A STUDY OF ORGANIZATIONAL RESPONSES TO INFORMATION PRIVACY THREATS IN THE HEALTHCARE CONTEXT

A Dissertation in
Information Sciences and Technology

by

Rachida Fachtal Parks

© 2012 Rachida Fachtal Parks

Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

August 2012
The dissertation of Rachida Fachtal Parks was reviewed and approved* by the following:

**Chao-Hsien Chu**  
Professor of Information Sciences and Technology  
Dissertation Co-Advisor  
Co-Chair of Committee

**Heng Xu**  
Associate Professor of Information Sciences and Technology  
PNC Technologies Career Development Professorship  
Dissertation Co-Advisor  
Co-Chair of Committee

**Sandeep Purao**  
Professor of Information Sciences and Technology

**Barbara Gray**  
Professor of Organizational Behavior

**Allen Lee**  
Professor of Information Systems  
Special Member  
Virginia Commonwealth University

**Mary Beth Rosson**  
Professor of Information Sciences and Technology  
Director of Graduate Programs

*Signatures are on file in the Graduate School
ABSTRACT

The proliferation of digitized healthcare holds great promise for sharing medical data, improving healthcare quality, saving patient lives, and reducing costs. However, these potential benefits also draw much attention to the issue of information privacy. In the presence of increasing penalties for non-compliance, reputational loss, and privacy operational issues, organizations must find ways to appropriately respond to privacy threats without impeding healthcare workflow and work practices. Thus, the broad research question examined in this study is: How do healthcare organizations respond to information privacy threats and issues?

This dissertation reports the results of a grounded theory study investigating the organizational responses to information privacy threats. The empirical evidence has been derived from healthcare organizations within the United States of America. The key finding is the emergence of the Privacy Impact Assessment, a central element in the process of effective organizational response to information privacy threats. Assessing the influences and dynamics of different drivers, while simultaneously accounting for the intended (positive impacts) and unintended (negative impacts) consequences is critical to understanding the processes by which organizations respond to privacy threats. The findings are summarized within a theoretical framework of organizational responses to information privacy threats.

The theoretical framework developed from this work is stated below:
The Privacy Impact Assessment (PIA) within healthcare organizations is shaped by a dynamic interplay between privacy threats, organizational drivers, and the Imbalance Challenge. Responding to privacy threats without accounting for the Imbalance Challenge causes potential negative operational impacts to outweigh positive impacts. Therefore, the Privacy Impact Assessment is characterized by the iteration between undertaking a risk assessment of privacy threats and existing drivers, management of privacy safeguards, and evaluation of their impacts. In order to manage this process, healthcare leaders are driven to act proactively and to apply appropriate strategies to accurately assess privacy threats while handling the impact of privacy safeguard enactments on healthcare workflow and work practices.

This dissertation makes several contributions to the research literature in information systems, organizational behavior, and health informatics. First, this research provides new theoretical insights into understanding privacy management by targeting the organizational level of analysis through a grounded theory approach. Second, this study responds to a compelling call for research investigating the effectiveness and consequences of enacting privacy safeguards. Moreover, using a grounded theory, this study provides a rich lens to understand the consequences of privacy safeguards enactments and their implications on privacy compliance. Finally, this interdisciplinary study converges the research streams of information systems, organizational behavior, and Health informatics, and promotes synergy between academia and practice by offering practical implications for healthcare practitioners and insights for further theory development.
# TABLE OF CONTENTS

LIST OF FIGURES .................................................................................................................. ix
LIST OF TABLES .................................................................................................................... x
GLOSSARY ............................................................................................................................... xi
ACKNOWLEDGEMENTS .......................................................................................................... xii
DEDICATION .......................................................................................................................... xv

Chapter 1 Introduction .......................................................................................................... 1
  1.1 Problem Statement ......................................................................................................... 1
  1.2 Study Motivation ............................................................................................................ 3
  1.3 Research Objectives and Questions .............................................................................. 5
  1.4 Significance and Contributions of the Study ............................................................... 8
  1.5 Thesis Organization ..................................................................................................... 9

Chapter 2 Literature Review ................................................................................................. 11
  2.1 Interdisciplinary Literature .......................................................................................... 11
     2.1.1 Literature Review Domains .................................................................................. 12
     2.1.2 Literature Review Sources ................................................................................... 12
     2.1.3 Literature Review Search Strategy ....................................................................... 13
  2.2 Definition and Scope of Information Privacy and EHRs .............................................. 16
     2.2.1 Information Privacy ............................................................................................. 16
     2.2.2 Electronic Health Records (EHRs) ...................................................................... 18
  2.3 Information Privacy Issues & Threats .......................................................................... 20
     2.3.1 Data Collection ...................................................................................................... 22
     2.3.2 Unauthorized Access ............................................................................................ 22
     2.3.3 Secondary Use ...................................................................................................... 22
     2.3.4 Data Use and Disclosure ...................................................................................... 23
     2.3.5 Errors ..................................................................................................................... 23
  2.4 Protecting and Managing Information Privacy ............................................................ 24
     2.4.1 Technical Approach ............................................................................................. 26
     2.4.2 Human Approach ................................................................................................ 30
  2.5 Factors Influencing Privacy Responses ......................................................................... 32
     2.5.1 Institutional Pressures ......................................................................................... 33
     2.5.2 Resources and Competitive Advantage .............................................................. 34
     2.5.4 Ethical Responsibility ........................................................................................... 35
  2.6 Implications of Enacting Privacy Responses ................................................................. 36
     2.6.1 Unavailability of Information ............................................................................... 37
     2.6.2 Workflow Disruptions ........................................................................................... 38
     2.6.3 Usability Issues ..................................................................................................... 38
     2.6.4 Operational Feasibility Issues .............................................................................. 39
5.1 Shaping the Theoretical Framework .......................................................... 105
  5.1.1 The First Emerging Theme: The PIA .................................................... 106
  5.1.2 The Second Emerging Theme: Imbalance Challenge ........................... 109
  5.1.3 The Entwined Relationship between the Themes ................................ 112
5.2 Formulating the Theoretical Framework .................................................. 113
  5.2.1 Discussion of the PIA ........................................................................ 115
  5.2.2 Implications of the Enactment of Privacy Safeguards .......................... 117
  5.2.3 Effect of Positive and Negative Impacts on Imbalance Challenge .......... 119
  5.2.4 Effect of the Imbalance Challenge on Privacy Compliance .................. 120
  5.2.6 Iterative Relationship between the PIA and the Imbalance Challenge .... 123
5.3 Relating to the Literature ........................................................................ 126
  5.3.1 Relating to the Literature on Risk Management .................................... 127
  5.3.2 Relating to the Theory of Balance ...................................................... 129
  5.3.3 Relating to Privacy Calculus ............................................................... 130
  5.3.4 Relating to Organizational Behavior Literature .................................... 130
5.4 Evaluating the Study .................................................................................. 135

Chapter 6 Conclusion ..................................................................................... 142
  6.1 Summary of the Study ........................................................................... 142
  6.2 Revisiting the Research Questions ......................................................... 144
  6.3 Contributions and Implications for Research ......................................... 147
  6.4 Contributions and Implications for Practice .......................................... 150
  6.5 Limitations ............................................................................................. 152
  6.6 Future Research ..................................................................................... 153

References ....................................................................................................... 156

Appendix A  Semi–Structured Interview Protocol for Information Privacy Experts .......... 181
Appendix B  Illustrative Supporting Data for Privacy Threats ............................ 183
Appendix C  Illustrative Supporting Data for Drivers of Privacy Safeguards ............ 186
Appendix D  Illustrative Supporting Data for Privacy Safeguards ....................... 190
Appendix E  Illustrative Supporting Data for Imbalance Impacts ....................... 194
Appendix F  Illustrative Supporting Data for Organizational Context .................. 199
Appendix G  Illustrative Supporting Data for PIA ............................................ 201
Appendix H  List of State Breach Notification Laws ......................................... 203
Appendix I  Informed Consent ....................................................................... 206
Appendix J  Example Solicitation Email ......................................................... 208
Appendix K  Sample Documentation ................................................................ 209
LIST OF FIGURES

Figure 1-1 Dissertation Organization .................................................................................. 10
Figure 2-1 Classification of Information Privacy Research Issues ........................................ 16
Figure 2-2 Mapping of Privacy Threats to Technical Countermeasures ............................. 29
Figure 3-1 Data Analysis Procedures .................................................................................. 58
Figure 4-1 Emergent Dimensions: Threats, Drivers, and Safeguards ................................. 65
Figure 4-2 Emergent Concepts, Themes, and Dimensions in Organizational Privacy
Responses .......................................................................................................................... 66
Figure 4-3 Perceived Privacy Threats .................................................................................. 67
Figure 4-4 Imbalance Challenge ....................................................................................... 97
Figure 5-1 Enabling and Inhibiting Drivers ....................................................................... 109
Figure 5-2 The Emerging Theoretical Framework ............................................................... 114
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table 2-1</th>
<th>Interdisciplinary Literature Review</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2-2</td>
<td>Summary of Privacy Issues and Threats</td>
<td>21</td>
</tr>
<tr>
<td>Table 2-3</td>
<td>Summary of Privacy Countermeasures</td>
<td>26</td>
</tr>
<tr>
<td>Table 2-4</td>
<td>Mapping of Privacy Threats to Their Countermeasures</td>
<td>27</td>
</tr>
<tr>
<td>Table 2-5</td>
<td>Summary of Drivers Influencing Privacy Responses</td>
<td>33</td>
</tr>
<tr>
<td>Table 3-1</td>
<td>The Research Process</td>
<td>44</td>
</tr>
<tr>
<td>Table 3-2</td>
<td>Comparison of Data Analysis Steps between Glaser and Strauss</td>
<td>50</td>
</tr>
<tr>
<td>Table 3-3</td>
<td>Interview Data Sources</td>
<td>53</td>
</tr>
<tr>
<td>Table 3-4</td>
<td>Workshops and Round Tables Data Sources</td>
<td>54</td>
</tr>
<tr>
<td>Table 3-5</td>
<td>Trustworthiness Criteria</td>
<td>61</td>
</tr>
<tr>
<td>Table 3-6</td>
<td>Ensuring the Adequacy of the Empirical Grounding</td>
<td>62</td>
</tr>
<tr>
<td>Table 3-7</td>
<td>Ensuring the Adequacy of the Research Process</td>
<td>63</td>
</tr>
<tr>
<td>Table 4-1</td>
<td>Institutional Pressures as a Driver</td>
<td>73</td>
</tr>
<tr>
<td>Table 4-2</td>
<td>Resources as a Driver</td>
<td>75</td>
</tr>
<tr>
<td>Table 4-3</td>
<td>Ethical Integrity as a Driver</td>
<td>77</td>
</tr>
<tr>
<td>Table 4-4</td>
<td>Classification of Organizational Privacy Responses</td>
<td>80</td>
</tr>
<tr>
<td>Table 5-1</td>
<td>Strategies for Resistance and Accommodation to Institutional Pressures</td>
<td>134</td>
</tr>
<tr>
<td>Table 5-2</td>
<td>Empirical Grounding of the Study</td>
<td>137</td>
</tr>
<tr>
<td>Table 5-3</td>
<td>Research Process Evaluation Criteria</td>
<td>139</td>
</tr>
</tbody>
</table>
## GLOSSARY

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CMIO</td>
<td>Chief Medical Information Officer</td>
</tr>
<tr>
<td>CPO</td>
<td>Chief Privacy Officer</td>
</tr>
<tr>
<td>HIMSS</td>
<td>Healthcare Information and Management Systems Society</td>
</tr>
<tr>
<td>HIPAA</td>
<td>The Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HITECH</td>
<td>The Health Information Technology for Economic and Clinical Health</td>
</tr>
<tr>
<td>CIHDS</td>
<td>Center for Integrated Healthcare Delivery Systems</td>
</tr>
<tr>
<td>EHRs</td>
<td>Electronic Health Records</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic Medical Records</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
</tbody>
</table>
| CHIME   | The College of Healthcare Information Management Executives.  
http://www.cio-chime.org/ |
| PIA     | Privacy Impact Assessment |
| WHITE   | Workshop on Health Information and Economics |
ACKNOWLEDGEMENTS

Glory to God for the wisdom, the spiritual and professional growth he bestowed upon me. This has been an interesting, life-changing journey, and it is a blessing to finally write this section. I would like to thank and share my joy with various individuals who played vital roles in my Ph.D. journey and my development as a scholar.

First, I express my deepest gratitude to my major advisor Dr. Chao Chu, for providing me with the right mixture of toughness, encouragement, and wisdom throughout my four years at Penn State. My co-advisor Dr. Heng Xu, I appreciate the role model she was for me and the good counsel she provided throughout this process. I also want to thank the three other committee members: Dr. Sandeep Purao, for his encouragements and valuable comments on my research; Dr. Barbara Gray, for initiating my interest in qualitative research and pushing for deeper and richer analysis; and, last but not least, Dr. Allen Lee, for believing in my work and providing constructive, supportive feedback.

I would like to thank several friends and colleagues who inspired and supported me in this journey. A special thanks to my dear friend from Orlando, Dr. Las Adams, for providing tireless support and feedback through tough times. Thanks also to Dr. Andrea Tapia for being a professor, a friend, a babysitter, and a role model. I am grateful for my IST cohort, especially my great friends Anna Levy and Heidi Webb. I enjoyed our girls’ nights out, as well as our research debate sessions. Thank you, Dr. Kayla Hales, for being a friend, a reviewer, and a confidant. Thanks also to Talia Carroll, my writing buddy, whose ‘food dance’ has always been very uplifting. My gratitude goes to Louis-Marie
Ngamassi and his family for genuinely enlightening my life. Thank you Lee Erickson and Nick Giacobe, for not being afraid to give me tough and constructive criticism while still being my friends. I would also like to thank Dr. Stephanie Troutman and Shaeeda Mensah for their wonderful friendship and for our children’s play dates. Thank you to Dr. Suzanne Adair for her guidance and financial support through OGEEP, and to Dr. Lisa Lenze for supporting my teaching. I am also grateful to Dr. Jim Courtney and Dr. Paul Cheney from my previous life at UCF. Thank you for keeping up with me and still writing references for me. My thanks go to Betty Blair for simply being there for me and kicking me when needed. Thank you, also, to everyone in PIC and the graduate assistant office. I also thank all those who allow me directly or indirectly to succeed in pursuing my dream.

