, such as chief executive officer, chief information officer, chief privacy officer, chief medical information officer, information technology director and privacy officer. Appendix A summarises the informants' titles and types of organisations. Among hospitals, the study distinguishes between small, medium and large hospitals based on the number of beds. The American Hospital Association classifies hospitals with 100 or fewer beds as small (AHA, 2016), 500 or more beds as large (Kaunitz *et al.*, 1984) and between 101 and 499 beds as medium. 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 organisations to mitigate privacy threats and their impacts on healthcare activities and practices. Our interview questionnaire evolved during the process of conducting this research. When we started identifying themes, we developed probe questions to explain differences in the informants' privacy conceptualisations. These probe questions became more specific as we advanced in our data analysis. Details about the interview items are provided in Appendixes B and C.

In grounded theory, sampling is driven by conceptual emergence and limited by theoretical saturation (Glaser & Strauss, 1967). Consequently, the selection of data sources is neither a random selection nor totally a priori. For example, we decided a priori that a combination of different hospital sizes was most appropriate for this study; however, pursuing a particular hospital size for further analysis depended on the emergent themes. Strauss & Corbin (1998) note that researchers must be flexible to

handle what arises 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 organisations 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, to include more specific questions about the operational impacts 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 had difficulty obtaining informants because of the critical sensitivity of privacy and security topics (Crossler *et al.*, 2013), as well as the scheduling challenges of healthcare executives, we managed to secure interviews with 30 informants. Our success was due to our involvement and membership with the healthcare information and management systems society (HIMSS), the Penn State center for integrated healthcare delivery systems (CIHDS), and finally to using the snowball technique (Lincoln & Guba, 1985) where we were able to identify the next informant based on the last informant's connections. We conducted data collection and analysis until the point of saturation, when we reached redundancy in the data and found no new concepts (Corbin & Strauss, 2008).

Data Analysis

In this section, we provide an overview of the steps undertaken using the grounded theory approach, as depicted in Figure 1.

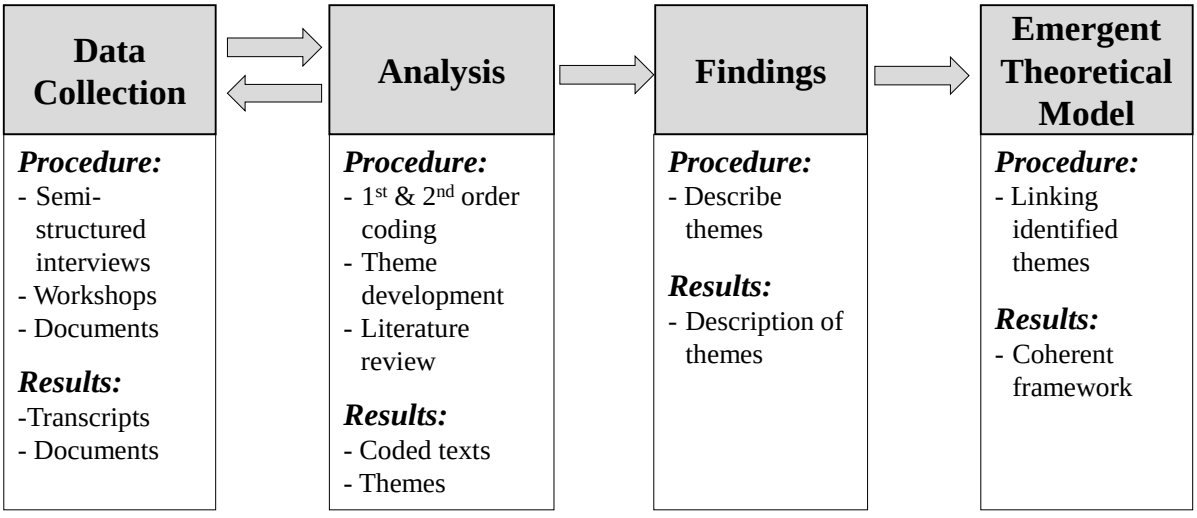

Figure 1. Grounded Theory Analysis Process

All interviews were audio recorded and transcribed verbatim. The transcribed interviews were imported into a computer on which the qualitative data analysis software tool NVivo (v.9) was installed. Notably, NVivo does not automatically code transcribed interviews but is used to organise the different codes and categories that are identified during the first- and second-order analyses. NVivo supports different stages of analysis, including defining concepts within themes, called nodes, and providing data analysis capabilities for searching, grouping and relating these nodes. We coded the interviews in several steps. First, we used open coding techniques to inductively identify preliminary categories, with no a priori coding or categorisation. The next step used was axial coding, which helped to develop the categories into themes (Corbin & Strauss, 2008). Finally, we implemented selective coding, where we integrated the categories 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 the potential contributions of our findings to the privacy literature in the healthcare domain.

During the coding process, every piece of data was contrasted against other pieces through constant comparison to ensure that the appropriate codes were applied to informants' views. Having embraced the constant comparative method, we continued looking for information until the categories were saturated and no additional data were found. The constant comparative method has been a key concept in the development and understanding of grounded theory (Glaser, 2001). According to Glaser & Strauss (1967, pp. 113-114), the constant comparative method facilitates the generation of complex "theories of process, sequence, and change pertaining to organisations, positions, and social interaction [that] correspond closely to the data since the constant comparison force the analyst to consider much diversity in the data." Constant comparisons determine the relevance to the emergent theory or the assumptions made by the emergent theory.

.

Evaluative and Trustworthiness Criteria

The evaluation of every research poses the question of the appropriate criteria to be used for making judgments. Positivist researchers employ the criteria of internal validity, external validity, reliability and objectivity. These criteria are not appropriate for interpretive studies. We used two approaches for judging interpretive research: (1) ensuring trustworthiness (Lincoln & Guba, 1985) and (2) ensuring the adequacy of the research process and its empirical grounding (Strauss & Corbin, 1998; Corbin & Strauss, 2008). These approaches are explained next and applied to the theoretical framework (See Appendix F and G).

Ensuring Trustworthiness:

The aim of trustworthiness is to support the assumption that a study's findings are 'worth paying attention to' (Lincoln & Guba, 1985, p. 290). Lincoln & Guba (1985) offer a set of four trustworthiness

criteria appropriate for interpretive research that are analogous to positivist research: credibility, transferability, dependability and confirmability. To address credibility, we used multiple methods and sources to ensure triangulation of the findings, such as single interviews, group interviews and data collection from different sources (e.g. hospitals and government administrators, consultants and IT designers). Triangulation was also achieved by using supplemental information gathered during privacy and/or healthcare workshops and roundtables attended by the authors, along with the associated documentation.[1] Moreover, the first author has several years of industry experience in healthcare IT, in addition to being an active member of a healthcare research centre (Penn State CHIDS) and a national healthcare professional association (HIMSS). To ensure transferability, we provide a detailed first-order analysis of the phenomenon and context, which should provide enough background for readers to judge the plausibility of the findings and their applicability beyond the scope of this project (Van Maanen & Schein, 1979). We conducted an inquiry audit rather an inter-rater reliability, because interpretive research assumes that each researcher will have a unique interpretation of the findings (Lincoln & Guba, 1985). An inquiry audit was performed by one professor of organisational behaviour and one 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 were supported by the data collected; we shared the study with three professors, two graduate students and two healthcare professionals to solicit critical feedback. The consensus suggests that this research analysis and theoretical model accurately reflect the data.

Ensuring the Adequacy of the Research Process and the Empirical Grounding:

Corbin & Strauss (2008) identify several criteria for evaluating an interpretive research. The empirical grounding includes evaluating eight criteria including assessing if the concepts used in the research are grounded in the data, if there is linkage between concepts, insights and if the theoretical framework is able to withstand future testing and research, every criterion is evaluated and documented in appendix F. The adequacy of the research process includes seven criteria pertaining to the selection of the original sample, the categories that emerged, how did theoretical formulations guide some of the data collections, and how and why was the core category selected? All seven criteria and their evaluation are documented in detail in appendix G,

Findings

[1] There were a total of four events: The first event was a privacy and security workshop in Florida where the attendees included healthcare consultants, faculty and healthcare government representatives. The second event also took place in Florida in the form of a privacy roundtable. The attendees included chief privacy officers, chief information officers, lawyers and consultants. The third event was a healthcare workshop that took place in Pennsylvania with faculty, EHR developers and hospital administrators. The fourth event was a healthcare workshop in the District of Columbia where the attendees were faculty and healthcare government representatives.

Using a grounded theory approach, we present the concepts and categories that emerged from the iterative process of data gathering and analysis (Figure 2). The findings are presented by interweaving the first order codes along with the second order themes to provide an overarching structure through a thick description of the data (Kreiner *et al.*, 2006).

Intended Desirable Consequences

We found that the intended desirable consequences include controlled access, the deterrence effect and tracking mechanisms. These categories and representative data for each category are presented in Appendix E.

Controlled access: The creation of technical privacy safeguards, such as role-based access control (RBAC) mechanisms, allowed for better control over who could access the system. Hence, filtering out users who have no business looking at patient information was a positive consequence of privacy safeguards—each employee is granted access based on their need to know, which is defined by their role within the organisation. As one healthcare executive commented:

> *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.*

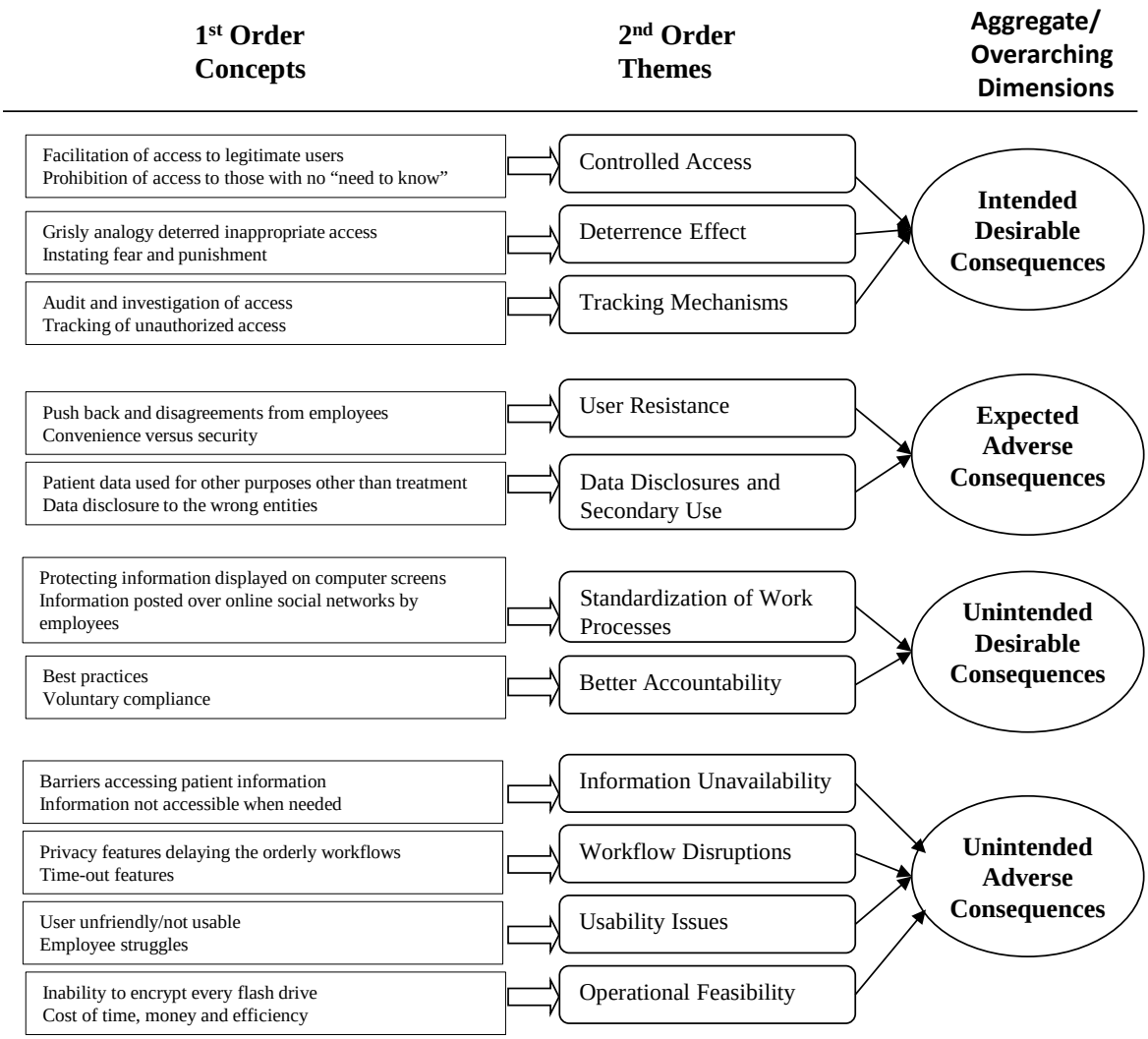

Figure 2. Emergent Concepts, Themes and Dimensions

Consequently, hospitals that enact privacy safeguards such as access control within their systems have better outcomes regarding who is accessing the data and for what purpose.

Deterrence effect: Informants emphasised 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 patient information. A chief privacy officer of a large hospital used an analogy to refer to how his organisation 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 co-workers 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.*

Instating fear and punishment for not protecting organisational data is perceived as an important and desirable consequence of enacting privacy safeguards, as it makes a clear statement of the expectations and consequences, which prevents misjudgements. A similar positive influence of fear was recently shown empirically in a study on motivating users to protect organisational security assets (Boss *et al.*, 2015).

Tracking mechanisms: In addition to controlled access**,** healthcare executives believed that the ability to track who accesses specific records and when they were accessed was a major positive outcome of privacy safeguard enactment. One chief medical information officer stated:

> *One of the nice things about EHRs [electronic health records] 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.*

This ability to perform audits and investigate who accessed the system is viewed as an intended and desirable consequences, deterring access that is not authorised.

Expected Adverse Consequences

Healthcare executives also expected some negative outcomes of privacy efforts. These outcomes resulted in user resistance, data disclosures and secondary use. Appendix E presents these categories and representative data for each category.

User resistance: The creation of new privacy safeguards created some resistance and complaints from users. Integrating privacy and security mechanisms in healthcare systems, which restrict clinicians' access to patient information, is challenging. As stated by one chief privacy officer:

> *The dilemma is to give the clinicians the most important information that they can with the least amount of resistance.*

This resistance emerged in instances in which instating passwords that are too complex and/or need to be changed frequently, thus making it hard for users to remember and adhere to the requirements. This challenge was described by one chief of information security officer:

> *If the security is too hard, people wouldn't do it. If it is beyond their work flow, 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 always is… so, a lot of push-back or complaints.*

Data disclosures and secondary use: Informants emphasised their concern over patient information when it is not used for direct treatment. This concern was perceived as a negative impact because the hospital no longer has direct control over the data when shared with other entities for purposes of payment, coding, medical research or other. One a healthcare executive commented:

> *How do you secure information that's being used for secondary purposes for research, for research, for quality, for billing and [for] coding?*

Another healthcare executive stated:

> *There are many times when a clerical person will hit the wrong number on the fax machine and fax a lab result for a patient to a Sheetz store [convenience store]… this happens all the time.*

Unintended Desirable Consequences

Healthcare executives reported several positive outcomes of privacy efforts that were not initially intended. These privacy efforts yielded benefits such as standardisation of work processes and better accountability. Appendix E presents these categories and the representative data for each category.

Standardisation of work processes: The creation of privacy policies prompted organisations to be more aware of their physical operational surroundings and the visual setup of computers. For instance, in certain departments where patients are present, extra initiatives were taken to protect patient information, such as monitor screen protectors to make devices impossible to read at angles other than that of the user. One informant stated:

> *We must make sure that it is [patient information] handled appropriately … provide basic stuff of making sure people close curtains, close doors, they position their computers and equipment so that people can't read or see the information.*

Another desirable and unintended consequence regarding work processes was related to the use of online social media (ONS). Employees sometimes make ONS posts about patients or about the hospital not thinking about potential privacy breaches. These situations are motivating hospitals to have procedures in place to standardise online posts. One privacy officer explained:

> *Here' is how we get in trouble on Facebook and how a lot of guys get in trouble. I think a lot of the marketing teams like using Facebook for marketing. So, people get in there and say some good things without asking, but then you could also say bad things about a manager or certain things going on. That's when our privacy comes in … you want to say something bad about [our hospital], what do you do then? There has to be some procedures and protocols around that.*

Accountability: Healthcare executives also reported individual and organisational behaviours that showed better accountability in protecting patient information. Best practices toward patient data even if the law/regulation is not established and voluntary compliance were among the behaviours described. Accountability has long been a powerful deterrent against undesired behaviours and refers to 'the implicit

or explicit pressure to justify one's beliefs and actions to others' (Lerner & Tetlock, 1999; Tadmor & Tetlock, 2009, p. 8). Recent IS policy compliance research shows the powerful, positive organisation effects of fostering accountability in employees through accountability theory (Vance *et al.*, 2013, 2015). Vance *et al.* (2015) explain how accountability works to increase organisational policy compliance, as follows:

> *Accountability theory explains how the perceived need to justify one's behaviours to another party causes one to consider and feel accountable for the process by which decisions and judgments have been reached. In turn, this perceived need to account for a decision-making process and outcome increases the likelihood that one will think deeply and systematically about one's procedural behaviours* (p. 347).

Focusing on doing the right thing through best practices makes the environment much more accountable at protecting patient information rather than only focusing on meeting the regulatory requirements. In this regard, one chief privacy officer stated:

> *I do think that there are a number of motivating factors. One of them is the right thing to do and that is the right attitude, and that would get you a lot further than going off checking off check boxes and say we did this, we did this, we are done, because you are never really done, even if you followed all the rules. You have those who do a lot of compliance very voluntarily and that is why I am only half joking when I said that those laws are meant to address those who are not willing to bring themselves into high standards and compliance; that's why we have them. Think about it, most people who work in a bank don't embezzle money, but you have rules against that because you have few bad actors, and that is the same here.*
>
> *You just try to set that base line high enough to make sure that the information is secure. So, that is the purpose of the regulation and some of the certification requirements it to make sure that you have a fairly high baseline to make sure that the information is adequately protected, but we would encourage people to go beyond that and I don't know how you dictate attitude. And if you are not going to do it, I think the party line is if you are not going to do it because you have the right attitude, then we will make you do it through regulation and enforcement.*

Several healthcare executives noted their voluntary compliance beyond compliance with regulatory mandates:

> *It is not like we did not care about information before [HIPAA] and now all of the sudden the legislation makes you compliant with this. That is a poor assumption! We clearly value patient health information security at the highest level and have had for years …. For example, when we were building the EHRs eight years ago, before HITECH and even before HIPAA, all those considerations of who need to see what information, where is it secured, and where the displays for the screens are, were all inherent to what we are doing. Also, the policies and procedure associated with that. We actually have people who are hired to oversee those things in the institutions—patient privacy officers—so there are people who live and breathe this every day.*
>
> *When the HIPAA privacy rule came out, because it was a mandate, organisations did comply because they knew they needed to. However, I don't think that's the only thing, because most organisations that I've come in contact with either, because I've worked there or I know their privacy officers, they do compliance because it's a good thing to do.*

> *We like to see particularly security as being an essential element of an electronic system, and other people see it and add on. That is not the right perspective to have. When you have that perspective, then it flows to the bottom of piles of the things that you are doing. So, yes, now we have this wonderful electronic system, but we don't have the money to put the adequate security on it. While in reality, you have to. It is part of the price of doing business.*

Unintended Adverse Consequences

Although it is natural to make the inference that creating technical and human privacy safeguards leads to better organisational compliance and fewer privacy breaches, our analysis shows some unexpected results. Several executives reported unintended and undesirable impacts of privacy safeguard enactment. This includes information unavailability, workflow disruptions, usability issues and operational feasibility issues. Appendix D summarises the categories of unintended consequences and the representative data for each category.