My Ph.D. journey would not have been the same without my involvement with the Ph.D. Project. The Ph.D. Project has been a second family since 2008 so I give my thanks to all of the ISDSA members. I would like to acknowledge the support of the Center for Integrated Healthcare Delivery Systems (CIHDS), especially Dr. Harriet B. Nembhard, who took time to have several coffee breaks to cultivate our friendship and provide scholarly support. CIHDS has been very supportive of my healthcare IT oriented research and of my data collection. I thank all the members who facilitated this work.

Finally, I would like to thank my family for their support. I am deeply grateful for my father Mohamed Fachtal and my mother Fatima Badgaoui, and particularly for their early retirement to support my Ph.D. journey by helping out with my three children, especially my two-year-old. To my brother Hamid and my sisters, Mouna and Asmaa, I
love you so much and thank you for tirelessly listening to me. Thank you to my beautiful children, Nora, Ameen, and Adam. You are my biggest supporters in following my dream and my distraction from going nuts. Last, but certainly not least, I thank my wonderful husband, Walter (Patrick) for the intellectual debates, the emotional support, and the tremendous help with the kids, in addition to being a great cook. I am now looking forward to a lifetime with you, post-dissertation.
DEDICATION

To my parents & my children
Chapter 1

Introduction

1.1 Problem Statement

The healthcare sector exerts a significant impact on an individual’s quality of life. It is also known as an information intensive industry where patients’ information is stored, processed, and transferred to several entities, such as doctors’ offices, hospitals and laboratories. The ability to accurately access patients’ medical data in a timely manner can facilitate diagnosis and reduce medical errors. The integration of Information Technology (IT) and healthcare allowed the development of computer applications that have laid the path to exponential growth in the electronic acquisition, storage, manipulation, and communication of health-related data – health informatics (Kluge, 2011).

Digitized healthcare, or health informatics, emerged within the last four decades (Hersh, 2004; Smith et al., 1999) with recent major governmental initiatives (Bush, 2004; Obama, 2009) supporting the implementation of electronic health records (EHRs) in the United States (Angst et al., 2009). Technologies such as EHRs have the potential to transform healthcare processes by increasing the availability of patients’ information and fostering communication and cooperation among clinicians, administration, and other health entities across systems and geographic locations.
In spite of potential benefits of healthcare IT, major issues and barriers have been associated with the use of EHRs, such as cost, technical issues, standardization, and privacy concerns (Hersh, 2004). While extensive research has focused on implementation costs and technical solutions (Aberdeen et al., 2010; Agarwal et al., 2007; Blobel et al., 2006; Boyd et al., 2007; Chen et al., 2010; Chiang et al., 2003; Claerhout et al., 2005; Haas et al., 2011; Kluge, 2007; Lovis et al., 2007; Mohan et al., 2004; Neubauer et al., 2011; Ohno-Machado et al., 2004; Quantin et al., 2000; Ravera et al., 2004; Reni et al., 2004; Sujansky et al., 2010), privacy concerns remain a thorny subject for both practitioners and researchers. Thus, this study will focus on the privacy issues with regard to healthcare IT.

Information privacy issues and threats have drawn considerable attention from researchers and practitioners. Media publicity around recent privacy breaches—such as stolen portable computers with patient information, unauthorized access, or disclosure—brings attention to potential individual harms and organizations’ responses and behaviors (Hodgkinson et al., 2010). At the individual level, harmful situations such as inappropriate disclosures of a mental disorder diagnosis or a sexually transmitted disease can severely impact employment or insurance coverage (Cushman et al., 2010). At the organizational level, privacy breaches may have direct consequences for the organization’s reputation, increased monetary fines, along with potential civil and criminal liabilities (Culnan & Williams, 2009). As a result, organizations now carefully focus on developing privacy programs and safeguards to mitigate privacy threats and protect sensitive information. However, the evidence indicates that these initiatives are
failing because “breaches continue to occur, suggesting that existing compliance programs are not effective” (Culnan & Williams, 2009, p.678).

1.2 Study Motivation

According to Smith et al. (2011), prior research into privacy issues and threats can be grouped by level of analysis (individual, group, organizational, and societal) and by industry sector (e.g., e-commerce, finance, government, and healthcare). Many previous studies on information privacy have been at the individual level of analysis (Angst et al., 2009; Chen et al., 2009; Son et al., 2008; Xu et al., 2008a) instead of the organizational level, because “most rigorous studies of organizational privacy policies and practices would likely include a set of exhaustive interviews with an organization’s members and stakeholders, and some amount of deep process tracing would also likely be involved” (Smith et al., 2011, p. 36-37). Despite the consensus in multidisciplinary research reviews, studies on privacy breaches and responses at the organizational level remains under-researched (Appari & Johnson, 2010; Culnan & Williams, 2009; Greenaway & Chan., 2005; Smith et al., 2011). Moreover, there are limited theoretical guidelines on how organizations develop their responses to information privacy threats (Greenaway & Chan, 2005) and which factors impact their choices.

Beyond the level of analysis, privacy studies also varied in their contexts; for example, studies have examined e-commerce (Cranor et al., 2007; Van Slyke et al., 2006) and online social networks (Bulgurcu et al., 2010b; Chen et al., 2009). Examining privacy threats in the healthcare context is difficult because of its complexity, changeability, strict
regulations, and policies (Garfinkel et al., 2002; Thatcher et al., 2000). The U.S. Congress’s realization that advances in e-health could erode privacy and confidentiality of health information led to the adoption of privacy standards for protecting individually identifiable health information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) lay out a broad set of specifications for privacy at the federal level and define the regulatory requirements for protected health information (PHI). Federal regulatory requirements can be overridden by state laws, which lead to variability in how privacy is implemented in each state (Appari et al., 2009). Such variability at the state level is considered a major impediment to healthcare organizational compliance with regulations (Hodge Jr. 1999; Langenderfer and Cook 2004).

Developing robust privacy programs is a difficult and costly process (Culnan & Williams, 2009), but it is even more challenging in the healthcare sector. Healthcare organizations are expected to have safeguards in place against privacy threats (Liginlal et al., 2009) and therefore, the healthcare industry has an emerging need for a business model (Appari & Johnson, 2010, p. 281). One possible explanation for this lack of research is organizations’ unwillingness to share information and statistics about their practices (Kotulic et al., 2004; Sinclaire 2003) and the complexity of organizational data collection (Smith et al., 2011).

In the presence of increasing healthcare penalties for non-compliance (Fernando et al., 2009; Mohan et al., 2004) and privacy operational challenges (Croll 2011), organizations are facing challenges in how to appropriately respond to privacy threats while not impeding healthcare workflows. To date, no comprehensive model has been
developed to empirically explore the different theoretical explanations while identifying the intended and unintended consequences of privacy safeguards implementation. This study provides a unique perspective on information privacy in the context of healthcare.

1.3 Research Objectives and Questions

This study aims to address the lack of theories and research that focus on responding to information privacy threats at the organizational level. This study also aims to promote synergy between academia and practice, especially because investigating privacy responses within healthcare organizations is a top priority for both practitioners and researchers. From a practical point of view, understanding the ways organizations respond to information privacy threats and how these responses impact work practices is very important. Also of relevance is securing the privacy of patients’ health information without impeding the flow of information or workflow processes.

The key research issue examined in this dissertation is: How do healthcare organizations respond to information privacy threats? This research issue is further subdivided into three main research questions that kept evolving¹ throughout the study (Strauss et al., 1998; Strauss et al., 2008). Healthcare organizations face significant challenges in designing and implementing the appropriate safeguards to mitigate information privacy threats. Moreover, mitigating privacy threats must take into consideration several drivers that influence actions and responses. Therefore, the first

¹ This is consistent with the qualitative research claims that research questions should mature and develop during the data analysis phase (Creswell 2009).
research question (RQ1) is pertinent to the reasons behind organizational responses, and it is further broken into two sub-questions (RQ1a and RQ1b).

**Research Question 1:** Why do healthcare organizations respond to information privacy threats?

  **RQ1a:** What are the different types of threats faced by healthcare organizations?

  **RQ1b:** What are the different types of drivers healthcare organizations have to consider?

  To understand organizational responses to privacy threats, it is important to distinguish between different types of responses while identifying mechanisms of applying the appropriate safeguards, which lead to the second research question (RQ2).

**Research Question 2:** What are the safeguards and mechanisms used by healthcare organizations to mitigate information privacy threats?

  **RQ2a:** What are the different types of safeguards implemented?

  **RQ2b:** What are the mechanisms undertaken to apply the appropriate safeguards?

  There is little research theoretically explaining the outcomes of enacting privacy safeguards and the subsequent effects on privacy compliance. As Belanger and Crossler (2011, p. 1022) pointed out, “there are many behavioral questions to be explored with respect to not only use of potential privacy protection tools but also effectiveness and consequences of use.” Similarly, this void in extant privacy literature has also been
identified by an interdisciplinary literature review (Smith et al., 2011) that highlights the need for more privacy research to consider actual outcomes. Following these calls for research on examining impacts and outcomes of privacy safeguards, we aim to investigate the conditions under which the negative impacts\(^2\) of privacy safeguard enactments outweigh the positive ones (i.e., the Imbalance Challenge occurs) and to identify the implications for privacy compliance. Specifically, we aim to address the following two research questions in this work

**Research Question 3:** How does the enactment of privacy safeguards impact healthcare workflow and processes?

- **RQ3a:** What are the intended consequences (positive impacts) of privacy safeguards?
- **RQ3b:** What are the unintended consequences (negative impacts) of privacy safeguards?
- **RQ3c:** What are the implications of these opposing impacts on privacy compliance (Imbalance Challenge) and what are the outcomes of the Imbalance Challenge?

Grounded theory-building methodology has been used to address the aforementioned research questions. As a result, a theoretical framework of organizational responses to information privacy threats is expressed by the means of propositions.

\(^2\) In this study, the term “impact” is used to describe the challenges organizational leaders identified from their operational processes and work practices after the enactment of privacy safeguards.
1.4 Significance and Contributions of the Study

This study contributes to existing privacy research in several ways. First, Smith et al. (2011) have shown a lack of organizational level privacy research in extant literature partially because these studies “are necessarily more complex and less conducive to ‘quick’ data collection techniques such as written and online surveys” (p. 1006). This research provides new theoretical insights into understanding privacy management by targeting to this under-researched level of analysis through a grounded theory approach that uncovers the construct of the Privacy Impact Assessment. Second, following the call by Belanger and Crossler (2011), we have studied the outcome of enacting privacy safeguards and the subsequent effects on privacy compliance specifically; the construct of the Imbalance Challenge emerged as an analytical construct to capture unintended consequences caused by the situation where the negative impacts of privacy safeguards outweigh the positive ones. Third, this study was designed to gain an in-depth understanding of organizational responses to privacy threats and the actual outcomes and implications of the privacy practices in healthcare organizations. Therefore, using a grounded theory methodology provided a rich lens to understand the mechanisms of privacy responses and the consequences of privacy safeguards enactments on privacy compliance. Fourth, this study contributes to the recent need for interdisciplinary research by converging the research streams of IS, organizational behavior, and health informatics.
The findings of this study have useful practical implications for healthcare organizations in general and hospitals in particular. These implications promote a synergy between academia and practice. The emergence of the Privacy Impact Assessment reinforces the importance of a proactive risk assessment approach of different drivers when responding to information privacy threats, while the emergence of the Imbalance Challenge provides a clearer understanding of the unintended consequences of privacy safeguard enactments and their implications on the organization’s overall privacy compliance. More detailed discussions on contributions of this research are presented in Chapter 6.

1.5 Thesis Organization

This dissertation consists of six chapters. Each chapter is briefly discussed below. Figure 1-1 provides a graphical representation of the structure of this dissertation.

Chapter 1 introduces the research problem, the research motivation, and the significance of the study. Chapter 2 presents a literature review on information privacy, institutional theory, resource-based view, and ethical considerations. In addition, it integrates all discussed approaches and identifies a research gap. Chapter 3 describes the research paradigm with the epistemology and ontology adopted. It describes the grounded theory methodology and the reason for its selection. This chapter also describes the data collection and analytical procedures and concludes with by outlining the applied evaluation criteria. Chapter 4 presents the findings, including different categories and themes. This chapter reports the results of the first two main steps of data analysis, first
order codes and second order themes, which result in an overarching structure. This chapter also provides a contextual background for analysis and discussion in the subsequent chapter. Chapter 5 discusses the emerging theoretical framework, relates it to the literature, and uses criteria from Chapter 3 to evaluate it. Finally, Chapter 6 summarizes the study by presenting an analysis of contributions and implications for both researchers and practitioners. It also discusses the limitations of this study and outlines further research possibilities in the domain of healthcare information privacy.

Figure 1-1 Dissertation Organization
Chapter 2

Literature Review

The notion of privacy issues and threats varies depending on several factors, such as industry sectors, regulatory laws, and cultures (Malhotra et al., 2004; Milberg et al., 1995; Xu et al., 2008a). In the United States, federal privacy laws have taken the form of sector-specific legislation (Culnan & Williams, 2009), such as the Gramm-Leach-Bliley Act of 1999 for financial services (http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act) and the Communications Act of 1996 for telecommunications (http://transition.fcc.gov/telecom.html). Thus, information privacy as a concept holds different definitions or expectations across industries. Consequently, privacy issues and threats will be better understood when they are bounded by a specific context (e.g., the healthcare industry) (Bansal et al., 2008; Johns 2006). Therefore, in this literature review section, research studies from both the information systems (IS) and the Health Informatics communities will be integrated in order to provide in-depth and context-specific insights about information privacy in the healthcare.

2.1 Interdisciplinary Literature

The literature review in this study is based on defining three criteria: domain, sources, and search strategy (Cooper, 1998). The domains of the study are identified first, followed by the sources of the literature review and the search strategy.
2.1.1 Literature Review Domains

Prior to identifying the sources of the literature review, the study defined the domains to be reviewed. Based on the background introduced in Chapter 1, three domains are included. First, literature on information privacy for IS was reviewed, as this research seeks to investigate information privacy threats with regard to technology use (e.g., electronic health records or EHRs). Second, literature on health informatics was reviewed, as it provides a contextual relevance to the study. Third, literature on organizational behavior and management was included, as this study focuses on organizational level responses.

2.1.2 Literature Review Sources

For the IS literature, this research focuses on the top five IS outlets identified by Lyytinen et al. (2007): Management Information Systems Quarterly (MISQ), Information Systems Research (ISR), the Journal of Management Information Systems (JMIS), the Journal of the Association for Information Systems (JAIS), and the European Journal of Information Systems (EJIS). In addition, the Information Systems Journal (ISJ) and the International Conference on Information Systems (ICIS) were also included in the literature review.