Information unavailability: Notably, a question about the influence of privacy safeguards on the availability of information was not explicitly asked during the interviews. Rather, the informants themselves introduced this challenge while explaining the impacts of privacy safeguard enactment. This challenge was described by one chief information security officer as having two directives:

> *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 jobs the right way.*

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 healthcare delivery appeared to have created serious issues for clinicians trying to provide care for their patients, which opened up doors for potential unauthorised access and impacted privacy compliance. As 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.*

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 healthcare, where patient information is

often needed on a continual basis. Our results highlight the dilemma of ensuring availability and access to patient information for authorised healthcare providers without breaching the confidentiality of medical information. If the information needed by healthcare professionals to reach critical clinical decisions were unavailable due to tight access controls, patients may be incorrectly treated. Therefore, the unavailability of information may have dire consequences for the quality of patient care.

Workflow disruptions: As part of the interview protocol (Appendix A), the first author explored the effects of privacy and security safeguards on healthcare workflows. Comments about workflow disruption issues came up during the semi-structured interviews. The data analysis shows that these workflow disruptions were reflected through conflicts and push-back from employees as noted by one informant:

> *Do you want me not to administer that medication because everything didn't line up in the security behind the scenes?*

The implementation of certain privacy technologies resulted in conflicts and push-back. For example, timeout features are supposed to log off employees whose sessions are inactive to prevent unauthorised access by other employees. Although, hypothetically, this feature is an effective privacy initiative, it is not always positively received by certain healthcare professionals, especially 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.*

Healthcare organisations tend to consider these impacts to avoid push-back 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 implemented to bring the hospitals into compliance, in some cases, they ended up negatively impacting the hospitals' adherence to regulations. In cases of workflow disruptions issues, employees found ways around these mitigation tools to accomplish their duties. This disruption was illustrated by the nurses' workflows that one of the study informants shared:

> *Forty percent of the work that a nurse does is to administer medication; 40% of her day, she's looking for pills and administering them. . . she is logging in and waiting, waiting, waiting and 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 and 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 they leave it logged on. But when they go back to the medicine room, it's logged on, and that's a security risk.*

Our results suggest that, in the pursuit of privacy compliance, organisations implement processes that may change their employees' operational workflows. These changes may involve encrypting network transmission, pulling staff out for training or instating timeout features. As a result, users may not always positively react to implemented changes, especially when these changes disrupt their work routines.

Usability issues: Usability has long been defined as the degree of efficiency, ease and effectiveness of use, and this concept has been applied to a broad range of users, tasks, tools and environments (Kushniruk, 2002; Kushniruk & Patel, 2004; Lowry *et al.*, 2006; Lowry *et al.*, 2013). Usability is particularly crucial to medical systems (Kushniruk, 2002; Kushniruk & Patel, 2004). With the design and implementation of privacy protective technologies, usability has become an extremely important, albeit poorly understood, element of privacy. The end results of poor usability are user dissatisfaction and unusable systems (Johnson *et al.*, 2005). In the healthcare industry, understanding the interplay between usability and privacy is essential because various privacy-enhancing technologies have been introduced to control access to medical facilities and protect the confidentiality of patient information.

The usability challenges we found during data analysis include current applications or systems of EHRs. The challenges arose from dealing with inherent difficulties associated with 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 had implemented:

> *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 addressing usability issues causes employees not to use privacy protocols or to find ways around them to accomplish their tasks, which could negatively impact the organisational privacy compliance.

Operational feasibility issues: Many of the informants commented on the operational feasibility of the privacy safeguards implemented in their hospitals, including 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 alerts 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 negatively influence the overall performance of healthcare delivery. Regarding healthcare regulations, hospitals face major operational issues due to how healthcare policies are crafted. The challenges that healthcare leaders face regarding operational feasibility are weighed against the patients' best interests and, therefore, they impact privacy compliance. One privacy compliance officer stated:

'We have 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.'

In summary, operational feasibility is an important factor for the deployment of new privacy safeguards in medical practices. 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. Our data showed unintended adverse consequences of the enactment of privacy safeguards on operational feasibility, resulting in performance degradation.

The Imbalance Challenge

Throughout this research project, healthcare leaders stated on numerous occasions that privacy threats do not end with the implementation of controls and safeguards. They also reported that both intended consequences and unintended consequences may occur during the enactment of privacy safeguards. Although intended consequences—both desirable and undesirable—are expected and accounted for, it is the emergence of unintended consequence, especially adverse consequences, which causes imbalance between maintaining patient privacy and not inhibiting workflows. The imbalance challenge is an analytical construct that was created to make sense of what organisations reported as the results of enacting information privacy safeguards. The imbalance challenge, which is the result of unintended consequences outweighing intended consequences of privacy safeguard enactment, outlines the organisations' struggles in maintaining patient privacy without inhibiting business processes. Although no mathematical formula was presented or derived, the privacy leaders pointed specifically to adverse unintended consequences as the main culprit for this imbalance.

According to privacy leaders, an imbalance challenge occurs when the unintended consequences of enacting privacy safeguards outweigh the intended ones. A chief information officer stated:

Cost and safety pretty much drive a good portion of what we do and I am not talking about the cost of [technology] …. I am talking about the cost of not getting the results to the patient fast

> *enough. I am talking about the cost of delivering the wrong medication dose … the technology piece of it is expensive, but it is not nearly as expensive as the down side of not doing it.*

The same chief information officer continued:

> *My dilemma is stability versus intricacy like meeting the requirements. The requirements are such that I can't always offer a stable system, but if I am a patient and I just had hip surgery and I am in excruciating pain and I need pain meds, they [patients] really don't care that my seven application solution works or not, they just want the pain medication. So, there is the dilemma, stability offering enough flexibility and don't let yourself get caught but giving out too much information.*

One privacy officer illustrated this imbalance challenge by stating:

> *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.*

Privacy leaders uniformly emphasised the need for better understanding and handling of conflicting challenges. Hence, a thorough understanding of these factors and their influence on business practices is fundamental for explaining and addressing the imbalance challenge. The imbalance challenge is of pronounced concern to healthcare privacy leaders as 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.*

Discussion of the Emergent Theoretical Framework

This section presents the emergent theoretical framework, the unintended consequences of privacy safeguard enactment (UCPSE framework), illustrating the intended and unintended consequences, the emergence of workarounds implications and the impacts on the organisation's privacy compliance (Figure 3). The model describes a process that includes the following categories: the enactment of privacy safeguards, intended (desirable and adverse) and unintended (desirable and adverse) consequences of implementing privacy safeguards, the imbalance challenge, workarounds and organisational privacy compliance. Close analysis of the data revealed interrelations among these categories and allowed for their integration into a theoretical framework (Strauss & Corbin, 1998). These major categories are found within both IS and health informatics communities, yet they are 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 safeguard enactment, the causes of the workarounds and the impacts on organisational privacy compliance. This section also compares the categories and relationships of the theoretical framework with those from related literature (Eisenhardt, 1989). The interpretations suggest that the process diverges in two paths when unintended consequences outweigh intended consequences.

Enacting and Evaluating Privacy Safeguards

Organisations enact privacy safeguards to mitigate information privacy threats and ensure legal compliance. However, much of the organisational research on privacy safeguards ignores a comprehensive view of reality: it tends to focus on intended consequences but overlooks unintended adverse consequences. Therefore, in this study, we propose an emergent theoretical framework that includes a more realistic range of intended and unintended consequences that can lead to the imbalance challenge. This framework requires that the following four quadrants of potential consequences of safeguards be considered: (1) intended consequences that are desirable, (2) expected consequences that are undesirable, (3) unintended consequence that are desirable and (4) unintended consequences that are undesirable. Figure 4, visually portrays these quadrants with actual examples from our data collection.