For the management literature, articles from the Academy of Management, Organization Science, and the Academy of Management Review were included in the literature review.
For health informatics literature, the study uses journal rankings based on Le Rouge et al. (2010), which identifies a list of leading journals on health informatics. The four top journals included in the literature review are: the *Journal of the American Medical Informatics Association* (JAMIA), *IEEE Transactions on Information Technology in Biomedicine*, the *International Journal of Medical Informatics*, and the *Journal of Biomedical Informatics*.

### 2.1.3 Literature Review Search Strategy

For the search strategy, the keywords “privacy” and “information privacy” were used. The interdisciplinary literature search returned over 450 article titles (Table 2-1). The management literature search returned no articles, with the exception of four articles published by *Organization Sciences*.

In the preliminary screening of abstracts, a number of articles were removed because they did not pertain to information privacy, were merely tables of contents, or were editorial comments. Over 200 articles were read, and further articles were removed primarily because of the level of analysis. Because this study focuses on the organizational level, articles pertaining to the individual, group, or societal level of analysis were excluded. The articles were coded by level of analysis, methodology, privacy threats, privacy safeguards, drivers, and theoretical contributions. Articles were

---

3 Articles pertaining to methods to protect privacy were classified as organizational, as were articles that covered both individual and organizational levels of analysis.
then classified based on the definition of privacy, privacy threats, countermeasures, and factors driving organizational responses.

Table 2-1 Interdisciplinary Literature Review

<table>
<thead>
<tr>
<th>Publication</th>
<th>No. of Articles Returned</th>
<th>Article Removed</th>
<th>Articles Read</th>
<th>Pertinent Articles at the Organizational Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IS Literature</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Information Systems Quarterly</td>
<td>79</td>
<td>57</td>
<td>22</td>
<td>7</td>
</tr>
<tr>
<td>Information Systems Research</td>
<td>18</td>
<td>7</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>Journal of the Association for Information Systems</td>
<td>16</td>
<td>1</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Journal of Management Information Systems</td>
<td>12</td>
<td>2</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>International Conference on Information Systems</td>
<td>18</td>
<td>1</td>
<td>17</td>
<td>3</td>
</tr>
<tr>
<td>European Journal of Information Systems</td>
<td>13</td>
<td>5</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Information Systems Journal</td>
<td>53</td>
<td>41</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>209</td>
<td>114</td>
<td>95</td>
<td>21</td>
</tr>
<tr>
<td><strong>Health/Medical Informatics Literature</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Journal of the American Medical Informatics Association</td>
<td>78</td>
<td>38</td>
<td>39</td>
<td>18</td>
</tr>
<tr>
<td>IEEE Transactions on Information Technology in Biomedicine</td>
<td>102</td>
<td>87</td>
<td>21</td>
<td>15</td>
</tr>
<tr>
<td>International Journal of Medical Informatics</td>
<td>67</td>
<td>30</td>
<td>37</td>
<td>26</td>
</tr>
<tr>
<td>Journal of Biomedical Informatics</td>
<td>9</td>
<td>0</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>256</td>
<td>155</td>
<td>106</td>
<td>63</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>465</strong></td>
<td><strong>269</strong></td>
<td><strong>201</strong></td>
<td><strong>84</strong></td>
</tr>
</tbody>
</table>
During the review, articles were classified into four broad categories: (a) the scope and definition of privacy and EHRs, (b) the privacy threats and vulnerabilities, (c) the measures used to address and manage privacy, and (d) the influencing factors referred to as drivers (see Figure 2-1). This classification, based on “What,” “Why,” and “How” logic, was used to glean a more comprehensive understanding of existing research in order to provide a clear picture for further research in healthcare information privacy. The “What” logic allowed for a definition of information privacy from different communities, as well as that of organizational privacy issues. The question of how organizations address such threats was handled through the “How” logic by means of providing a taxonomy of privacy measures. Finally, the question of why organizations respond was based on the drivers that influenced their responses.

This classification was also supported by the ongoing analysis of the interviews with key informants in healthcare organizations. The interviews were conducted as part of the qualitative study (see Chapter 3). Quotes from these healthcare experts were used throughout the chapter to support the literature classification and to assist in identifying and analyzing relevant issues and gaps in the literatures.
2.2 Definition and Scope of Information Privacy and EHRs

2.2.1 Information Privacy

Defining privacy has been notoriously difficult (Tsai et al., 2010) because of its multidimensionality (Culnan & Williams, 2009) and its broadness (Smith, 1993). In certain countries, the concept of privacy was not even previously defined (Ishikawa,
2000). In the United States, the meaning of privacy has evolved considerably since the eighteenth century (Etzioni, 1999). Initially, privacy was interpreted in terms of physical privacy (Warren et al., 1890), as implied by the Fourth Amendment to the U.S. Constitution. In the late twentieth century, privacy became associated with protecting personal information (i.e., information privacy). The scope of this research pertains specifically to information privacy, which has been defined as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin 1967, p. 7). This ability to control how personal information is acquired and used has been embraced by several scholars (Culnan & Williams, 2009; Peleg et al., 2008; Smith et al., 1996).

In healthcare, the notion of protecting patients’ privacy in the physician-patient relationship goes back to the Hippocratic Oath, which states, “I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know” (Lasagna 1964). In health informatics, the patient information privacy definition is based on a code of conduct that values confidentiality, integrity, availability, and accountability (France 1998; Ishikawa 2000). When asked to define information privacy, one healthcare expert stated: “I think at the core (privacy is) a philosophical issue, and it has been very much tied to personal autonomy. It’s not necessarily just about confidentiality, but it is somewhat about choosing what information you share about yourself with others and who can access that information and how information about you is collected.”

At the core, the definition of information privacy among IS and health informatics communities seems similar. However, with the advent of electronic medical records and
the Internet, protecting patients’ medical data became a context-specific topic that involves addressing the influences and relationships between information privacy and the particularities of the healthcare environment. Examining information privacy issues in the healthcare environment is difficult because that environment is complex, changeable, and strictly regulated (Garfinkel et al., 2002; Thatcher et al., 2000). Federal regulations are usually overridden by state healthcare regulations (Appari et al., 2009). Since 2007, nearly sixty health IT-related laws have been enacted in 34 states (Appari & Johnson, 2010) with their primary focus being defining the scope and boundaries of all different stakeholders which ultimately have to be integrated. Thus, future research should address healthcare information privacy with an integrative focus rather than an isolated one.

At the organizational level, information privacy refers to the right to determine when, how, and to what extent information is communicated to others (Claerhout et al., 2005). For Greenaway and Chan (2005), organizational information privacy refers to how firms treat their customers’ personally identifiable information. This study adopts Greenaway’s definition, thereby focusing on how healthcare organizations treat their patients’ protected health information.

2.2.2 Electronic Health Records (EHRs)

Although the terms of electronic medical record (EMR) and EHRs have been used interchangeably, they describe two different concepts (Garets et al., 2006). This study will provide definitions of EMR and EHRs from the IS and health informatics communities.
In the IS and health informatics literature, EMR refers to electronic patient records that are created and maintained by one care delivery organization (CDO) and include a patient’s medical history, clinical documentation, medications, and laboratory and radiology test results (Tong et al., 2009). This definition is supported by the Institute of Medicine report (IOM 1991), which defines EMR as

“An electronic patient record that resides in a system specifically designed to support users through availability of complete and accurate data, reminders and alerts, clinical Decision Support Systems (DSS), links to bodies of medical knowledge and other aids.”

EHRs, on the other hand, capture patients’ information in a digital format and make the information available to other healthcare stakeholders (Angst et al., 2009). According to the ISO/TS 18308 standard,

“The primary purpose of the EHR is to provide a documented record of care which supports present and future care by the same or other clinicians. This documentation provides a means of communication among clinicians contributing to the patient’s care.”

EHRs represent the primary mechanism through which interoperability of health information can take place (Agarwal et al., 2007). This definition aligns with that from the health informatics community; as Garets et al. (2006) stated, “EHRs represents the ability to easily share medical information among stakeholders and to have a patient’s information follow him or her through the various modalities of care engaged by that individual.” Therefore, this literature review will focus on EHRs.
2.3 Information Privacy Issues & Threats

In IS literature, problems and challenges surrounding information privacy have centered on four dimensions of individuals’ concerns over organizational information privacy practices: (1) collection of personal information, (2) unauthorized secondary access, (3) errors, and (4) improper access (Smith et al., 1996; Stewart et al., 2002). Malhotra (2004) stated that the online marketing environment brings up privacy threats that are different from those addressed above by Smith (1996). In addition to concerns over data collection, privacy issues in e-commerce include control over the use of personal information (data disclosure) and awareness of privacy practice (Malhotra et al., 2004). Solove (2006) developed a privacy taxonomy that has been adopted by several researchers (Culnan & Williams, 2009; Gürses et al., 2008; Xu et al., 2008a). This taxonomy included information collection, information processing, information dissemination, and invasion. In health informatics, context issues that arise include data ownership (Van der Linden et al., 2009), the complexity of the evolving healthcare legislation (Croll 2011), and EHRs design (Kluge 2007). Table 2-2 contains a summary of relevant privacy issues and threats from the IS and health informatics literature. The analysis of the literature highlights several key privacy issues and threats: data collection, data use and disclosure, unauthorized access, secondary use, and errors. In the following sections, those key issues and threats will be examined in greater detail.
<table>
<thead>
<tr>
<th>Privacy Issues and Threats</th>
<th>Information Systems References</th>
<th>Health Informatics References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection</td>
<td>(Culnan &amp; Williams, 2009; Malhotra et al., 2004; Otjacques et al., 2007; Smith 1993; Smith et al., 1996; Solove 2006; Stewart et al., 2002)</td>
<td>(Croll 2011)</td>
</tr>
<tr>
<td>Data Use and Disclosure</td>
<td>(Dinev et al., 2006; Li et al., 2010a; Malhotra et al., 2004; Menon et al., 2005; Otjacques et al., 2007; Solove 2006)</td>
<td>(Agrawal et al., 2007; Boyd et al., 2007; Chen et al., 2010; Ishikawa 2000; Mohan et al., 2004; Ohno-Machado et al., 2004; Patel et al., 2000; Quantin et al., 2000)</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>(Culnan &amp; Williams, 2009; Smith et al., 1996; Solove 2006; Stewart et al., 2002)</td>
<td>(Chen et al., 2010; Croll 2011; Kluge 2007; Mohan et al., 2004; Neubauer et al., 2011; Patel et al., 2000; Reni et al., 2004; Sujansky et al., 2010; Van der Linden et al., 2009)</td>
</tr>
<tr>
<td>Secondary Use</td>
<td>(Culnan &amp; Williams, 2009; Culnan 1993; Smith et al., 1996; Solove 2006; Stewart et al., 2002)</td>
<td>(Aberdeen et al., 2010; Chiang et al., 2003; Croll, 2011; Ishikawa 2000; Neubauer et al., 2011; Quantin et al., 2000)</td>
</tr>
<tr>
<td>Errors</td>
<td>(Smith et al., 1996; Stewart et al., 2002)</td>
<td>(Croll 2011; Mohan et al., 2004; Reni et al., 2004)</td>
</tr>
<tr>
<td>Ownership of the Data</td>
<td></td>
<td>(Sadan 2001; Van der Linden et al., 2009)</td>
</tr>
<tr>
<td>Balance Challenges</td>
<td></td>
<td>(Croll 2011; Mohan et al., 2004)</td>
</tr>
<tr>
<td>Awareness of Privacy Practices</td>
<td>(Malhotra et al., 2004)</td>
<td>(Croll, 2011)</td>
</tr>
<tr>
<td>EHRs Design and Lack of Standards</td>
<td></td>
<td>(Kluge, 2007)</td>
</tr>
</tbody>
</table>
2.3.1 Data Collection

Organizations should only collect for a purpose identified as essential (Croll 2011; Culnan & Williams, 2009). However, individual perceptions of the fairness of data collected by organizations vary (Malhotra et al., 2004) and pose a number of concerns associated with data collection (Smith et al., 1996).

2.3.2 Unauthorized Access

Health and medical data are privileged information and should be accessed only when needed (Croll, 2011; Fernando et al., 2009; Mohan et al., 2004). This is known as the “need to know” principle (Blobel et al., 2006; Ishikawa, 2000; Van der Linden et al., 2009). Among the most recognized and acted-upon privacy issues and threats is unauthorized access, also referred to as improper access (Smith et al., 1996). This type of threat includes abuse by authorized personnel when browsing records for curiosity purposes (e.g., to access family members’ information) or ulterior motives (e.g., to access celebrities’ medical information) (Culnan & Williams, 2009). It also includes hacking by external entities, which results in harms such as data breaches.

2.3.3 Secondary Use

Information secondary use involves new uses for the information collected by organizations (Culnan & Williams, 2009). Smith (1996) differentiated between internal secondary use and external secondary use: in other words, when information collected for
one purpose is used for another within the same organization vs. being disclosed to an external organization (Croll 2011; Ishikawa 2000). Once the information is disclosed to an external institution, there is little control over its use. For instance, in one case from Lazarus’s study, an outsourced transcriber threatened the disclosure of medical records that she had been processing (Lazarus 2003). In a study by Geller et al. (1996), insurance companies used the results from genetic tests to discriminate against applicants. Secondary uses of the PHI include medical, research, social services, public health, regulation, litigation, and commercial purposes (Anderson 2000).

2.3.4 Data Use and Disclosure

In the healthcare industry, it is often necessary to disclose medical data to patients or among clinicians to support patients’ treatment (Ishikawa 2000). Data also can be disclosed to outside entities (Ohno-Machado et al., 2004) for other purposes, such as billing and research. Patients’ data disclosure could lead to patients’ harassment, discrimination, economic harm, or denial of service from insurance or employers (Neubauer et al., 2011; Ohno-Machado et al., 2004; Sadan 2001).

2.3.5 Errors

Organizations face the issues of deliberate or accidental error in handling their consumers’ information (Smith 1993). While deliberate errors are easy to trap and handle via technical measures, accidental errors are hard to detect and correct, leaving consumer
information either subject to incorrect interpretation or even mistaken identity (Smith 1993).