Evaluating Whether an Imbalance Challenge Exists

Once these consequences are explored, one can better assess whether an imbalance challenge is likely to happen by examining the unintended consequences and more specifically the undesirable consequences. These types of undesirable consequences tend to negatively shift the organisations' desired balance. For example, we expect the unavailability of information needed to treat a patient to create an imbalance challenge between protecting patient information and treating patients. Similarly, disruptions in workflow, usability and operational issues impede healthcare delivery. Ideally, the organisation minimises the negative impacts and enhances the positive ones, because healthcare organisations seek to achieve

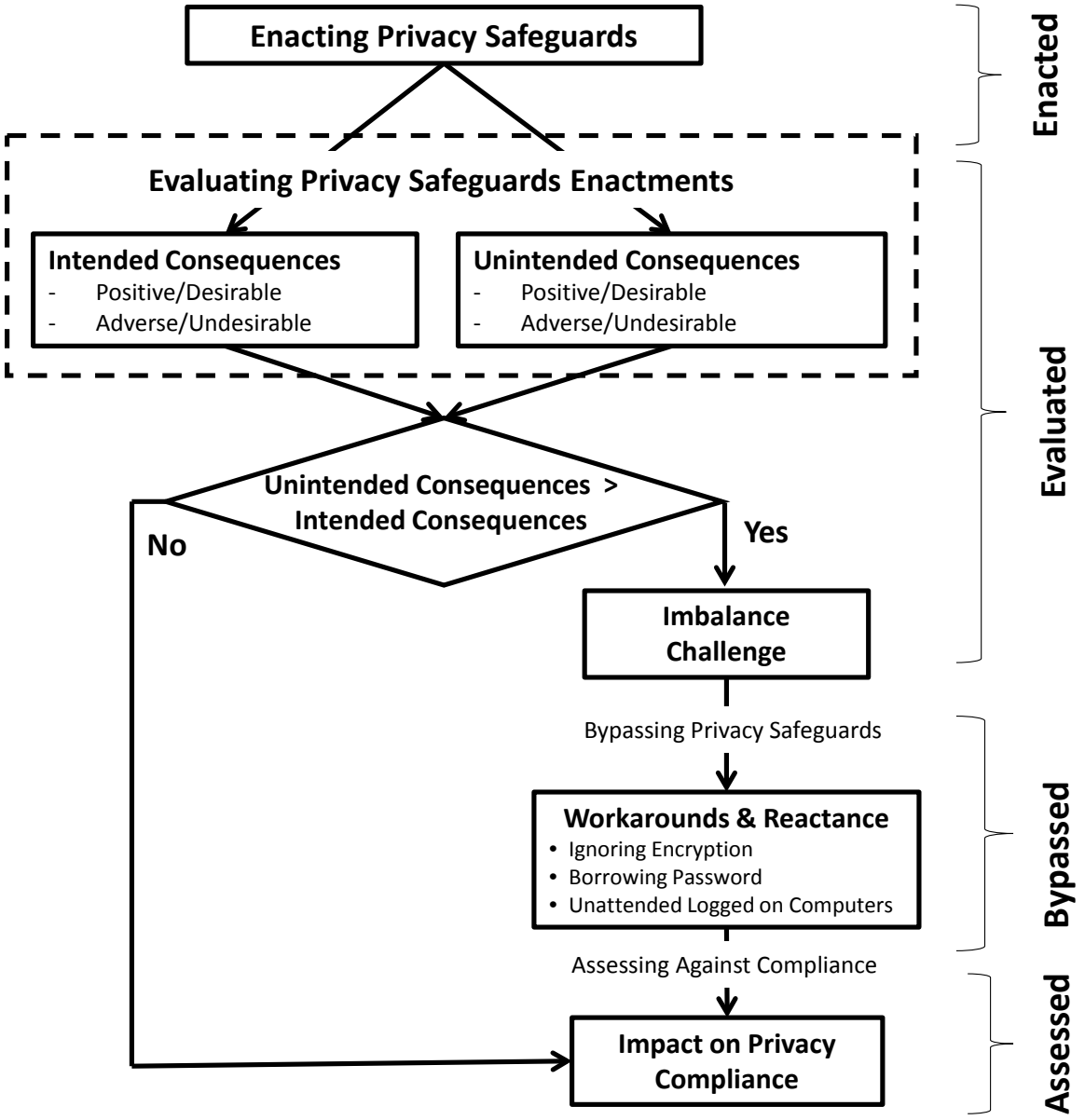

Figure 3. The Unintended Consequences of Privacy Safeguard Enactment (UCPSE) Framework

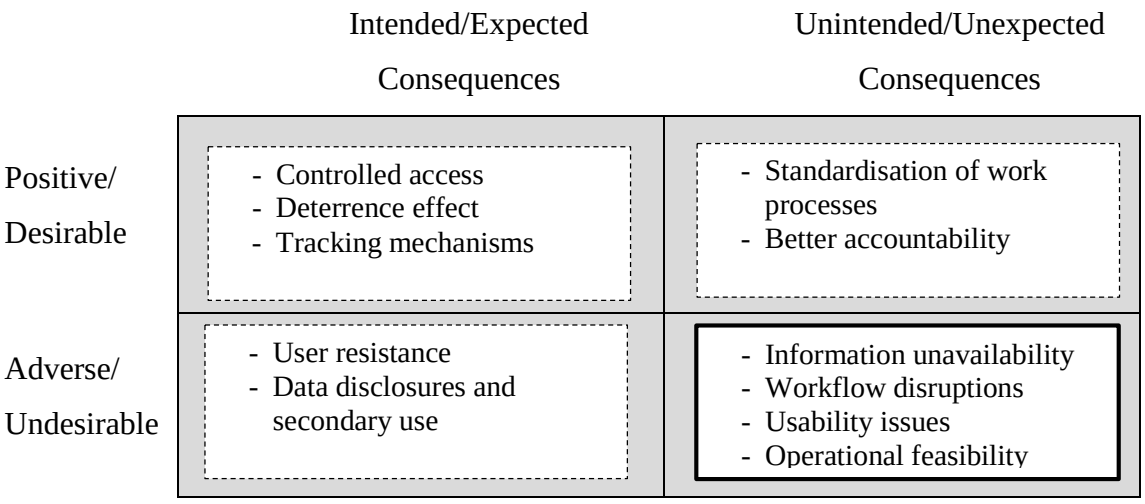

Figure 4. Intended and Unintended Consequences

both protection of patient information and regulatory compliance. In doing so, they implement privacy safeguards to minimise privacy breaches and abide by regulatory pressures.

Our data analysis revealed that the enactment of information privacy protective safeguards influences healthcare workflows through intended and unintended consequences, thus creating the imbalance challenge. Achieving a balance between privacy and utility by maximally reducing unintended negative impacts is challenging because of the dynamic environment of healthcare delivery. The dynamics inherent in medical practices, such as scheduled and unscheduled patient visits, clinicians' unscheduled shifts, dynamic collaborations among clinicians and workforce needed at unexpected times and locations, often conflict with privacy role-based access safeguards (Boxwala *et al.*, 2011; Chen & Xu, 2013) and, thus, make the imbalance challenge even more vital. The intended positive consequences of enacting privacy safeguards may function as a facilitator to privacy compliance, whereas the unintended adverse consequences may function as inhibitors.

When relating the imbalance challenge to the literature, we applied the lens of balance theory to seek an explanation for the contradictory intended and unintended impacts and the imbalance challenge. According to Heider (1946) and Lewin (1951), balance theory is 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. However, contrary to the balance theory's expectation of detachment, our data indicated that once healthcare leaders become aware of unintended impacts, they work on resolving those adverse impacts rather than distancing themselves from them. In situations in which privacy safeguards impede healthcare delivery, healthcare leaders increase their involvement rather than reduce it. For example, when needed information was not available to clinicians, leaders reviewed the policies and a 'break-the-glass' feature was created to allow clinicians to bypass the controls. Also, because of the

penalties associated with privacy breaches, organisations could not afford to avoid taking actions. Hence, balance theory is not the right theoretical lens to fully understand the imbalance challenge.

Likewise, the opposing concepts of negative and positive impacts of the imbalance challenge led us to consider the privacy calculus theory in the privacy literature (e.g, Culnan & Bies, 2003). This theoretical framework has been applied at the individual level (e.g., Dinev & Hart, 2006; Xu *et al.*, 2009; Keith *et al.*, 2013) and provides insights that are worth taking into account at the organisation level. Privacy calculus considers two sets of opposing factors: inhibitors and facilitators to behavioural intentions, such as willingness to conduct online transactions or intentions to disclose information. An individual's decision to transact online is based on the outcome of weighing both sets of factors: if the effects of the facilitating factors (e.g. perceived benefits, trust and control) are greater than those of inhibiting factors (e.g. privacy concerns and perceived risk), the individual is more likely to engage in a transaction. Although it is individuals who make the a priori decisions, the theoretical model of the imbalance challenge pertains to consequences of these decisions at the organisation level. Moreover, privacy calculus allows the individual to 'calculate' whether it is beneficial to engage in a transaction, whereas in the theoretical model of the imbalance challenge, organisations do not calculate but deal with the consequences in the form of the imbalance challenge. To reiterate, the imbalance challenge results from unintended negative impacts outweighing intended positive impacts. Hence, whereas the imbalance challenge does consider costs and benefits, it does not share the same lens or individual-level assumptions of privacy calculus. Hence, privacy calculus is not an accurate theoretical lens to fully understand the imbalance challenge.

Bypassing Privacy Safeguards: Workarounds and Reactance

Our findings suggest that the issues surrounding the organisational struggles to meet the ever-increasing privacy constraints and to comply with regulatory requirements have become a central concern to healthcare leaders. Again, the imbalance challenge emerged as the key concept regarding these struggles. An unattended imbalance challenge can potentially be harmful to the organisation's privacy compliance because, in many cases, employees use this imbalance to justify workarounds and negative reactance to privacy safeguards. These workarounds range from legitimate to not legitimate and finally illegitimate user reactions. A striking example of legitimate use of workarounds was provided by a chief privacy officer who stated that clinicians sometimes bypass privacy safeguards to do their jobs, which involves saving lives. He emphasised that he would rather explain to the Office of Civil Rights why one of the hospital's employees inappropriately accessed information (e.g. used someone else's log-in credentials) rather than having to explain to a family member that he could not save their loved one because of privacy safeguards. The concern surrounding such actions is that the same access that saves lives could also hinder privacy compliance. An illegitimate example of workarounds was provided by the

same chief privacy officer when he referred to the case of an Arizona congresswoman who was admitted to a hospital after being shot and how several employees lost their jobs for inappropriately looking up her medical records. Finally, less legitimate uses of workarounds included bypassing encryption or leaving computer unintended while logged on to save time.