As the summary reveals, MIS literature focused more on data collection issues, while medical informatics literature is more concerned with issues related to data use and disclosure, unauthorized access, secondary use, and errors. Recent medical informatics studies focus on some specific threats to healthcare, such as issues of data ownership (Van der Linden et al., 2009); EHRs’ design and lack of standards (Kluge 2007); and the balance between privacy policies’, clinical users’, and patients’ expectations (Croll 2011).

2.4 Protecting and Managing Information Privacy

Since organizations face such a wide variety of privacy issues and threats, along with the associated breaches, one might expect there to be an abundance of empirical research studies addressing these problems. This literature review revealed that this is not the case (Smith et al., 2011); moreover, the theories proposed to address identified problems remain underdeveloped (Greenaway & Chan, 2005).

While several researchers provided a categorization of privacy problems and issues (Smith et al., 1996; Solove 2006), very few attempted to categorize the countermeasures to address these threats (Culnan & Williams, 2009; Greenaway & Chan, 2005). The current study endeavors not only to provide a taxonomy of privacy measures, but also to map the technical measures onto the appropriate threats.
Organizations are expected to have safeguards in place against various threats to privacy (Culnan & Williams, 2009; Liginlal et al., 2009). In healthcare, organizations must design and implement privacy programs to protect patients’ right to privacy (Agrawal et al., 2007; Ohno-Machado et al., 2004). The literature review revealed a variety of ways in which organizations attempt to address and manage existing privacy problems and threats (See Table 2-3).

The literature analysis distinguishes between different protection mechanisms. These mechanisms or safeguards fall into a technical (Aberdeen et al., 2010; Chiang et al., 2003; Kluge 2007; Ohno-Machado et al., 2004; Quantin et al., 2000; Tsai et al., 2010) and a human equation (D'Arcy et al., 2009; Fernando et al., 2009; Herath et al., 2009; Ishikawa 2000; Straub et al., 1990; Yeh et al., 2007).
Table 2-3 Summary of Privacy Countermeasures

<table>
<thead>
<tr>
<th>Privacy Measures</th>
<th>Information Systems References</th>
<th>Medical Informatics References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>(Garfinkel et al., 2007; Li et al., 2010a; Mai et al., 2010; Menon et al., 2005; Tsai et al., 2010)</td>
<td>(Aberdeen et al., 2010; Agarwal et al., 2007; Blobel et al., 2006; Boyd et al., 2007; Chen et al., 2010; Chiang et al., 2003; Claerhout et al., 2005; Haas et al., 2011; Kluge 2007; Lovis et al., 2007; Mohan et al., 2004; Neubauer et al., 2011; Ohno-Machado et al., 2004; Quantin et al., 2000; Ravera et al., 2004; Reni et al., 2004; Sujansky et al., 2010)</td>
</tr>
<tr>
<td>Policy</td>
<td>(Greenaway &amp; Chan, 2005; Smith 1993; Tsai et al., 2010)</td>
<td>(Anderson 2000; Croll 2011; Ishikawa 2000; Jinye et al., 2010; Mohan et al., 2004; Ravera et al., 2004; Smith 2000)</td>
</tr>
<tr>
<td>Training and Education</td>
<td>(D'Arcy et al., 2009; Yeh et al., 2007)</td>
<td>(Fernando et al., 2009; Ishikawa 2000; Mohan et al., 2004; Patel et al., 2000; Smith 2000)</td>
</tr>
<tr>
<td>Culture of Privacy</td>
<td>(Culnan &amp; Williams, 2009)</td>
<td>(Ishikawa 2000; Mohan et al., 2004)</td>
</tr>
<tr>
<td>Privacy Impact Assessment</td>
<td>(Culnan &amp; Williams, 2009)</td>
<td>(Croll 2011)</td>
</tr>
<tr>
<td>Disciplinary Actions</td>
<td>(Herath et al., 2009; Straub et al., 1990)</td>
<td>(Fernando et al., 2009; Mohan et al., 2004)</td>
</tr>
<tr>
<td>Physical Measures</td>
<td></td>
<td>(Mohan et al., 2004)</td>
</tr>
</tbody>
</table>

2.4.1 Technical Approach

As a reaction to data breaches, unauthorized data access, or other threats, healthcare organizations develop technical measures (Chen et al., 2010; Ohno-Machado et al., 2004) or draft policies (Mohan et al., 2004; Smith 1993). This response is usually driven by compliance to external pressures such as HIPAA and HITECH. For example,
HITECH requires covered entities to implement the privacy and security rules to protect PHI and to notify patients in case of a security breach. Healthcare organizations are pressured to comply with these rules in order to avoid civil and criminal penalties.

Various technologies have been used to address health information privacy threats (see Table 2-4). The proposed mapping is based on the literature (see Figure 1-1).

Table 2-4 Mapping of Privacy Threats to Their Countermeasures

<table>
<thead>
<tr>
<th>Privacy Threat</th>
<th>Matching Technical Countermeasure</th>
<th>IS and Medical Informatics References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Collection</strong></td>
<td>Anonymization</td>
<td>(Claerhout et al., 2005)</td>
</tr>
<tr>
<td><strong>Use &amp; Disclosure</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anonymization</td>
<td>(Boyd et al., 2007; Chiang et al., 2003; Li et al., 2010b; Mohan et al., 2004; Neubauer et al., 2011; Ohno-Machado et al., 2004; Quantin et al., 2000)</td>
</tr>
<tr>
<td></td>
<td>Cryptography</td>
<td>(Canim et al., 2012; Kantarcioglu et al., 2008; Lee et al., 2011; Lee et al., 2008; Quantin et al., 2000)</td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td>(Chen et al., 2010; Haas et al., 2011)</td>
</tr>
<tr>
<td><strong>Unauthorized Access</strong></td>
<td>Access Control Mechanism</td>
<td>(Blobel et al., 2006; Chen et al., 2010; Lovis et al., 2007; Mohan et al., 2004; Peleg et al., 2008; Reni et al., 2004; Sujansky et al., 2010; Vander Linden et al., 2009)</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>(Blanquer et al., 2009; Choe et al., 2008; Gritzalis et al., 2005; Kluge 2007)</td>
</tr>
<tr>
<td></td>
<td>Anonymization</td>
<td>(Boyd et al., 2007; Neubauer et al., 2011)</td>
</tr>
<tr>
<td><strong>Secondary Use</strong></td>
<td>Anonymization</td>
<td>(Aberdeen et al., 2010; Neubauer et al., 2011)</td>
</tr>
</tbody>
</table>
A conventional approach to addressing access issues as well as data use and disclosure is the use of access control mechanisms. This approach focuses on designing access roles and policies to handle the right accesses to clinical information (Blobel et al., 2006; Peleg et al., 2008; Reni et al., 2004; Van der Linden et al., 2009). Managing access to patient information is challenging, as the organization needs to balance controlling information and controlling operational activities for healthcare providers (Lovis et al., 2007).

The extent and breadth of these technologies vary depending on the issue and the context. Several technologies have been utilized to protect patients’ privacy from using anonymization and pseudonymization through the removal of the identifier from medical data (Aberdeen et al., 2010; Chiang et al., 2003; Neubauer et al., 2011; Ohno-Machado et al., 2004), to encryption and cryptographic methods (Kluge 2007; Quantin et al., 2000).
Concerning the effect of policies in managing privacy, Smith (1993) conducted an organizational-level study about the development of policies and practices with respect to personal information. Findings from seven organizations confirmed a cycle of “drift-threat-reaction,” meaning that organizations’ privacy measures tend to drift until they are faced with an external threat, at which point, the organization reacts with formalized policies and interventions. Smith’s (1993) study concluded that protective approaches accounted for market pressures and legal regulations. Almost two decades later, Smith conducted an interdisciplinary literature review of information privacy research which still recommended further research and “deep process tracing” at the organizational level (Smith et al., 2011, p. 37).
2.4.2 Human Approach

Information privacy issues and threats cannot be addressed solely by using more advanced technologies (Chen et al., 2010; Chiang et al., 2003) or developing policies (Mohan et al., 2004). Existing privacy programs do not seem adequate enough; as Culnan and Williams (2009, p. 678) argued, “breaches continue to occur, suggesting that existing compliance programs are not effective.” With medical data disclosures being the second highest reported breaches (Hasan et al., 2006), privacy issues in the healthcare sector are moving to the forefront. These concerns over information security and privacy in healthcare have prompted the federal government to support initiatives, including allocating $17.3 million over three years to develop state-level solutions to the privacy and security challenges (Miller et al., 2009) in order to transcend the dominant reactive approaches to privacy (Culnan & Williams, 2009). Though a perfect privacy program does not exist, organizations can initiate proactive attitudes by creating cultures of privacy that involve buy-ins from the leaders (Culnan & Williams, 2009; Ishikawa, 2000) and ongoing commitments by all stakeholders to safeguard patient health information (Mohan et al., 2004) using a human-technology equation (Patel et al., 2000).

Education and training are emerging as important tools, because they provide awareness of potential risks and the organizations’ practices (Ishikawa 2000; Mohan et al., 2004). However, training sessions tend to be informational and are not integrated into the users’ daily activities (Patel et al., 2000), which lead to disciplinary actions (Mohan et al., 2004). Thus, this gap needs to be bridged for appropriate and effective training.
Another proactive measure, which has been mentioned in a limited number of papers, is the Privacy Impact Assessment (PIA). The PIA is a “risk assessment tool used to ensure that any new systems or new uses of personal information comply with legal requirements . . . to mitigate privacy risks before the new application is developed” (Culnan & Williams, 2009, p. 684). Identifying a priori these key PIA leads to addressing potential privacy issues and threats (Croll, 2011) and complying with fair information practices (Culnan & Williams, 2009).

Not only are robust privacy programs difficult and costly (Culnan & Williams, 2009), but they are also more challenging in the healthcare setting. Healthcare organizations are expected to have safeguards in place against these threats (Liginlal et al., 2009) and thus have a need for a business model specific for the healthcare industry (Appari & Johnson, 2010, p. 281). Despite the apparent consensus among scholars that information privacy responses at the organizational level are under-researched (Appari & Johnson, 2010; Culnan & Williams, 2009; Greenaway & Chan, 2005; Smith et al., 2011), there is a limited number of theoretical guidelines on how organizations should develop their responses to information privacy threats (Greenaway & Chan, 2005) and which factors impact their choices. One possible explanation for this lack of research is the unwillingness of organizations to share information and statistics about their practices (Kotulic et al., 2004; Sinclaire 2003).
2.5 Factors Influencing Privacy Responses

Which factors explain consumer privacy valuation? Several research papers have investigated individual behaviors through the concept of trust (Culnan et al., 1999; Malhotra et al., 2004) and the ways in which organizations handle their information according to fair information practices (Culnan & Williams, 2009). By exhibiting privacy seals and other privacy-enhancing technologies, organizations can mitigate privacy fears and gain their consumers’ trust (Malhotra et al., 2004; Xu et al., 2008b). Ultimately, the way organizations handle consumer information can mitigate the fears and concerns of their consumers. Therefore, it is extremely important to explore the factors that influence organizational responses to privacy issues and threats.

Despite expressed interest in information privacy, existing literature provides limited insights into the factors that may explain organizational responses and behaviors (Greenaway & Chan, 2005). Only a small number of studies provide some theoretical explanation of the measures undertaken by organizations (see Table 2-5).

Three major themes are prevalent when considering the influential factors: (1) legitimacy (Agrawal et al., 2007; Greenaway & Chan, 2005; Neubauer et al., 2011), (2) resources and competitive advantage (Greenaway & Chan, 2005; Smith 2000), and (3) moral and ethical considerations (Culnan & Williams, 2009; Kluge 2007; Mohan et al., 2004). A very limited number of researchers (Greenaway & Chan, 2005) combine more than one theme to provide a richer understanding of organizational responses.
Table 2-5 Summary of Drivers Influencing Privacy Responses

<table>
<thead>
<tr>
<th>Factors</th>
<th>Information Systems Literature</th>
<th>Medical Informatics Literature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legitimacy (Institutional Forces)</strong></td>
<td>(Greenaway &amp; Chan, 2005)</td>
<td>(Agarwal et al., 2007; Kluge 2007; Neubauer et al., 2011; Smith 2000)</td>
</tr>
<tr>
<td>- Social approach to privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Conformism to legal requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Conforming to the norms of external groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resources and Competitive Advantage</strong></td>
<td>(Greenaway &amp; Chan, 2005; Smith, 1993)</td>
<td>(Smith 2000) (Fernando et al., 2009; Moehr et al., 1998; Smith 2000)</td>
</tr>
<tr>
<td>- Economic approach to privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Competitive advantage based on strategic differentiation of information privacy approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Resources contribute to achieving sustainable competitive advantage</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Moral and Ethical Considerations</strong></td>
<td>(Culnan &amp; Williams, 2009; Greenaway &amp; Chan, 2005; Smith, 1993; Stewart et al., 2002)</td>
<td>(Claerhout et al., 2005; Ishikawa et al., 2007; Kluge 2007; Mohan et al., 2004)</td>
</tr>
<tr>
<td>- Conformism to FIP principles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Achievement of moral legitimacy through a culture of integrity that combines legal compliance and managerial ethical behavior</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.5.1 Institutional Pressures

Research on Institutional Theory has generated extensive insights into how organizations respond to external pressures (Oliver 1991). Organizations’ actions and decisions often are affected by their business relationships with external parties such as regulatory institutions, market dynamics, and industry associations (DiMaggio and Powell 1983). Institutional Theory posits that organizations respond to institutional
pressures and adopt behavioral and structural changes in order to achieve legitimacy and conformity (DiMaggio et al., 1983; Meyer et al., 1977). Institutional pressures can be imposed by the state, interest groups, and the general public (Oliver 1991). Healthcare legislation, such as the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, defines the federal regulatory requirements for handling patients’ PHI.

Healthcare organizations must adhere to these regulations (Appari & Johnson, 2010; Neubauer et al., 2011). Institutional theory has received significant attention from IS and organizational researchers (Goodstein 1994; Orlikowski et al., 2001; Teo et al., 2003) (Mignerat et al., 2009; Orlikowski et al., 2001). Thus, the theory seems to offer an appropriate lens to examine the regulatory effects on organizational information privacy responses. With compliance being the major goal for organizations to protect patient health information, organizations develop policies and processes that are in alignment with healthcare regulations. While complying with healthcare regulation is inescapable in order to avoid penalties, organizations with a built-in culture that values patients’ privacy started to embrace a proactive approach (Culnan & Williams, 2009).