This study provides evidence, with support from the literature, that when unintended adverse impacts outweigh intended ones, healthcare professionals may see a need to improvise or workaround their workflows. For example, information unavailability can be circumvented by users borrowing passwords or smart cards to access records they are not authorised to access (France, 1998). They may also ignore required encryption mechanisms because of their impact on job performance. The potential harm resides in subsequent use of patient information (e.g. copying and transmitting) under different users' log-ins. Extant health informatics literature describes workarounds as clever alternative methods developed by users to accomplish what the system does not easily allow them to do (Ash *et al.*, 2004). Similarly, Morath & 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). Workarounds are recognised in both IS and health informatics literature (Pollock, 2005); however, few studies seek to theoretically explain this concept (Halbesleben *et al.*, 2008), especially with regard to information privacy.

Aside from workarounds, a dangerous unintended consequence organisations may face in a compliance context is negative employee reactance. Recently, in the IS policy compliance literature, this is addressed in terms of negative employee reactance to policies, including pushing back, doing the opposite of what is required, workarounds, malicious compliance and anger (Posey *et al.*, 2011; Lowry & Moody, 2015; Lowry *et al.*, 2015). This literature indicates that these unintended consequences occur because of employees' perceived threats to freedom, perceived unfairness or perceived privacy invasion of the employee. An illustrative example was provided by a chief information officer who stated that nurses within his hospital exhibited reactance towards some of their computer privacy policies by doing the opposite of what is mandated. In fact, 40% of a nurse's work is to administer medication in timely manner to different patients. However, having to log in and log out between patients was getting in the way of delivering care. As a reaction, several nurses were purposely leaving their computers logged on, simply wheeling the machine between rooms or while seeking medication for their patients.

Assessing the Impacts on Organisational Privacy Compliance

In using grounded theory, Urquhart *et al.* (2010) emphasise leveraging a systematic and iterative approach to theory conceptualisation. Embracing this approach enabled us to further analyse the unintended adverse consequences. We pursued a theoretical sampling in an attempt to increase our knowledge of the intended and unintended consequences of privacy safeguard enactment, their impacts on

business practices and their implications for privacy compliance. Further analysis allowed us to distinguish between: (1) organisations where leaders were not aware of the unintended negative impacts and (2) organisations where leaders were aware of the unintended 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, unaware leaders indicated that there were no formal metrics in place to assess the impacts and consequences, intended or unintended, of privacy safeguard enactment. Instead, they relied on the number of complaints or reported privacy breaches as an indication of the effectiveness of their privacy safeguards. Once these leaders became aware of the unintended adverse impacts, they considered revisiting their safeguards to account for the imbalance challenge. In these instances, awareness only happened when privacy compliance became an issue for the organisation. Clearly, this is a dangerous and suboptimal approach, because it relies on reactive assessment of negative privacy breaches. If the organisations' privacy compliances were not in jeopardy, would the leaders have ever become aware of any unintended adverse impacts? Moreover, such an approach waits for catastrophic privacy breaches to further inform policy development.

Additional analysis revealed that leaders who were aware of the unintended adverse impacts performed some sort of privacy risk assessment a priori instead of waiting for breaches to occur. Such initiatives enabled leaders to look out for these impacts and sometimes to prevent or minimise them. Ultimately, a proactive assessment versus a reactive approach distinguishes these two types of organisations and further explains the imbalance challenge. Indeed, organisations that take a proactive approach try to develop privacy metrics (see Appendix H) to assess unintended adverse impacts and therefore limit workarounds and increase the level of their overall privacy compliance.

Research Contributions and Implications

To date, most studies on privacy focus on designing and implementing the appropriate safeguards to mitigate information privacy threats. The key limitation of this literature, however, is that it generally assumes only expected positive consequences and does not consider negative consequences or unintended consequences. Hence, this research lacks a realistic grounding in actual healthcare privacy practice. Accordingly, there have been recent calls for research to investigate the effectiveness and consequences of enacting privacy safeguards; as Belanger & Crossler (2011) point out: 'there are many behavioural questions to be explored with respect to not only use of potential privacy protection tools but also effectiveness and consequences of use' (p. 1022). Similarly, this void in extant privacy literature is also identified in an interdisciplinary literature review by Smith *et al.* (2011), which highlights the need for more privacy research to consider actual outcomes. By using an interpretive approach, our study was able to capture and gain insights into how healthcare executives understand the process by which individual privacy safeguards are evaluated and subsequently bypassed and the resulting influences on the

organisation's privacy compliance. This led to the development of our emergent theoretical framework, the UCPSE framework.

Methodologically, using grounded theory provides a rich lens through which to understand the consequences of privacy safeguards and their implications for privacy compliance. We selected grounded theory because of the lack of extant theory to explain how organisations interpret the implications of privacy safeguards, the context of the healthcare domain provides practical relevance and suitability to study healthcare processes. This grounded theory study spanned over 16 months, during which we interviewed 30 privacy leaders from several healthcare organisations, including government agencies, uncovering subtle organisational 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 informants was crucial for reaching data saturation.

This study contributes to the need for interdisciplinary research by converging the research streams of both IS and health informatics, uncovering the challenges that healthcare organisations face and presenting an in-depth overview of privacy management within the healthcare domain. In doing so, we uncovered and defined the rich construct of the imbalance challenge. In contrast to previous research involving balance theory and privacy calculus, we make the case for the uniqueness of the imbalance challenge and why a new theoretical framework (the UCPSE) was needed to understand it. Contrary to the balance theory's expectation of detachment, our data indicated that once healthcare leaders become aware of unintended impacts, they work to resolve those adverse impacts rather than distance themselves from them. In other words, in situations in which privacy safeguards were in the way of healthcare delivery, healthcare leaders increased their involvement rather than reduced it.

Likewise, the consumer theory of privacy calculus also does not fit well, because the imbalance challenge pertains to consequences of these decisions at the organisation level. Privacy calculus allows the individual to 'calculate' whether it is beneficial to engage in a transaction, whereas in the UCPSE framework, organisations do not calculate but deal with the consequences in the form of the imbalance challenge. The imbalance challenge results when the unintended negative impacts outweigh the intended positive impacts. Hence, whereas the imbalance challenge does consider costs and benefits, it does not do so from the same lens or individual-level assumptions seen in privacy calculus. Hence, privacy calculus is not an accurate theoretical lens to fully understand the imbalance challenge. We contribute to key theoretical products that are highly contextualised and unique to the healthcare privacy context: namely, a rich construct (the imbalance challenge) and a framework (the UCPSE framework). Hassan & Lowry (2015) explain how original IS theory cannot emerge without richly contextualised constructs, because the core of theory is in its unique constructs. Interestingly, they also explain how grounded theory is an excellent starting place for concepts and constructs to emerge so that they lack superficiality. Meanwhile,

they explain how frameworks are highly useful in setting out the territory for research, including its key constructs and their relationships.

Finally, none of these insights would be possible without conducting organisational-level data collection on privacy issues, which is rarely done. This research provides new theoretical insights into understanding privacy management by targeting the organisation level of analysis through a grounded theory approach. In the IS field, Smith *et al.* (2011) make an explicit call for research on studying information privacy at the organisation level (p. 1006):

> *Indeed, most rigorous studies of organisational privacy policies and practices would likely include a set of exhaustive interviews with an organisation'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 organisational dynamics that drive privacy policies and practices.*

Thus, while collecting organisational-level data, we carefully evaluated it through Strauss and Corbin's (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).

Implications and Suggestions for Healthcare Professionals

The dynamics between enacting privacy safeguards and ensuring privacy compliance constitute a major concern for healthcare executives. We investigate this relationship by introducing the imbalance challenge, which perspective encourages healthcare practitioners to evaluate intended and unintended consequences of privacy safeguards enactments. The imbalance challenge is the result of unintended consequences outweighing intended consequences of privacy safeguards enactments. Such imbalance may lead to workarounds that can be counterintuitive to the privacy safeguards in place.

To minimise the imbalance challenge, first we propose that practitioners embrace a proactive approach in their privacy safeguards enactment. Such approach should start by instating a privacy impact assessment tool (See Appendix H) supplemented with a column that tracks the impact and/or workarounds of each item on business practices. Such approach creates an environment of awareness and monitoring. Furthermore, healthcare practitioners should strive to develop a culture of continuous, rather than one-time privacy risk assessment that examines the cycle of threats, actions and impact. To facilitate this continuous assessment, we propose establishing triggers to alert administrators of common conditions that may indicate workarounds may be occurring. As illustration, when a nurse or physician is not logged in while present during his/her shift, an alert should be established for further investigation as the nurse/physician may be using someone else's login credentials. Likewise, if a nurse or physician is logged in past his/her shit that would indicate the possibility of accidental open access to their account, which should also be investigated.

Second, our data analysis reveals different level of workarounds from legitimate, less legitimate to illegitimate. We propose that practitioners embrace this distinction as workarounds to save lives are very distinct from workarounds to save time or workarounds that involve malicious data abuse. Hence, accounting for and/or revisiting privacy safeguards to create a 'break the glass' feature – when lives are involved. 'Break the glass' is an escape mechanism that allows certain users to escape the domain constraint (Lovis *et al.*, 2007) and thereby bypass role-based access control privacy mechanisms. Through 'break the glass,' the physician would justify his or her need to access a particular patient's information and he will be granted access.