2.5.2 Resources and Competitive Advantage

In a conceptual paper, Greenaway and Chan (2005) expressed their concern about the lack of theories that can support scholarly investigation of information privacy at the organizational level. The authors also argued that the Institutional Theory, with its social approach, is not sufficient to explain organizational behaviors. Integrating it with an
economic approach, the Resource Based View (RBV) Theory provided much richer insights into organizational information privacy. RBV posits that organizations possess resources that can be a source of sustained competitive advantage (Barney 1986; Rumelt 1984; Wernerfelt 1984). RBV has been explored as a theoretical explanation for organizations seeking competitive advantage through their privacy programs (Greenaway & Chan, 2005). Organizations investing in privacy programs can gain competitive advantage (Bowie et al., 2006; Smith 1993). In healthcare, by using the right combination of human and financial resources, organizations can differentiate themselves by being trustworthy in their handling of patients’ information.

2.5.4 Ethical Responsibility

Organizations recognize that focusing strictly on institutional compliance is not appropriate. Integrating moral responsibility and ethical considerations in their practices is becoming increasingly important though with limited coverage (Culnan & Williams, 2009; Mohan et al., 2004). Ethical considerations are associated with organizational behaviors beyond avoiding illegal practices (Silverman 2000). Organizations that recognize moral and ethical responsibilities will gain more commitment from their employees and customers. Using two privacy breach case studies, Culnan and Williams (2009) offered a set of best practices to help organizations transcend their reactive approaches to be more proactive. These best practices include fostering a culture of privacy, implementing governance processes, and avoiding decoupling. These ethics translate into having best business practices that account for Fair Information Practices.
(FIPs). FIPs are a set of global standards originally developed by the US Department of Health, Education, and Welfare (HEW 1973). In the context of information privacy, FIPs provide guidance to organizations about responsible privacy behaviors (Smith 1993). In the United States, there is no omnibus law for organizations to adhere to FIPs; rather, each domain adopts a sectorial approach (Culnan and Williams, 2009). In the context of healthcare information privacy, FIPs include notice to patients of the use and disclosure of their PHI and their access to that information, as well as security from unauthorized access and enforcement mechanisms to handle violations (Parks et al, 2010). Applying FIPs provides organizations with a basic understanding of and responsibility for handling data collection and use (Greenaway & Chan, 2005).

Despite these ethical considerations (Culnan and Williams, 2009), the operationalization of organizational ethics is unclear. This led to a call for sophisticated ethical analyses that could serve as guidance in particular situations (Moor 2005).

2.6 Implications of Enacting Privacy Responses

In healthcare, the need to implement the appropriate privacy safeguards is as unquestionable as the need to protect patient privacy, confidentiality, and the integrity of electronic health records. However, defining how privacy safeguards can be effective, and what their implications are, is a far more complex task.

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

2.6.1 Unavailability of Information

Healthcare professionals, such as doctors and nurses, are increasingly dependent on the availability and accuracy of patient information to provide adequate treatment and make other healthcare-related decisions. This information is often needed on a continuous, 24/7 basis. Traditionally, non-availability of information is linked with computer failures, programs’ or human errors, and environmental conditions (Bakker 1998). However, existing privacy research in the field of health informatics highlighted the dilemma of ensuring availability and access to patient information for authorized healthcare providers without breaching the confidentiality and privacy of medical information (Salomon et al., 2010; Smith and Eloff 1999). If the information needed by healthcare professionals to reach critical clinical decisions was unavailable due to tight access controls, patients may be incorrectly treated. Therefore, unavailability of information may have dire consequences for the quality of patient care.
2.6.2 Workflow Disruptions

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

2.6.3 Usability Issues

Usability has been defined as the degree of efficiency and effectiveness of use (Bennett 1984; Shackel 1984). The concept of usability has been applied within a range of users, tasks, tools, and environments. With the design and implementation of privacy protective technologies, usability has become an extremely important, albeit still poorly understood element of both privacy and security. The end results are user dissatisfaction and unusable systems (Johnson et al., 2005). In the healthcare industry, understanding the
interplay between usability and privacy is essential. Privacy safeguards technologies such as biometrics have been introduced to control access to medical facilities and protect the privacy and confidentiality of patient information (Marohn 2006). However, using biometrics also poses several usability issues due to the impact of temperature, humidity, and dirt (Flores Zuniga et al., 2010). The usability issues of biometrics can also stem from the user’s age, skin color, or certain health conditions where the use of hygienic gloves is required (Flores Zuniga et al., 2010). This study pertains to the impacts of privacy safeguard enactments on workflow and work practices; therefore, we will focus on usability issues perceived by healthcare workers.

2.6.4 Operational Feasibility Issues

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

2.7 Identifying the Gaps

The need for generating a new theory arises when significant gaps in the literature on organizational privacy responses and their outcomes are considered together. Existing organizational research has used a limited repertoire of theories to explicate how organizations respond to privacy issues and threats (Greenaway & Chan, 2005). Greenaway and Chan considered the Institutional and Resource Based View Theories to account for social external forces as well as sustainable competitive advantage. Prior organizational research on privacy has also considered moral responsibility in the ways organizations respond to privacy threats (Culnan and Williams, 2009). Each theory points to a need to understand the processes by which organizational privacy responses unfold. Yet, these theories are very seldom interconnected in the literature. This study presents a theoretical framework of the Privacy Impact Assessment that unifies these theories and contributes to the explanation of organizational privacy responses. The Privacy Impact Assessment is a privacy risk assessment approach that accounts for the interrelationships among different drivers and the actual outcomes and implications of enacting privacy safeguards. Previous studies have defined the Privacy Impact Assessment as a risk management tool utilized to assess the use of privacy safeguards (Culnan and Williams, 2009). PIA uses the Fair Information Practices to assess any impact on patients’ privacy.
The U.S. Department of Homeland Security defines the Privacy Impact Assessment as a decision-making tool used to identify and mitigate privacy risks at the beginning and throughout the development life cycle of a program (DHS 2010). In accordance with the guidelines set forward in the e-Government Act of 2002, the U.S. Department of Health and Human Services (HHS) began promoting the PIA as an assurance mechanism for the adequate protection of patient information (HHS 2011b). While the proposed PIA serves the interest of different health agencies (e.g., the Food and Drug Administration, the Centers for Disease Control and Prevention), it is argued that it can also serve the interest of healthcare organizations such as hospitals. Thus, it is essential to assess the privacy risks of different drivers under which organizational privacy responses might be impacted. It is also essential to assess the privacy risks associated with the practical impact. A better understanding of how to assess these privacy risks will further enhance the theoretical understanding of privacy in healthcare and its impact on healthcare practices.

Once a Privacy Impact Assessment is conducted, a variety of privacy responses are implemented to reduce the impact of a given risk. Previous studies focused more on the safeguards themselves rather than a privacy approach that takes into consideration the drivers and impacts. Thus, it can be argued that the existing frameworks are not cohesive enough to explain how and why organizations respond to privacy issues and threats (Smith et al., 2011).

http://www.bls.gov/opub/cwc/cm20030220yb02p1.htm
Empirical evidence suggests that effective privacy safeguards should account for business impact (Choi, et al., 2006; Parks, Chu, Xu, & Adams, 2011; Stahl, Doherty, & Shaw, 2011). However, very little is known about the negative impacts of privacy safeguards such as clinicians’ need for information or the impact on workflow. Moreover, there is no clear understanding of how these impacts affect the organizations’ privacy compliance. As a result, organizational leaders lack understanding of these challenges. Clearly, “there are many behavioral questions to be explored with respect to not only use of potential privacy protection tools but also effectiveness and consequences of use” (Belanger & Crossler, 2011, p. 1022). Following these calls for more efficient operational impacts of privacy safeguards, the study pursues further discussion of the factors causing the Imbalance Challenge.

A better understanding of organizational responses, their drivers, and their operational impact would allow for a better information privacy operational model to be developed in which the Privacy Impact Assessment can be an integrative part of the model. Therefore, this study aims to (1) explore the safeguards developed by healthcare organizations with regard to healthcare privacy threats stemming from the use of electronic health technologies such as EHRs, (2) understand the major drivers influencing these privacy responses in healthcare, (3) identify the outcomes of these responses on healthcare practice and delivery, and (4) identify the Privacy Impact Assessment process.
Chapter 3
Research Methodology

This chapter explains the research philosophy and how this philosophy informs the methodology adopted. It also describes the inductive theory building approach and the reasons for adopting grounded theory methodology. Data collection and analysis are described, and finally, evaluation criteria are discussed.

3.1 Research Design

Crotty (1998) outlines four elements of the research process: The ontology or (philosophical stance); the epistemology (theory of knowledge); the methodology (process of research); and the method to carry out the process data collection and analysis. Although this study has taken the interpretive perspective standpoint, the table below presents comparative definitions of the four research process aforementioned elements from both positivist and interpretive perspectives.
### Table 3-1 The Research Process

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Positivist</th>
<th>Interpretive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ontology</strong></td>
<td>What is the nature of reality?</td>
<td>Singular Reality (rejecting or failing to reject hypothesis)</td>
<td>Multiple realities (subjective)</td>
</tr>
<tr>
<td><strong>Epistemology</strong></td>
<td>Nature and scope of knowledge</td>
<td>Positivist: empirical-analytic, objectivist, functionalist</td>
<td>Interpretive: Constructivist, Post-positivist</td>
</tr>
<tr>
<td><strong>Methodology</strong></td>
<td>What is the process of research?</td>
<td>Deductive approach (based on testing a priori theories)</td>
<td>Inductive (participants views that are theorized) &amp; Deductive</td>
</tr>
<tr>
<td><strong>Methods</strong></td>
<td>What are the activities of techniques carried out?</td>
<td>Well defined sequence of operations (Surveys, experiments)</td>
<td>Ethnography, observations, interviews, surveys</td>
</tr>
</tbody>
</table>

Ontology is defined as the essence of reality under investigation (Orlikowski et al., 1991). That is, the reality is either independent of human (objective) or it only exists through human actions and interactions (subjective) (Burrell et al., 1979). Researchers who bring an objective ontology to their research believe that there is one true and objective reality. Researchers in the subjective camp believe that reality is a function of the individual’s interpretation of events and as such there is not one reality but reality is a function of individual perceptions.

Epistemology refers to the nature and scope of knowledge. That is, how do we come to know what we know? (Burrell et al., 1979; Walsham 1995). Epistemology can be broken into three broad camps: positivist, interpretive, and critical. Positivist studies, based on a priori fixed relationships, aim to test theory and increase prediction through a deductive approach (Orlikowski et al., 1991). Interpretive studies are associated with understanding phenomena under investigation through the meaning and interpretations.
assigned to them by participants and rejecting the objective and the factual (Orlikowski et al., 1991). Finally, critical studies adopt a critical stance on existing social practices (Orlikowski et al., 1991).

Methodology is defined as the strategy or plan of action that will be used to answer the research question such as: ethnography, grounded theory, case study, and survey research. Finally, research methods are defined as the activities and techniques to be carried out to collect and analyze the data such as instrument based questionnaires, interviews, focus groups, and observations.

This study used a grounded theory methodology to examine the influences, processes and impacts of how organizational responses to privacy threats. This methodology is well suited to an interpretivist epistemology that is guided by a subjective ontology.

3.1.1 Ontological and Epistemological Assumptions

I will first present my assumptions about the form and nature of reality (ontology) followed by my assumptions about the nature of knowledge claims (epistemology) while keeping consistency between both assumptions.

Ontology refers to the assumptions about knowledge. I believe that reality is subjective. That is, reality does not exist outside of an individual’s interpretations of reality. Each of us has a subjective reality that is formed by our individual perceptions and experiences. Therefore, in order to capture or identify knowledge (reality) I must
seek out individual’s interpretations of reality. This interpretivist epistemology dictates that a researcher should question individuals about their concepts and understanding of reality and only through those interpretations will I truly understand the nature of reality. My ontological assumptions recognize the existence of a subjective world where reality is “produced and reinforced by humans through their action and interaction” (Orlikowski et al., 1991, p. 14). Unlike an objective ontological research that views participants’ biases as negative, my interpretivist assumption depends on the researcher’s ability to play an active role in deciding where to investigate next and what to ask.

In case of this research study, epistemology assumptions are based on accessing reality by constructing interpretations that explain the creation of subjective meanings (Orlikowski et al., 1991; Walsham 1995). Interpretive studies assume reality is a social product where human make sense of their perceived worlds. Therefore, interpretive researchers investigate phenomena through the meanings assigned by people (Orlikowski et al., 1991). Unlike positivist research, which is based on hypothetical deductions and predetermined dependent and independent variables, interpretive research focuses on the meanings that people assign to phenomena under investigation (Klein et al., 1999). So, where does this study position itself with regard to interpretivism? This study was designed to gain an in-depth understanding of the phenomena of privacy responses in healthcare organizations. It assumes and recognizes the meanings assigned to the phenomena by organization leaders and is specific to the healthcare industry. As such, an interpretive epistemology is well suited to the research question addressed in this dissertation.
While the underlying epistemology is interpretive, this research also adopts some aspects of postpositivism. For instance, this study generated a theoretical framework based on testable propositions emerging from the constant comparison of the data. This aligns with the ontological beliefs of postpositivism (Guba and Lincoln, 1994).

3.1.2 Choice of Grounded Theory

In the early 1990s, qualitative studies, more specifically interpretive studies, represented a limited percentage (3.2%) in IS field publications (Orlikowski et al., 1991). This trend has progressively shifted, and many IS journals are now consistently publishing qualitative studies (Mingers 2003; Trauth 2001) including special issues (e.g., European Journal of Information systems, volume 21, issue 2, March 2012). Although the potential relevance of this type of research of studying real problems with real people is promising, the challenges faced by researchers engaged in qualitative studies must be emphasized (Lee, 2001). From the sample selection constraints, to good social skills, the journey can be messy with unexpected events and logistics hurdles (Edmondson et al., 2007).

Trauth (2001) presented five factors influencing the choice of qualitative research: the research problem, the researcher’s theoretical lens, the degree of uncertainty surrounding the phenomenon, the researcher skills, and, finally, the academic politics. The researcher’s choice to embrace a qualitative study stems from the nature of the research problem and the degree of uncertainty. Indeed, little is known about how organizations handle these information privacy threats (Culnan and Williams, 2009).
Thus, understanding the theoretical explanations and the outcomes of organizational information privacy is still surrounded by a high degree of uncertainty. Therefore, a grounded theory approach with an interpretive epistemology is appropriate and well suited for this study (Trauth 2001).