Third, practitioners should re-evaluate their policies and privacy processes by involving all stakeholders including but not limited to physicians, nurses, administrators, insurance companies, and business associates. For example when privacy policy or process is impacting 40% of a nurse work by having to log in and log off when she see the patient, when she leaves to get medication and when she gets back to administer several times a day, he/she will embrace workarounds such as leaving her computer logged in. The more different stakeholders are involved in the practice of privacy, the less likelihood of negative consequences. This is also why mere privacy policies alone (unless developed with stakeholders and carefully monitored and enforced) can be highly superficial and virtually meaningless to an organization. What is needed is real privacy advocacy and protection built as a process into an organization, and led by senior management.

It is important for healthcare executives to understand that an effective way to minimize the imbalance challenge begins with efforts to minimize the unintended consequences. Through the above discussed implications, our study has created a preliminary benchmark by which healthcare executives can better account for unintended consequences and ultimately achieve privacy compliance.

Study Limitations and Future Research Opportunities

This study has several limitations that suggest future research opportunities. Regarding the validity of an emergent theory, it is worth referring to generalisability, which is 'the validity of a theory in a setting different from the one where it was empirically tested and confirmed' (Lee & Baskerville, 2003, p. 221). Lee & Baskerville (2003) clarify that the appropriate type of generalisability (not only statistical) should be applied to this particular type of theory-development study. The purpose of our study was not to achieve statistical validation but to discover patterns for the purpose of theory building and to gain a better understanding of the main issues in this context. It is reasonable to assume that the insights from this emergent framework would guide future research to a more formal theory (Orlikowski, 1993). Hence, additional data collection and testing are needed to further clarify this study's findings and to formalise its framework into theory. Likewise, more empirical and theoretical work is needed that more closely examines the relationships among privacy safeguard enactment, the imbalance challenge, workarounds

and privacy compliance. In doing so, longitudinal data would be useful so that a better understanding of the underlying casual mechanisms can emerge.

Moreover, another limitation of this study is that the findings are based solely on the U.S. hospitals. There could be differences in other countries because of differences in legal systems and basic economic structures. Moreover, some IS researchers demonstrate that there are differences in information privacy issues across countries and cultures (Milberg *et al.*, 2000; Bellman *et al.*, 2004; Posey *et al.*, 2010; Lowry *et al.*, 2011). Hence, another research opportunity would be a comparative study of the factors impacting this imbalance, taking into consideration country and cultural influences.

Finally, several of the phenomena we observed can be further studied in terms of lower-order causal mechanisms and IT artefacts. As an example, we showed that the presence of accountability is a positive privacy facilitation factor in several organisations. However, no one has studied the lower-order components of accountability in this privacy context. Accountability theory proposes several mechanisms that increase accountability perceptions and subsequent organisational policy compliance (Vance *et al.*, 2013, 2015): identifiability, expectation of evaluation, awareness of monitoring and social presence. Vance *et al.* empirically validate these and tie them to IT artefact design in security compliance settings. Similar IT artefact, design-oriented research could be highly useful in a healthcare domain, especially because many medical systems have broad access so that many different medical practitioners can access patient information.

Conclusion

The recent literature suggests that most extant information privacy research focuses on the creation of privacy safeguards and neglects the actual consequences of enacting the practices in which organisations engage. An imbalance challenge occurs when the unintended consequences outweigh the intended consequences of privacy safeguard enactment. To address the imbalance challenge, organisations need to achieve a balance between privacy and utility, meeting privacy requirements without impeding workflows. Using an interpretive grounded theory research approach, this study investigates the consequences of privacy safeguards and their effects on meeting privacy requirements without impeding workflow in medical practices.

This research responds to a theoretical challenge that was overlooked in prior research, and it makes several contributions. First, it introduces a theoretical framework (the UCPSE) that explicates the process by which both the intended and unintended consequences of implementing privacy safeguards are evaluated and bypassed and the impacts on organisational privacy compliance. Second, this study was designed to gain an in-depth understanding of the actual outcomes and implications of privacy safeguards in healthcare organisations. Therefore, using a grounded theory methodology provides a rich lens to understand the actual consequences of privacy safeguards and their implications for privacy compliance.

Recognising the state of imbalance where unintended consequences outweigh intended consequences constitutes a strong conceptual foundation for the impacts of enacting privacy safeguards. Third, this research contributes to the recent call for interdisciplinary research by converging the research streams of both IS and health informatics and presents an in-depth view of privacy management within the healthcare domain. Fourth, this study responds to the lack of organisation-level privacy research and provides new theoretical insights into understanding privacy management by targeting this under-researched level of analysis through a grounded theory approach.

References

ABERDEEN J, BAYER S, YENITERZI R, WELLNER B, CLARK C, *et al.* (2010) The MITRE Identification Scrubber Toolkit: Design, training, and assessment. *International Journal of Medical Informatics* 79(12), 849-859.

AHA (2016) Section for small or rural hospitals.

ASH JS, BERG M and COIERA E (2004) 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(2), 104-112.

BELANGER F and CROSSLER RE (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 36(4), 1017-1041.

BELLMAN S, JOHNSON EJ, KOBRIN SJ and LOHSE GL (2004) International differences in information privacy concerns: A global survey of consumers. *The Information Society* 20(5), 313-324.

BLANQUER I, HERNÁNDEZ V, SEGRELLES D and TORRES E (2009) Enhancing privacy and authorization control scalability in the grid through ontologies. *IEEE Transactions on Information Technology in Biomedicine* 13(1), 16-24.

BLOBEL B, NORDBERG R, DAVIS JM and PHAROW P (2006) Modelling privilege management and access control. *International Journal of Medical Informatics* 75(8), 597-623.

BOSS SR, GALLETTA DF, LOWRY PB, MOODY GD and POLAK P (2015) What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly* 39(in press).

BOXWALA AA, KIM J, GRILLO JM 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), 498-505.

BOYD AD, HOSNER C, HUNSCHER DA, ATHEY BD, CLAUW DJ, *et al.* (2007) An 'Honest Broker'mechanism to maintain privacy for patient care and academic medical research. *International journal of medical informatics* 76(5), 407-411.

BROWN KL (2000) Analyzing the role of the project consultant: Cultural change implementation. *Project Management Journal* 31(3), 52-55.

BULGURCU B, CAVUSOGLU H and BENBASAT I (2010) Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. [Article]. *MIS Quarterly* 34(3), 523-A527.

CAMPBELL EM, SITTIG DF, ASH JS, GUAPPONE KP and DYKSTRA RH (2006) Types of unintended consequences related to computerized provider order entry. *Journal of the American Medical Informatics Association* 13(5), 547-556.

CANIM M, KANTARCIOGLU M and MALIN B (2012) Secure management of biomedical data with cryptographic hardware. *IEEE Transactions on Information Technology in Biomedicine* 16(1), 166-175.

CHEN K, CHANG YC and WANG DW (2010) Aspect-oriented design and implementation of adaptable access control for electronic medical records. *International Journal of Medical Informatics* 79(3), 181-203.
CHEN Y and XU H (2013) Privacy management in dynamic groups: Understanding information privacy in medical practices. In *16th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*, pp 541-552, San Antonio, TX.
CHOE J and YOO SK (2008) Web-based secure access from multiple patient repositories. *International Journal of Medical Informatics* 77(4), 242-248.
CHOI YB, CAPITAN KE, KRAUSE JS and STREEPER MM (2006) Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules. *Journal of Medical Systems* 30(1), 57-64.
CLAERHOUT B and DEMOOR G (2005) Privacy protection for clinical and genomic data: The use of privacy-enhancing techniques in medicine. *International Journal of Medical Informatics* 74(2), 257-265.
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), 129-140.
COOPER HM (1998) Synthesizing Research: A Guide for Literature Reviews. (Vol. 2). Sage.
CORBIN JM and STRAUSS AL (2008) Basics of Qualitative Research: Grounded Theory Procedures and Techniques. (3rd ed.). Sage, Newbury Park, CA.
CROLL PR (2011) Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling. *International Journal of Medical Informatics* 80(2), e32-e38.
CROSSLER RE, JOHNSTON AC, LOWRY PB, HU Q, WARKENTIN M, *et al.* (2013) Future directions for behavioral information security research. *Computers & Security* 32(1), 90-101.
CULNAN MJ and BIES RJ (2003) Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues* 59(2), 323-343.
CULNAN MJ and WILLIAMS CC (2009) How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly* 33(4), 673-687.
D'ARCY J, HOVAV A and GALLETTA D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20(1), 79-98.
DHILLON G and MOORES TT (2001) Internet privacy: Interpreting key issues. *Information Resources Management Journal* 14(4), 33-37.
DINEV T and HART P (2006) An extended privacy calculus model for e-commerce transactions. [Article]. *Information Systems Research* 17(1), 61-80.
EISENHARDT KM (1989) Building theories from case study research. *Academy of Management Review* 14(4), 532-550.
FERNANDO JI and DAWSON LL (2009) The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics* 78(12), 815-826.
FRANCE FHR (1998) Ethics and biomedical information. *International Journal of Medical Informatics* 49(1), 111-115.
GLASER BG and STRAUSS AL (1967) The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine de Gruyter, New York, NY.
GREENAWAY KE and CHAN YE (2005) Theoretical explanations for firms' information privacy behaviors. *Journal of the Association for Information Systems* 6(5), 171-198.
GRITZALIS S, LAMBRINOUDAKIS C, LEKKAS D and DEFTEREOS S (2005) Technical guidelines for enhancing privacy and data protection in modern electronic medical environments. *IEEE Transactions on Information Technology in Biomedicine* 9(3), 413-423.
HAAS S, WOHLGEMUTH S, ECHIZEN I, SONEHARA N and MÜLLER G (2011) Aspects of privacy for electronic health records. *International Journal of Medical Informatics* 80(2), e26-e31.

HALBESLEBEN JR, WAKEFIELD DS and WAKEFIELD BJ (2008) Work-arounds in health care settings: Literature review and research agenda. *Health Care Management Review* 33(1), 2-12.
HARRISON MI, KOPPEL R and BAR-LEV S (2007) Unintended consequences of information technologies in health care—An interactive sociotechnical analysis. *Journal of the American Medical Informatics Association* 14(5), 542-549.
HASSAN NR and LOWRY PB (2015) Seeking middle-range theories in information systems research. In *International Conference on Information Systems (ICIS 2015)*, AIS, Fort Worth, TX.
HEIDER F (1946) Attitudes and cognitive organization. *Journal of Psychology* 21(1), 107-112.
HHS (2016) Breaches affecting 500 or more individuals. March 12, 2016, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
HSU J, SHIH S-P, HUNG YW and LOWRY PB (2015) How extra-role behaviors can improve information security policy effectiveness. *Information Systems Research* 26(2), 282-300.
HU Q, XU Z, DINEV T and LING H (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM* 54(6), 54-60.
JOHNSON CM, JOHNSON TR and ZHANG J (2005) A user-centered framework for redesigning health care interfaces. *Journal of Biomedical Informatics* 38(1), 75-87.
KANTARCIOGLU M, JIANG W, LIU Y and MALIN B (2008) A cryptographic approach to securely share and query genomic sequences. *IEEE Transactions on Information Technology in Biomedicine* 12(5), 606-617.
KAUNITZ AM, GRIMES DA, HUGHES JM, SMITH JC and HOGUE JR. C (1984) Maternal deaths in the United States by size of hospital. *Obstetrics & Gynecology* 64(3), 311-314.
KEITH MJ, THOMPSON SC, HALE J, LOWRY PB and GREER C (2013) Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies* 71(12), 1163-1173.
KREINER GE, HOLLENSBE EC and SHEEP ML (2006) Where is the "me" among the "we"? Identity work and the search for optimal balance. *Academy of Management Journal* 49(5), 1031-1057.
KUSHNIRUK A (2002) Evaluation in the design of health information systems: Application of approaches emerging from usability engineering. *Computers in Biology and Medicine* 32(3), 141-149.
KUSHNIRUK AW and PATEL VL (2004) Cognitive and usability engineering methods for the evaluation of clinical information systems. *Journal of Biomedical Informatics* 37(1), 56-76.
LAL D (2001) Unintended Consequences: The Impact of Factor Endowments, Culture, and Politics on Long-Run Economic Performance. (Vol. 7). MIT Press, Cambridge, MA.
LE ROUGE CM and DE LEO G (2010) Information systems and healthcare XXXV: Health informatics forums for health information systems scholars. *Communications of the Association for Information Systems* 27(7), 99-112.
LEE AS and BASKERVILLE RL (2003) Generalizing generalizability in information systems research. *Information Systems Research* 14(3), 221-243.
LEE WB and LEE CD (2008) A cryptographic key management solution for HIPAA privacy/security regulations. *IEEE Transactions on Information Technology in Biomedicine* 12(1), 34-41.
LERNER JS and TETLOCK PE (1999) Accounting for the effects of accountability. *Psychological Bulletin* 125(2), 255-275.
LEWIN K (1951) Field Theory in Social Science: Selected Theoretical Papers. Harpers, Oxford, UK.
LI M, CARRELL D, ABERDEEN J, HIRSCHMAN L and MALIN BA (2014) De-identification of clinical narratives through writing complexity measures. *International Journal of Medical Informatics* 83(10), 750-767.
LINCOLN YS and GUBA EG (1985) Naturalistic Inquiry. (Vol. 75). Sage.
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), 466-470.

LOWRY PB, CAO J and EVERARD A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems* 27(4), 163-200.
LOWRY PB, GASKIN J, TWYMAN NW, HAMMER B and ROBERTS TL (2013) Taking 'fun and games' seriously: Proposing the hedonic-motivation system adoption model (HMSAM). *Journal of the Association for Information Systems* 14(11), 617-671.
LOWRY PB and MOODY GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal* 25(5).
LOWRY PB, POSEY C, BENNETT RJ and ROBERTS TL (2015) Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal* 25(3), 193-230.
LOWRY PB, SPAULDING T, WELLS T, MOODY GD, MOFFIT K, *et al.* (2006) A theoretical model and empirical results linking website interactivity and usability satisfaction. In *39th Annual Hawaii International Conference on System Sciences (HICSS 2006)*, pp 1-9, IEEE, Kaui, HI.
LYYTINEN K, BASKERVILLE R, IIVARI J and TE'ENI D (2007) Why the old world cannot publish? Overcoming challenges in publishing high-impact IS research. *European Journal of Information Systems* 16(4), 317-326.
MAGASIN M and GEHLEN FL (1999) Unwise decisions and unanticipated consequences. *Sloan Management Review* 1999(Fall), 37-60.
MILBERG SJ, SMITH HJ and BURKE SJ (2000) Information privacy: Corporate management and national regulation. *Organization Science* 11(1), 35-57.
MILNE GR and CULNAN MJ (2002) Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998–2001 U.S. web surveys. *Information Society* 18(5), 345-359.
MOHAN J and YAACOB RRR (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), 217-227.
MORATH JM and TURNBULL JE (2005) To do no harm: ensuring patient safety in health care organizations. Jossey-Bass, San Francisco, CA.
MURPHY A, REDDY M and XU H (2014) Privacy practices in collaborative environments: A study of emergency department staff. In *17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*, pp 269-282, ACM, Baltimore, MD.
NORD GD and MCCUBBINS TF (2006) Privacy, legislation, and surveillance software. *Communications of the ACM* 49(8), 73-78.
OHNO-MACHADO L, SILVEIRA PSP and VINTERBO S (2004) Protecting patient privacy by quantifiable control of disclosures in disseminated databases. *International Journal of Medical Informatics* 73(7), 599-606.
ORLIKOWSKI WJ (1993) CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS Quarterly* 17(3), 309-340.
PARKS R, CHU C and XU H (2011a) Healthcare information privacy research: Issues, gaps and what next. In *17th Americas Conference on Information Systems (AMCIS)*, AIS, Detroit, MI.
PARKS R, CHU C, XU H and ADAMS L (2011b) Understanding the drivers and outcomes of healthcare organizational privacy responses. In *32nd Annual International Conference on Information Systems (ICIS 2011)*, Shanghai, China.
PESLAK AR (2006) Internet privacy policies of the largest international companies. *Journal of Electronic Commerce in Organizations* 4(3), 46-62.
POLLOCK N (2005) When is a work-around? Conflict and negotiation in computer systems development. *Science, Technology & Human Values* 30(4), 496-514.

POSEY C, BENNETT RJ, ROBERTS TL and LOWRY PB (2011) When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security* 7(1), 24-47.
POSEY C, LOWRY PB, ROBERTS TL and ELLIS S (2010) Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems* 19(2), 181-195.
PRC (2016) Chronology of data breaches security breaches 2005. March 18, 2016, http://www.privacyrights.org/data-breach.
QUANTIN C, ALLAERT F-A and DUSSERRE L (2000) Anonymous statistical methods versus cryptographic methods in epidemiology. *International Journal of Medical Informatics* 60(2), 177-183.
RAVERA L, COLOMBO I, TEDESCHI M and RAVERA A (2004) Security and privacy at the private multispecialty hospital istituto clinico humanitas: Strategy and reality. *International Journal of Medical Informatics* 73(3), 321-324.
ROGERS EM (1998) Diffusion of Innovations. Free Press, New York, NY.
SIPONEN M and VANCE A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. [Article]. *MIS Quarterly* 34(3), 487-A412.
SMITH J (1993) Privacy policies and practices: Inside the organizational maze. *Communications of the ACM* 36(12), 104-104.
SMITH JH, DINEV T and XU H (2011) Information privacy research: An interdisciplinary review. *MIS Quarterly* 35(4), 989-1015.
STRAUSS AL and CORBIN JM (1998) Basics of Qualitative Research. Techniques and Procedures for Developing Grounded Theory. Sage, Thousand Oaks, CA.
TADMOR C and TETLOCK PE (2009) Accountability. In *The Cambridge Dictionary of Psychology* (MATSUMOTO D, Ed.), p 8, Cambridge University Press, Cambridge.
URQUHART C, LEHMANN H and MYERS MD (2010) Putting the 'theory'back into grounded theory: guidelines for grounded theory studies in information systems. *Information Systems Journal* 20(4), 357-381.
VAN MAANEN J and SCHEIN EH (1979) Toward a theory of organizational socialization. *Research in Organizational Behavior* 1(1), 209-264.
VANCE A, LOWRY PB and EGGETT D (2013) Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems* 29(4), 263-289.
VANCE A, LOWRY PB and EGGETT D (2015) A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly* 39(2), 345-366.
WALCZUCH RM and STEEGHS L (2001) Implications of the new EU directive on data protection for multinational corporations. *Information Technology and People* 14(2), 142-162.
WALL JD, LOWRY PB and BARLOW J (2015) Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems* forthcoming.
XU H, TEO H-H, TAN BC and AGARWAL R (2009) The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems* 26(3), 135-174.
YEH QJ and CHANG AJT (2007) Threats and countermeasures for information system security: A cross-industry study. *Information & Management* 44(5), 480-491.