Klein and Myers (2001) identified a plethora of qualitative methodologies including ethnography, phenomenology, deconstruction, action research, grounded theory method and ethnomethodology. Of these methods, a grounded theory method presented the best match to this study for various reasons: lack of theory, contextualization, and practical relevance.

Corbin and Strauss (2008) describe grounded theory as a systematic approach of gathering and analyzing data that allows the research to derive constructs and build theories. Grounded theory is becoming increasingly common in the IS research literature because the method is extremely useful in developing context-based descriptions and explanations of the phenomenon (Orlikowski 1993). In this study, grounded theory methodology (Glaser et al., 1967; Strauss et al., 1998; Strauss et al., 2008) was applied for the three following reasons described below.

- **Lack of theories.** There is a lack of theories that provide ample answers on how organizations respond to privacy threats (Culnan and Williams, 2009). Thus, an inductive and theory building approach is expected to support gaining an in-depth understanding of the phenomena.

- **Dynamic and complex environment of healthcare.** Ploesser (2009) and Rosemann (2008) state that business processes are dependent on their context and
environment. Grounded theory methodology enables to “produce a theoretical accounts which are understandable to those in the area studied and which are useful in giving them a superior understanding of the nature of their own situation” (Turner 1983, p. 348). It also emphasizes the contextual complexities of the phenomena under investigation (Orlikowski 1993). Thus, grounded theory is very appropriate for the dynamic and complex environment of healthcare.

- **Practical relevance.** Healthcare research focuses on practical relevance. Grounded Theory methodology has its origin in healthcare settings (Glaser and Strauss, 1967) and thus is well suited and applicable for understanding responses to information privacy issues within healthcare organizations.

### 3.1.3 Straussian versus Glaserian Grounded Theory

Grounded theory was first introduced as a qualitative research method by Barney Glaser and Anselm Strauss in 1967 with the publication of *Discovering Grounded Theory*. In 1990, Strauss and Corbin published a book titled “Basics of qualitative research: grounded theory procedures and techniques”. This publication was highly criticized by Glaser (Glaser 1992) resulting in the emergence of the ‘Straussian’ and ‘Glaserian’ streams of grounded theory (Stern 1994). The following table (Table 3-2) attempts to summarize the data analysis differences between Glaser and Strauss.
Table 3-2 Comparison of Data Analysis Steps between Glaser and Strauss

<table>
<thead>
<tr>
<th></th>
<th>Glaser</th>
<th>Strauss and Corbin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Coding</strong></td>
<td>Open coding</td>
<td>Open Coding</td>
</tr>
<tr>
<td><strong>Intermediate Phase</strong></td>
<td>Categories Refinement</td>
<td>Axial coding</td>
</tr>
<tr>
<td><strong>Final Development</strong></td>
<td>Theoretical Coding</td>
<td>Selective Coding</td>
</tr>
<tr>
<td><strong>Theory</strong></td>
<td>Theory formulation:</td>
<td>Theory Writing</td>
</tr>
<tr>
<td></td>
<td>Substantive or formal</td>
<td></td>
</tr>
</tbody>
</table>

Both streams made valuable contributions to grounded theory research and it is important for a researcher to be aware of the type of grounded theory being used. While it is not the objective of this study to investigate in depth the disagreements between Strauss and Glaser, it is necessary to select the most appropriate approach and explain the reasons. Altogether, the approach of Strauss and Corbin seems fitting to the study’s research questions “by answering the questions of who, when, where, why, how, and with what consequences, analysts are able to relate structure with process” (Strauss et al., 1998, p. 127).

### 3.2 Data Collection

After receiving clearance from the Penn State Institutional Review Board (IRB), informants were contacted to participate in this study. The Informed Consent forms (appendix D) were emails to informants prior to conducting the interviews. Healthcare organizations were assured that the organization’s identity would be safeguarded and
would not be included in any research publications without prior permission from those organizations. To the informants, I 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. Informants were notified of the audio recording and given choice to have it turned off at any point at their request.

Data were collected from three sources: (1) semi-structured, one-on-one and group interviews, (2) participation in workshops and round tables, and (3) documentation provided by informants and/or published information. Interviews were used as the main source of data. The data collected by means of workshops and documentations were used for triangulation and for gaining additional perspectives.

Solicitation emails were sent to informants identified during workshops and conferences with large attendance by healthcare practitioners (e.g., HIMSS 2011, WHITE 2010). Request of assistance were also sent to the U.S. Department of Health and Human Services, HIMSS privacy and security committee, and Penn State Center for Integrated Healthcare Delivery Systems. An example of a solicitation email is presented in Appendix A. I used a “snowball” technique (Lincoln et al., 1985) to identify more informants.

The target population for this study consisted of key leaders who were involved in the decision making about privacy issues. The study included all common positions held by healthcare privacy experts. These positions were recommended by healthcare professionals. The study included informants holding key positions such as: Chief Information Officer (CIO), Chief Privacy Officer (CPO), Chief Medical Information
Officer (CMIO), Chief Executive Officer (CEO), and HIPAA privacy compliance officers (Table 3-3). Despite several lengthy interactions with the workshops and the round table attendees, they were not included in the interviews’ count. However their input was very valuable and used as a confirmation and validation of the findings. Table 3-3 records the type of healthcare organizations where the informants work (hospital, professional healthcare association, government, research firms and healthcare IT solution providers). Among hospitals, the study distinguishes between small, medium and large hospitals. This distinction is based on the number of beds. The American Hospital Association (AHA) classified hospitals with 100 or fewer beds into small hospitals, 500 or more into large hospitals (Kaunitz et al., 1984) while medium hospitals cover the numbers in between.

I conducted twenty three interviews with thirty informants from different healthcare organizations across the United States. Interviews were one-on-one as well as group interviews. Interviews lasted between 40 and 100 minutes and were all audio recorded (Table 3-3). The workshops and the round table (Table 3-4) lasted between one hour to sixteen (16) hours (two days).

5 http://www.aha.org/about/membership/constituency/smallrural/index.shtml
<table>
<thead>
<tr>
<th>Informant</th>
<th>Informant Position</th>
<th>Informant Background</th>
<th>Organization Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CMIO</td>
<td>Medical</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>CIO</td>
<td>IT</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>CPO</td>
<td>Business</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>CMIO</td>
<td>Medical</td>
<td>Hospital</td>
<td>Large</td>
</tr>
<tr>
<td>5</td>
<td>President</td>
<td>HPA&lt;sup&gt;6&lt;/sup&gt;</td>
<td>Healthcare Association</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>CPO</td>
<td>Law</td>
<td>Government</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>VP of IT</td>
<td>IT</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>8</td>
<td>CPO</td>
<td>Law</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>9</td>
<td>Security Officer</td>
<td>IT</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>10</td>
<td>CPO</td>
<td>Law</td>
<td>Hospital</td>
<td>Large</td>
</tr>
<tr>
<td>11</td>
<td>VP</td>
<td>HPA</td>
<td>EHRs Solutions</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>CEO</td>
<td>IT</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>13</td>
<td>Privacy Officer</td>
<td>Law</td>
<td>Hospital</td>
<td>Large</td>
</tr>
<tr>
<td>14</td>
<td>IS Director</td>
<td>IT</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>15</td>
<td>Security officer</td>
<td>IT</td>
<td>Hospital</td>
<td>Large</td>
</tr>
<tr>
<td>16</td>
<td>Privacy Officer</td>
<td>Law</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>17</td>
<td>CPO</td>
<td>Law</td>
<td>Global Research Firm</td>
<td>-</td>
</tr>
<tr>
<td>18</td>
<td>Privacy Officer</td>
<td>Law</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>19</td>
<td>IT Director</td>
<td>IT</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>20</td>
<td>CSO&lt;sup&gt;7&lt;/sup&gt;</td>
<td>IT</td>
<td>Hospital</td>
<td>Large</td>
</tr>
<tr>
<td>21</td>
<td>HIPAA Officer</td>
<td>IT</td>
<td>Hospital</td>
<td>Large</td>
</tr>
<tr>
<td>22</td>
<td>CEO</td>
<td>IT</td>
<td>Consulting Firm</td>
<td>-</td>
</tr>
<tr>
<td>23</td>
<td>CIO</td>
<td>IT</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>24</td>
<td>CIO</td>
<td>IT</td>
<td>Hospital</td>
<td>Medium</td>
</tr>
<tr>
<td>25</td>
<td>Executive Director</td>
<td>Business</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>26</td>
<td>Vice President</td>
<td>Business</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>27</td>
<td>Director of HIM&lt;sup&gt;8&lt;/sup&gt;</td>
<td>HIM</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>28</td>
<td>Executive Director</td>
<td>Healthcare</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>29</td>
<td>Privacy Officer</td>
<td>Law</td>
<td>Hospital</td>
<td>Small</td>
</tr>
<tr>
<td>30</td>
<td>IT Director</td>
<td>IT</td>
<td>Hospital</td>
<td>Small</td>
</tr>
</tbody>
</table>

<sup>6</sup> Health and Public Administration
<sup>7</sup> Chief Security Officer
<sup>8</sup> Health Information Management
Due to sensitivity of the subject of privacy, face–to–face interviews were favored initially because it allowed a more personal approach, kept the interviews deeply grounded in their contextual settings (Schultze et al., 2010), and allowed to overcome any unfamiliarity issues. Face-to-face interviews were only possible for those participants within 200-mile radius. For all others, phone interviews were conducted. Phone interview participants were not “blind dates”. For the most part, I have already met the informants at conferences and workshops and they agreed to a phone interview or were introduced through a mutual connection. Feeling comfortable and having already been introduced was the best approximation to a face-to-face personal approach. A phone interview approach expanded the geographic coverage to include healthcare organizations from

The preliminary data collection targeted only hospitals. Hospitals are categorized by ownership (for profit, not for profit), by bed size (small, medium, large), by location (rural, urban, suburban), and by activities (community, research, critical care). In this study, data collection was conducted with the purpose of doing theoretical sampling rather than by type of hospital (Glaser et al., 1967). That is, “data collection based on concepts/themes derived from the data” (Strauss et al., 2008, p. 143). Corbin and Strauss (2008) emphasize the analytical trail and the circular process between data collection and analysis until the research reaches saturation where all concepts are well defined and no new concepts emerge.

With regards to theoretical sampling, Strauss and Corbin note that the researcher must be flexible to handle the turns and twists as they arise during data collection and analysis. In this study, theoretical sampling is evident through the following statements:

- Interviewing informants has been initiated in the hospitals. However, after initial data analysis, this target was revisited to include other healthcare organizations and entities (e.g., U.S. Department of Health and Human Services, healthcare professional associations, healthcare IT providers, and healthcare privacy consultants). Based on informants’ recommendations, I also attended a week long healthcare IT conference with an attendance close to 31,000 representative healthcare government entities, academia, consultants and developers. I also
attended several education sessions as well as a privacy and security workshop and round tables.

- The initial interviews protocols addressed three major questions: (1) the privacy threats the organization face, (2) the countermeasures undertaken, and (3) the drivers behind these responses. After the analysis of the first interviews, the interview questions were also revisited to include another broad question related to the operational impacts as a result of implementing privacy safeguards. This is consistent with Strauss and Corbin’s approach to theoretical sampling where the researcher “adjusts the interviews and observations on the basis of emergent and relevant concepts” (1998, p. 207).

- The semi-structured nature of the interviews allowed further elaboration to be obtained during the interviews such as those based on the informants’ position(s) and background (e.g. an informant with a computer science background had a different perspective than an informant with a medical or a law background). Appendix B presents the interview protocol.

Although I was faced with the difficulty of getting participants because of the critical sensitivity of privacy and security topics (Kotulic and Clark, 2004), as well as the scheduling challenges of healthcare executives, interviews were conducted until the point of redundancy in the data was reached. Theoretical sampling assisted in further understanding the categories and strengthening their relationships. Hence, the theoretical saturation was reached in this study.
Documents were also collected during this study. Some documents were downloaded from the U.S. Department of Health and Human Services, HIMSS. Other information obtained directly from informants. Appendix K provides exemplary documents.

3.3 Data Analysis

In this section, for the purpose of clarity, an overview of the tasks undertaken using the grounded theory approach is provided. The data analysis revolved around identifying and relating the codes, categories, themes, and dimensions. These tasks were grouped into a two-stage process, the first order and the second order data analysis (Van Maanen 1979). The first order analysis represented identifying and relating the codes and categories, while the second order themes represented identifying and relating the themes and dimensions at a higher level of abstraction. NVivo (V.9), a computer-aided qualitative data analysis software tool, was used to assist at all levels of analysis. Nvivo facilitated setting up concepts within themes, called nodes, and provided some data analysis capabilities for searching, grouping, and relating nodes. Data Analysis steps are depicted in Figure 3-1.
3.3.1 First Order Data Analysis

The first step in data analysis involved coding of the interview transcripts. Coding is the process of conceptual abstraction. Put simply, coding means taking pieces of raw data and using labels (codes) to describe events, and characteristics. These codes were initially as close to the data as possible. In line with grounded theory methods, I used an inductive approach, which does not use a predefined set of codes, but rather identifies ‘in vivo’ codes that arise from the data. For the first order analysis, I embraced an open coding approach in order to brainstorm and open up the data to all potentials and possibilities. The coding involved the identification and comparison of key concepts using Corbin and Strauss’s (2008) constant comparative approach.
3.3.2 Second Order Data Analysis

Using the first order analysis results from the step above, there was the emergence of certain categories but not all relationships were defined. Corbin and Strauss (2008) refer to this step as axial coding which is the act of relating concepts and categories to each other and constructing a second order model at a higher theoretical level of abstraction. This step involved an iterative process of collapsing the first order codes into theoretically distinct themes (Eisenhardt 1989b). The safeguards used to mitigate privacy issues were grouped into technical, human, physical controls and administrative processes. The drivers influencing these safeguards were grouped into institutional, competitive advantage, resources and ethical integrity. Finally, the positive and negative impacts formed the Imbalance Challenge.

3.3.2 Emerging Theoretical Framework

The final stage of the analysis consisted of determining how the various themes that have been previously identified could be linked into a coherent framework explaining how organizations respond to information privacy threats. Axial coding was followed by selective coding where the core category was identified and other categories were linked to it. The core category of this study is represented by the Privacy Impact Assessment. Indeed, it is “not until the major categories are finally integrated to form a larger theoretical scheme that the research findings take the form of a theory” (p. 143). Developing the overall theoretical scheme by relating categories to the core category is followed by “refinement” (Strauss et al., 1998). Refinement of the theoretical framework
was accomplished by revisiting the data, documents, as well as relating to the literature documents.