Appendix A. Summary of Data Sources

Organisation	Organisation Type	Informant #	Title
1	Large Hospital	1	Chief Medical Information Officer
2	Medium Hospital	2	Chief Information Officer
		3	Chief Privacy Officer
3	Large	4	Chief Medical Information Officer
4	Healthcare Association	5	President
5	Healthcare Federal Agency	6	Chief Privacy Officer
6	Medium Hospital	7	Vice President of IT
7	Medium Hospital	8	Chief Privacy Officer
		9	Security Officer
8	Large Hospital	10	Chief Privacy Officer
		11	Privacy Officer
9	EMR vendor and cloud manager	12	Vice President Implementations
10	Small Hospital	13	Chief Executive Officer
11	Medium Hospital	14	IT Director
12	Large Hospital	15	Security Officer
13	Medium Hospital	16	Privacy Officer
14	Research/Consulting Firm	17	Chief Privacy Officer
15	Small Hospital	18	Privacy Officer
		19	IT Director
16	Large Hospital	20	Privacy Officer
17	Large Hospital	21	Security Officer
18	Consulting Firm	22	Chief Executive Officer
19	Small Hospital	23	Chief Information Officer
20	Medium Hospital	24	Chief Information Officer
21	Small Hospital	25	Business Executive Director
		26	Vice President
		27	Director of Health Information Management
		28	Healthcare Executive Director
		29	Privacy Officer
		30	IT Director

Appendix B. 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 organisation 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 organisation face in developing and enacting these privacy programs?
    - How does your organisation 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 C. 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 organisations in general
        i. Different Types, levels
        ii. Challenges
2. Privacy Measures
    a. What types of measures does your organisation 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 organisation to initiate these particular measures? (What prompted your hospital to initiate these measures?)
    c. Are your organisation'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 organisation 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 organisation 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 organisation 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 organisation 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 D. Illustrative Supporting Data for Unintended Consequences

2nd Order Themes	Illustrative 1st Order Data
Unintended/Desirable Consequences	
Standardization of Work Processes	• 'For us privacy we consider a component of quality healthcare. In other words, patients come to us and divulge very private information to us, and we are the protectors of that. We must make sure that it's handled appropriately … provide them basic stuff of making sure people close curtains, close doors, they position their computers and equipment so that people can't read or see the information'. • 'Say you had your Facebook account and you decide you want to say something bad about [our hospital], what do you do then? There has to be some procedures and protocols around that'. • 'In an emergency department or you are in a clinic setting, information being electronically viewable so you have to say where the device is, where the devices set up, the time outs and things, are they consistent with a comprehensive approach to visually securing any information ' • 'We have to assess each outside agency as to what their needs are and how to best set a special, private VPN channel that's highly secured that we only allow people in through that area that we can govern who comes in, when they come in, what their passwords are and so forth. And we can govern the movement of the data that way'.
Better Accountability	• 'You basically have to assess the situation, make the determination of what should be done. I will be honest with you. We will opt for patient safety and patient care above everything…the patient's life is in our hands and we are going to do what it takes to take care of that patient'. • 'I believe that most organisations now are much more aware of privacy and security than they were before that law came into place. And just seeing this as just a good business practice instead of something we have to do, makes all the difference in the world. I have heard some of the techy people call it hygienic environment'.
	• 'I try to make decisions here of course I want to do what's right for the business and our workflow. But at the same time at the end of the day I kind of put myself in a patient's viewpoint'. • I do think that there are a number of motivating factors. One of them is the right thing to do and that is the right attitude, and that would get you a lot further than going off checking off check boxes
Unintended Adverse Consequences	
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'. • 'We try to make it [information] 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	• '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'. • 'Once I log in, I don't want the system to log me out automatically. I don't like it'. • '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, and 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. 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 comes down to operational feasibility and weather what's being asked 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'. • '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 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'.

Appendix E. Illustrative Supporting Data for Intended or Expected Consequences

2nd Order Themes	Illustrative 1st Order Data
Intended/Desirable Consequences	
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'.
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 co-workers 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'.
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'.
Expected Adverse consequences	
User Resistance	• 'If there's a change in the regulation or policy, existing business process has to be altered or changed. Any time there's change there's going to be push back or potential disagreement'. • '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?' • • 'To use a safe password, is has to be eight characters long, it should have caps and this and that, and you change it every thirty days, and nobody does it'.
Data Disclosures & Secondary Use	• 'How do you secure information that is being used for secondary purposes for research, for research, for quality, for billing and coding'? • 'I think the very difficult issue we face is that there is a great need for secondary uses of health data. That's where much of the information comes from, we are now using for research for public health. And so to be able to find cures for diseases or to improve public health, to improve disparities, to improve access to care, all those many things that are on everyone's mind. When you're thinking about healthcare improvement, you need data to be able to do that. You need the research'. • 'There's many times when like a clerical person will hit the wrong number on the fax machine and fax a, a lab result for Rachida Parks to a Sheetz store or something and you know that happens all the time'.

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 1) that aims to depict the processes as a result of enacting privacy safeguards. The variance intended and unintended consequences
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 account?	Check if process has been considered.	This study focuses on understanding the outcomes of enacting privacy safeguards and 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 hospitals. However, after initial data analysis, this target was revisited to include other healthcare organisations 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-organisations 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, intended consequences, unintended consequences, 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 categories prove to be?	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., 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 leaders who exhibited very distinct behaviours regarding their approaches to responding to privacy threats, while others' behaviours 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, categories and themes were improved. Some did not hold up. For instance, at early stages of data analysis, we formulated the hypothesis that larger hospitals with more resources would thrive to achieve higher degree of privacy compliance and better address the imbalance issues. We further analysed 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.

Appendix H: Sample Privacy and Security Assessment Tool

Privacy and Security Assessment Tool				
Business Associate Name:		Date:		
Specific Requirement	Present	Absent	NA or See Comments	Comments
Privacy Standard				
1) Privacy/confidentiality policies and procedures designed to protect [hospital name] data.				
2) Policy or procedure that describes the allowed use and/or disclosure of [hospital name] data in accordance with the Business Associate Agreement.				
3) Procedure for the reporting of any suspected or actual intrusion, unauthorized use, or disclosure of [hospital name] data.				
4) A sample of your log of potential or actual intrusion, unauthorized use or disclosure of [hospital name] data.				
5) If required, is the following present: Template of the "confidentiality / Non-disclosure Agreement with the subcontractor. A list of any off-shore subcontractors who have access to [hospital name] member data.				
6) Procedure that describes how you allow for the amendments to [hospital name] data.				
7) Procedure for tracking non-routine disclosures or access of [hospital name] data.				
8) Documentation that describes your HIPAA privacy/security training for staff or others who would have access to [hospital name] data.				
9) A template of the confidentiality agreement that you require your employees to sign.				
10) Procedure that describes how you forward privacy questions or privacy requests from [hospital name] members to [hospital name].				

11) Policy requiring contact with [hospital name] prior to any use and/or disclosure of [hospital name] data beyond the defined obligations listed in the Business Associate Agreement.				
Security Standard				
Administrative Safeguards				
1) Policy or process for conducting an assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of [hospital name] data.				
2) Evidence of an assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of [hospital name] data.				
3) Process or procedures for implementing security measures to reduce risks and vulnerabilities to the confidentiality, integrity and availability of [hospital name] data.				
4) Policy or procedure for sanctions due to employee violations of your organisation's security policies and procedures.				
5) Process or procedure to regularly review records of information system activity, such as, audit logs, access reports, and security incident tracking reports.				
6) Evidence of an identified and documented responsibility of the security official accountable for the development and implementation of information security policies and procedures.				
7) Policy or procedure for protecting [hospital name] data from the other functions of the larger organisation if health care clearinghouse functions are performed.				
8) Policy and/or procedures to address security incidents.				
9) Policy and/or procedures for the backup of [hospital name] data.				
10) Evidence of a formal disaster recovery plan.				
11) Evidence of testing your disaster recovery plan within the last 12 months.				
12) Process or procedures to maintain security of [hospital name] data while operating in				

emergency mode due to technical failure or power outage.				
13) Procedure for performing periodic technical and nontechnical evaluations (auditing) to ensure that appropriate security has been implemented. (The evaluation may be internal or external.)				
14) Policy or procedure for reviewing existing business associate contracts, which involve [hospital name] data, to determine if HIPAA Security Rule requirements are addressed.				
Physical Safeguards				
1) Policy and/or procedures for ensuring that workstations capable of accessing [hospital name] data have been identified, their viewing areas limited to authorized users, and have been physically removed from areas where unauthorized users might see the information.				
2) Policy and/or procedures to ensure physical safeguards have been put in place to ensure that all servers and workstations that can access [hospital name] data are restricted to authorized users.				
3) Policy and/or procedure for allowing employees or organisations to remove [hospital name] data in either paper or electronic form from your facility(s).				
4) Policy and/or procedure for allowing employees access to [hospital name] data from a remote location, i.e. home, hotels, or public locations.				
5) Policy and/or procedure to address how [hospital name] data and software should be properly disposed, including any hardware or electronic media on which it is stored.				
6) Policy and procedure for removal of [hospital name] data from electronic media prior to making the media available for re-use.				
Technical Safeguards				
1) Policy and procedure to ensure that each user has a unique ID that can be used to track user activity within the system.				
2) Policy and/or procedure to identify users who would require access and to provide access to [hospital name] data during emergency situations.				

3) List and describe the audit control mechanisms implemented to record and examine activity in the system(s) containing [hospital name] data.				
4) List and describe the type of user authentication mechanisms currently used to ensure user authentication.				