Relevant literature was reviewed from both the IS and health informatics communities in order to identify potential contributions of the findings to the privacy literature in the healthcare context. The review consisted of information privacy related work with a special focus on existing theories and frameworks at the organizational level. I integrated the context of healthcare by reviewing health informatics research. Upon this review of the strengths and weaknesses of the existing literature, it was decided to 1) focus on the drivers influencing privacy safeguards and assess the privacy impact associated with each in order to strengthen the lack of theories explaining how organizations handle privacy responses (Greenaway & Chan, 2005), 2) break out of the box of drivers and responses (Hodgkinson et al., 2010) to include the Imbalance Challenge of privacy safeguards that were not part of the original research before the data analysis. Capturing the Imbalance Challenge allowed for a better integration of a Privacy Impact Assessment into the theoretical model.

### 3.4 Evaluation 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. In what follows, two approaches for judging interpretive research are presented: (1) ensuring trustworthiness (Lincoln et al., 1985) and (2) ensuring the
adequacy of the research process and the empirical grounding (Strauss et al., 1998; Strauss et al., 2008). These approaches are explained next and applied to the theoretical framework in the discussion chapter.

3.4.1 Ensuring Trustworthiness

The aim of trustworthiness is to support the premise that the study’s findings are “worth paying attention to” (Lincoln et al., 1985, p. 290). Lincoln and Guba (1985) offered a set of four trustworthiness criteria appropriate for interpretive research and analogous to positivist research: credibility, transferability, dependability, and confirmability. These criteria are listed and described next, and will be evaluated later in the study.

Table 3-5 Trustworthiness Criteria

<table>
<thead>
<tr>
<th>Trustworthiness Criteria</th>
<th>Traditional Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credibility</td>
<td>Internal Validity</td>
<td>Evaluation whether the study findings represent a credible interpretation of the data collected</td>
</tr>
<tr>
<td>Transferability</td>
<td>External Validity</td>
<td>Applicability and extension of the study’s findings beyond the bounds of the project</td>
</tr>
<tr>
<td>Dependability</td>
<td>Reliability</td>
<td>Assessment of stability and consistency of the study’s processes of data collection, data analysis, and theory generation</td>
</tr>
<tr>
<td>Confirmability</td>
<td>Objectivity</td>
<td>Measurement of how the study findings are supported by the data collected</td>
</tr>
</tbody>
</table>
3.4.2 Ensuring the Adequacy of the Research Process and the Empirical Grounding

Corbin and Strauss (2008) identified eight criteria for evaluating the empirical grounding component of the study (Table 3-6). Each criterion is described next and will be checked for applicability at the end of the discussion section.

### Table 3-6 Ensuring the Adequacy of the Empirical Grounding

<table>
<thead>
<tr>
<th>Evaluative Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion 1</td>
<td>Are concepts generated?</td>
</tr>
<tr>
<td>Criterion 2</td>
<td>Are the concepts systematically related?</td>
</tr>
<tr>
<td>Criterion 3</td>
<td>Are there many conceptual linkages and are the categories well developed? Do they have conceptual density?</td>
</tr>
<tr>
<td>Criterion 4</td>
<td>Is much variation built into the theory?</td>
</tr>
<tr>
<td>Criterion 5</td>
<td>Are the broader conditions that affect the study built into its explanation?</td>
</tr>
<tr>
<td>Criterion 6</td>
<td>Has process been taken into account?</td>
</tr>
<tr>
<td>Criterion 7</td>
<td>Do the theoretical findings seem significant and to what extent?</td>
</tr>
<tr>
<td>Criterion 8</td>
<td>Does the theory stand the test of time and become part of the discussions and ideas exchanged among relevant social and professional groups</td>
</tr>
</tbody>
</table>

Strauss and Corbin (1998) and Corbin and Strauss (2008) identified seven more criteria for evaluating the adequacy of the research process. The following criteria will be evaluated throughout the study (Table 3-7).
### Table 3-7 Ensuring the Adequacy of the Research Process

<table>
<thead>
<tr>
<th>Evaluative Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 1</strong></td>
<td>How was the original sample selected? On what grounds?</td>
</tr>
<tr>
<td><strong>Criterion 2</strong></td>
<td>What major categories emerged?</td>
</tr>
<tr>
<td><strong>Criterion 3</strong></td>
<td>What were some of the events, incidents, or actions (indicators) that pointed to some of these categories?</td>
</tr>
<tr>
<td><strong>Criterion 4</strong></td>
<td>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?</td>
</tr>
<tr>
<td><strong>Criterion 5</strong></td>
<td>What were some of the hypotheses pertaining to conceptual relations (i.e., among categories), and on what grounds were they formulated and validated?</td>
</tr>
<tr>
<td><strong>Criterion 6</strong></td>
<td>Were there instances in which hypotheses did not explain what was happening in the data? How were these discrepancies accounted for? Were hypotheses modified?</td>
</tr>
<tr>
<td><strong>Criterion 7</strong></td>
<td>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?</td>
</tr>
</tbody>
</table>

This chapter sets the methodological foundation for the data collection process and the data analysis. Grounded theory methodology was selected because of lack of existing theory to explain how organizations respond to privacy threats, contextualization of healthcare domain, practical relevance and suitability to study healthcare processes.
Chapter 4
Emergent Key Concepts, Themes, and Dimensions

In this chapter, 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). While Figure 4-1 and Figure 4-2 depict the emerging themes individually, it is worth noting that the dimensions were not as straightforward as suggested by these figures. Some themes were complex, and many were interactive with other themes. For example, when an organization considers the influencing drivers, it assesses the risk of not abiding by healthcare regulations. It also looks into the potential reputational damage along with the needed resources. One privacy officer stated:

“Everyone is constantly in the back of their minds measuring risk all the time. So, I think that’s why you always do what the law says. That’s a risk not worth taking. But then you have to look at other kinds of risks, too, for what you may do or may not do and what is the risk of reputational harm or financial harm or all those other kinds of things, how that comes into play.”
Figure 4-1 Emergent Dimensions: Threats, Drivers, and Safeguards
<table>
<thead>
<tr>
<th>1st Order Concepts</th>
<th>2nd Order Themes</th>
<th>Aggregate/Overarching dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilitation of access to legitimate users</td>
<td>Controlled Access</td>
<td>Positive Impacts</td>
</tr>
<tr>
<td>Prohibition of access to those with no “need to know”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grisly analogy deterred inappropriate access</td>
<td>Deterrence Effect</td>
<td></td>
</tr>
<tr>
<td>Awareness programs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit and investigation of access</td>
<td>Tracking Mechanisms</td>
<td></td>
</tr>
<tr>
<td>Tracking of unauthorized access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barriers accessing patient information</td>
<td>Information Unavailability</td>
<td>Negative Impacts</td>
</tr>
<tr>
<td>Information not accessible when needed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional privacy features delaying the orderly workflows</td>
<td>Workflow Disruptions</td>
<td></td>
</tr>
<tr>
<td>Time-out features</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User unfriendly/not usable</td>
<td>Usability Issues</td>
<td>Leadership Commitment</td>
</tr>
<tr>
<td>Employee struggles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inability to encrypt every flash drive</td>
<td>Operational Feasibility</td>
<td></td>
</tr>
<tr>
<td>Cost of time, money and efficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospital size</td>
<td>Organizational Context</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>Academic status of hospital</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leadership buy-ins</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leaders’ educational background</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessment of the all the drivers</td>
<td>Assessment of Drivers &amp; Impact</td>
<td></td>
</tr>
<tr>
<td>Implications of privacy safeguard enactments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance challenges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact of operational feasibility</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4-2 Emergent Concepts, Themes, and Dimensions in Organizational Privacy Responses
4.1 Perceived Privacy Threats

Though the focus of this study was on the way organizations respond to information privacy threats, it only made sense to ask the informants broad questions about the major privacy issues and threats facing healthcare organizations. The analysis indicated that four major factors contributed to the classification provided: (1) unauthorized and inappropriate access of patient information, (2) data disclosure and secondary use by third parties, (3) loss of hardware, and (4) ubiquitous technologies. These threats are illustrated in Figure 4-3.

![Healthcare Privacy Threats Diagram](image)

Figure 4-3 Perceived Privacy Threats

4.1.1 Unauthorized Access

Health and medical data are privileged information and should be accessed based on a “need to know” basis (Croll 2011; Halamka et al., 1997). This concept is hard to comprehend, especially by the medical staff who previously had unlimited and unquestioned access to all medical data, whether it belonged to their own patients, a
family member, or another individual. One Chief Medical Information Officer made the following statement:

“I think that any healthcare system will tell you that the concept of need to know in healthcare is probably the most difficult to understand . . . the old method of thinking was, if there is a patient in my hospital, I have a right to that information. It is our hospital and the idea that only having right to information that you need to know to do your job is a tough thing to get into their [clinicians’] heads.”

Unauthorized access, sometimes referred to as inappropriate access, is the most frequent and acted-upon privacy threat. This type of threat includes abuse by authorized personnel who are browsing records for curiosity purposes (e.g., accessing family members’ records) or who have ulterior motives (e.g., accessing celebrities’ medical information or credit card scams). One example of such behavior was described by a privacy officer, who explained:

“We had an employee who had access to billing information and credit card numbers, and this guy was a criminal, and he used that information, this guy had the need to know this information, he used that information, he had packages delivered to people’s houses, like he would go to stores, he would purchase online, purchase high ticket items, track the purchase of these high ticket items to these people’s houses. And before they could come out and pick up the boxes that were delivered by the UPS, he would swing by, pick up the package and go sell it back to the store that he bought from for cash.”
Unauthorized access also includes hacking by external entities, which results in damage such as data breaches.

### 4.1.2 Unintended Data Disclosure and Secondary Use

In the healthcare industry, it is often necessary to disclose medical data to patients or clinicians to support treatment. Data are also disclosed for billing, quality and research. Furthermore, data are not only disclosed to business associates\(^9\) but are also utilized for secondary use. Secondary use of information involves new uses of data collected by healthcare organizations. According to a Chief Privacy Officer, secondary uses of healthcare data are very important for research; the quotation below illustrates her thoughts on the subject about it:

> “There is a great need for secondary uses of health data. That’s where much of the information comes from that we are now using for research for public health. To be able to find cures for diseases or to improve public health, to improve disparities, or to improve access to care, all those many things that are on everyone’s mind.”

Secondary uses of patient data constitute a threat for several privacy leaders because of their fear of losing control over the ways these data are subsequently protected.

---

\(^9\) A business associate is any entity with whom the healthcare organization is doing business (e.g., doctor’s office, cleaning company, vendors, and suppliers).
4.1.3 Lost and Stolen Hardware

Lost and stolen devices accounted for 34% of healthcare reported breaches (HHS 2009). This threat was emphasized during a major privacy and security workshop (e.g., HIMSS 2011). Stolen devices included laptops, flash drives, and even servers. Often, clinicians access patient information from their mobile devices, then leave them in odd places, such as restaurants. Such devices are also stolen from unattended cars and even from hospitals. One Chief Information Officer stated:

“The area for most vulnerability for loss of data is the loss of hardware, primarily laptops and servers. This is surprising, but people steal servers. Yes, a big server! . . . Flash drives and laptops are probably one of the biggest [thefts].”

4.1.4 Misuse and Security Concerns of Ubiquitous Technologies

In a paper-dominated healthcare industry, access was centralized because healthcare workers needed to be physically present at the facility where they needed access to their patient records. With the recent advances in information and communication technology, employees can obtain access to the same data from their smart phones, laptops, home computers, and tablets. This practice represents a significant privacy threat in healthcare because it is very challenging to control who actually looks at those records from home and whether the device used to access information has the appropriate security mechanisms. The ubiquitous use of these technologies is adding further challenges to healthcare organizations. One Information Security Officer of a large hospital in the Northeast of the United States of America stated:
“We have a change in our environment because we have employees that are working from home . . . so that definitely adds additional challenges and things that need to be looked at and [they] drive our policy and some of the controls we have in place.”

An additional threat is associated with the use of social media (e.g., Facebook, Twitter, YouTube, etc.), where confidential information is informally disclosed. The vice president for information management shared his concern over social media and the privacy threat posed by employees posting sensitive information:

“[We] look at the social media and how to address that from a security and privacy perspective, and a couple of different avenues of what I’m talking about is how you handle employees posting information, say, on Facebook.”

Additional details for the above categories and representative data can be found in Appendix B.

4.2 Privacy Response Drivers

The data analysis revealed four categories of drivers that impact how privacy responses might be developed. These drivers include (1) institutional pressures in the form of regulatory and reputational pressures, (2) available resources, (3) competitive advantage, and (4) ethical considerations. Each driver is assessed to identify its impacts and the risks associated when not accounted for (e.g., penalties for not complying with healthcare regulations).
4.2.1 Regulatory Pressures

Healthcare organizations face different pressures influencing their decisions in responding to information privacy threats. These influences can be exercised by regulatory pressures but can also be derived from the organization’s fear of reputational damage associated with privacy breaches.

The data analysis revealed that federal (e.g., HIPAA and HITECH) and state laws\(^\text{10}\) and regulations are amongst the most cited drivers responsible for the ways organizations respond to privacy issues and threats. Organizations abide by the law because they have to do so. With the latest healthcare federal legislation (e.g. HITECH), the threats of higher penalties and imprisonment are forcing organizations to make efforts to comply with the law and develop the appropriate privacy safeguards. One privacy officer noted,

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

\(^{10}\) Appendix H provides a sample of breach notification laws by state.
Table 4-1 Institutional Pressures as a Driver

<table>
<thead>
<tr>
<th>Institutional Pressures</th>
<th>Type</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA</td>
<td>Federal (1994)</td>
<td>Privacy rule:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Requires appropriate safeguards to protect the privacy of personal health information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Sets limits and conditions on the uses and disclosures of patient information</td>
</tr>
<tr>
<td>HITECH</td>
<td>Federal (2009)</td>
<td>Amendments to HIPAA privacy rule:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Report of breaches of 500 patients or more</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Advertise in media outlets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Increased civil and criminal penalties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Reputational damage</td>
</tr>
<tr>
<td>State Regulations</td>
<td>State regulations vary from State to State (Appendix H)</td>
<td>Organizations need to abide by federal guidelines but must follow state regulations if they are more stringent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- According to the federal government, organizations have 60 days to report a breach.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- According to the State of California, organizations have five business days to report a privacy breach.</td>
</tr>
</tbody>
</table>

In addition to regulatory pressures, organizations reported that they feared the potential of reputational damage from privacy breaches. In fact, if a breach of 500 or more patients occurs, organizations have to reach out to every single patient, as well as advertise the breach through news media outlets. Reporting a breach in the media incurs reputational damage that healthcare organizations would rather avoid. One Chief Privacy Officer stressed the importance of reputational damage as stated below:
“If they are not treating individuals’ information with the respect, not safeguarding individual health information, then of course the repercussions from that can be really damaging. And the first thing is the reputational damage.”

When assessing whether to account for healthcare regulations or not, two elements were identified that should be weighed when responding to privacy threats: (1) the risks associated with following the law and negatively impacting healthcare processes creating a tension between the law and practice of medicine, and (2) risks associated with the fines and reputational damage for not abiding by the regulations. This dilemma is accurately illustrated by a healthcare leader in the following statement:

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

4.2.2 Resources

Organizations usually rely on internal as well as external sources to provide funding to support their privacy safeguards. Internal funding is directly associated with the organizational resources, while external is based on other sources such as government funding, grants, or loans. Funding safeguards to mitigate privacy threats are not inexpensive. The capital, technical, and human resources are outlined in Table 4-2. For example, to train employees to satisfy HIPAA privacy requirements, an organization
must account for the cost not only in dollars, but also in impact on and disruptions of healthcare delivery. According to a Chief Privacy Officer, the cost of training a hospital workforce in a large hospital can easily span beyond a million dollars:

“*We obviously expect the employees to get trained completely on HIPAA, we will do retraining if things change, but that’s not done that often. It’s actually very expensive to do, and if you think about it, a work force of 60,000 people, let’s just say on average, it takes half hour to complete the training, that’s 30,000 man hours; let’s put a labor rate of $50 an hour, it’s a $1,500,000 just in lost labor time. I understand that we need to do it, but it is a cost. There is a lot of training that we do in this organization, and you have to balance all of that against what the disruption is going to be on services.*”

Table 4-2 Resources as a Driver

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital resources</td>
<td>Hiring consultant firms or audit companies</td>
</tr>
<tr>
<td>Human resources</td>
<td>Privacy officers, legal staff</td>
</tr>
<tr>
<td>Technical resources</td>
<td>IT solutions and equipment</td>
</tr>
</tbody>
</table>

The availability of resources impacts how much organizations can invest into their privacy responses. From hiring the appropriate workforce to buying and maintaining technical solutions, the amount of resources needed to handle these initiatives is not insignificant. These resources are budgeted out of the organization’s operating budget.
4.2.3 Competitive Advantage

Protecting patient information from external and internal unauthorized access and other threats is considered a competitive advantage (Jinye et al., 2010; Ravera et al., 2004). To achieve such competitiveness, healthcare organizations rely on significant resources and invest in privacy safeguards. As stated by one Chief Medical Information Officer:

“There is the business driver whereas you want to be viewed at, you want to be competitive, and you need IT to be competitive, you need the safeguards to be competitive, because if you have a breach, would you come here? No.”

Healthcare organizations have to report their breaches to the U.S. Department of Health and Human Services, which maintains a website listing healthcare privacy breaches (HHS 2011a). This negative exposure could impact their market share and consumers’ trust. Competitive advantage, in terms of protecting patients’ information, is highly valued, as illustrated by a Chief Privacy Officer:

“When they [patients] go to a hospital, they expect that that hospital can be trusted with their money, their data, and their body. I think the difference, though, is healthcare for some individuals anyway, is such a personal kind of thing, maybe more so than the amount of money in their bank account.”
4.2.4 Ethical Integrity

The concept of ethical integrity initially was difficult to conceptualize because several informants were referring to the “right thing to do” vis-a-vis their patient information. The second order construct of "ethical integrity" emerged from the analysis to capture three first order constructs mentioned by informants: best practices, ethics, and culture of privacy. One privacy officer defined ethical integrity as doing the right thing regardless of any pressures:

“What do you do when nobody’s looking? Do you still do the right thing you know? And that, to me, is the definition of ethics.”

Table 4-3 Ethical Integrity as a Driver

<table>
<thead>
<tr>
<th>Ethical Integrity</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Practices</td>
<td>A set of practices that are exercised and practiced regardless of existence of mandated regulations (i.e., protecting data at rest and in motion, encouraging employees to go beyond basic patient requirements)</td>
</tr>
<tr>
<td>Ethics</td>
<td>Moral responsibility by leaders and clinicians</td>
</tr>
<tr>
<td>Culture of Privacy</td>
<td>Culture that promotes legal compliance with an emphasis on ethical behaviors where everyone is being held accountable</td>
</tr>
</tbody>
</table>

Implicitly or explicitly used by the informants, ethical integrity takes precedence over regulations, because it sets higher standards than simply meeting the regulatory requirements. This assumption is clearly stated by a Chief Medical Information Officer:
“It is not like we did not care about information before, now all of a sudden the legislation makes you compliant with this; that is a poor assumption. We clearly value patients, health information security at the highest level . . . 8 years ago, before HITECH, even before HIPAA stuff, all those considerations of who needs to see what information, where is it secured, where are the displays for the screens, things like that, were all inherent to what we are doing.”

Ethical integrity is also considered to be part of a set of good business practices rather than the mandates organizations have to adhere to. Good business practices allow organizations to operate in a healthy environment that fosters protection of patient information. One privacy officer noted:

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

Firms achieving ethical integrity have, for example, a culture of privacy that promotes legal compliance with an emphasis on ethical behaviors. The data analysis revealed the importance of a privacy culture, supported by leadership, to create an environment where everyone would hold themselves accountable. This concern for privacy is expressed by a Chief Privacy Officer who shared the possible struggles that could arise when a culture of privacy is lacking:
“Culture can make or break a privacy officer. It absolutely can. If you’ve got support at the very top from your CEO, that makes your job a whole lot easier because people will pay attention.”

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

4.3 Privacy Safeguards

With the goal of developing a taxonomy of privacy safeguards at the organizational level, this study sought to document the variations in responses to privacy issues, in the complex and challenging environment of healthcare. Therefore, the study included a broad question about privacy safeguards and countermeasures that are used in healthcare organizations. Evidence of four major types used to mitigate privacy issues in healthcare has been found in the course of this research (Table 4-4): (1) technical controls, (2) human controls, (3) physical controls, and (4) administrative processes. One Chief Medical Information Officer summarized most of these categories as follows:

“Privacy of health information is a priority and we have policies and procedures and infrastructure that support that approach to patient information. The details around it and what is required to operationalize [safeguards] get adjusted based upon both internal and external information. So if we would identify something internally where we have a risk, we would address that whether it is a technological fix, education, or process fix . . . If an external pressure like HIPAA
or HITECH would come by, we will, of course, need to adjust based upon additional information or additional requirements."

Table 4-4 Classification of Organizational Privacy Responses

<table>
<thead>
<tr>
<th>Privacy Safeguards</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Controls</strong></td>
<td>- Role-based access controls</td>
</tr>
<tr>
<td></td>
<td>- Encryption of data at rest and in transit</td>
</tr>
<tr>
<td></td>
<td>- Monitoring and audit controls</td>
</tr>
<tr>
<td></td>
<td>- Intrusion detection alerts</td>
</tr>
<tr>
<td><strong>Human Controls</strong></td>
<td>- Awareness, training, and education initiatives</td>
</tr>
<tr>
<td></td>
<td>- Disciplinary actions, including termination</td>
</tr>
<tr>
<td></td>
<td>- Creating staffing positions</td>
</tr>
<tr>
<td><strong>Physical Controls</strong></td>
<td>- Positioning and visual set up of computers</td>
</tr>
<tr>
<td></td>
<td>- Access to physical locations through badges</td>
</tr>
<tr>
<td></td>
<td>- Hidden location of data center</td>
</tr>
<tr>
<td><strong>Administrative Processes</strong></td>
<td>- Effective organizational policy generation and enforcement</td>
</tr>
<tr>
<td></td>
<td>- Developing privacy enhancing policies, guidelines, and recommendations at different levels of the organization</td>
</tr>
</tbody>
</table>

4.3.1 Technical Controls

Healthcare organizations develop a wide range of technical safeguards to handle the threats of accessing patients’ data from unauthorized users. Though the frequency of technical measures was high, the details about the technical specifications were not always granular. This was either due to the fact that technical safeguards were handled by a different department than the informant’s or to the fact that the background of the privacy officer (i.e. law, medical, business) did not allow him/her to provide thorough
details of his/her organization’s technical safeguards. The focus of this study was not mainly on technical safeguards, so while privacy leaders were given opportunities to elaborate during the interviews, no further questions were pushed by the researcher. For example, details about the different type of privacy safeguards were requested; however, no specific technical details were pursued (e.g., the level of encryption or the type of wireless security protocols).

The findings revealed three major types of technical safeguards: access control, encryption, and audit controls. With access being a major privacy issue, it was obvious that a large number of technology efforts were centered on this area, especially implementing role-based access and monitoring its use as illustrated by a Chief Information Officer:

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

Despite their already high commitments to technology, informants kept looking for more technological capabilities to handle data monitoring and audits. A Chief Privacy Officer stated:

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

4.3.2 Human Controls

Experts clearly distinguish between technical and human safeguards. In this section, the findings were categorized into education (including training and awareness efforts), disciplinary actions, creating privacy positions, and creating a culture of privacy. Education, training, and awareness programs are high on the list of priorities among the leaders of healthcare organizations. However, these educational efforts face challenges related to the cost and the amount of information retained by employees. The latter is a major concern, as one Chief Privacy Officer noted:

“[A] typical employee is going to retain three or four or maybe five concepts at most . . . people have done studies about what people retain. So what we try to do is, periodically [publish] articles in our employee newsletter to let people know what’s going on.”

Disciplinary actions, including termination of employment, were undertaken when employees failed to follow the privacy guidelines and principles outlined during their education, training, and awareness programs. According to a privacy officer:
“We have actually terminated people for accessing family, you know, particularly, say, if there is a messy relationship and one spouse complain and it is found to be true.”

Another interesting aspect of human controls is hiring privacy personnel or, more precisely, appointing existing personnel to a position of a privacy officer as is required by HIPAA. This is illustrated by a Chief Privacy Officer’s statement: “We have privacy officers . . . none of our privacy officers are full time, meaning they have other jobs.” The workload of these additional assignments takes about 25% of their time and increases up to 100% during investigations. Across organizations, these assignments were quite intriguing, as the backgrounds of the privacy leaders were completely diverse, from clinicians, to lawyers, to managers of medical records, to CIOs.

Finally, cultivating a culture of privacy starts with support from the organization’s top executives and survives through the employees’ buy-ins. Such sponsorship from organizational leadership is paramount to privacy initiatives within an organization, and it mainly translates into generously allocated resources to uphold privacy programs. As one Chief Privacy Officer stated:

“You’ve got support at the very top from your CEO that makes your job a whole lot easier, because people will pay attention. If you have others promoting you and your program, that helps a lot. If your company hired a Chief Privacy Officer just because they had to because HIPAA said we did or just because they want to pretend like they care, but they don’t really care, you’re not going to be
successful. Ultimately, you’re just going to continue to beat your head against a wall, and you won’t get the resources that you need, your budget won’t be what you need it to be, you won’t have the staffing, and it’s you know you’re standing in quick sand, hoping for the best and then it’s not working”

4.3.3 Physical Controls

Physical controls received the least amount of attention as far as their frequency in this study. However, they seem to represent a very important safeguard, the lack of which can be an open invitation for potential breaches. Physical countermeasures included such simple tools as one-way glass or simply asking for a physical badge before allowing access to an area. As part of their physical controls, a privacy officer of a medium size hospital stated:

“[W]e do rounding to look at the computers to see if a screen if visible. We have put one-way glass in certain area so the public cannot walk by and look in and see a computer. We’ve taken steps like that.”

4.3.4 Administrative Processes

Administrative processes, a perpetual hot bed for trials and errors, include two major components. The first component consists of developing effective organizational policy generation and its enforcement. Indeed, informants were stressing the importance
of having policies that were in sync with their healthcare operations rather than non-effective policies. One privacy officer noted:

“The worst thing you could do is have a lawyer write your policies and put them in a book. They are not true. It is better to have an operations person, the person who would actually have to do or supervise that work and then have them [policies] reviewed and tweaked to make sure that they meet the law. Because otherwise, if you just have policies that have been written by someone who has no idea how your organization runs, they will go to the binder but nobody follows them. And not following your policies is worse legally than not having a policy at all.”

The second component consists of developing a hierarchy of privacy-enhancing policies, guidelines, and recommendations at different levels of the organization, such as processes to handle data access and personnel termination. This is illustrated by a privacy officer who stated:

“Our current administration process, first of all, is making sure that those people who need access to the system they requested are audited, and we can know who they are. [There is a] process in place when someone leaves, whether it is a termination or a transfer. We have a process in place that we make sure that they get off the system and no longer have access to it.”

The above categories as well as representative data for each of the categories are presented in greater detail in Appendix D.
4.4 Imbalance Challenge

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

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

In this study, privacy leaders reported intended consequences (positive impacts) and unintended consequences (negative impacts) of enacting privacy safeguards in healthcare organizations. No concerns were noted when there was a dominance of positive impacts. However, when the negative impacts outweigh the positive impacts, a state of imbalance has been reported. Thus the term Imbalance Challenge emerged to reflect organizations’ struggles between maintaining patient privacy and not inhibiting the business.

In this section, findings about the positive impacts and negative impacts are reported. Negative impacts are identified by information unavailability, disruptions of workflows, usability issues, and operational feasibility issues. Positive impacts are identified through a deterrence approach, controlled access and tracking mechanisms.
When negative impacts outweigh positive impacts, a state of imbalance is created. This state of imbalance triggers privacy compliance challenges that are further discussed in the next chapter.

### 4.4.1 Negative Impacts

Throughout this research project, healthcare leaders stated on numerous occasions that privacy threats do not end with the implementation of privacy controls. They uniformly emphasized the need for better understanding and handling of the conflicting challenges that arise. Hence, a thorough understanding of these factors and their impacts on business practices is fundamental for explaining and possibly addressing the Imbalance Challenge. One Chief Privacy Officer commented, “There is a lot of indirect impact . . . It’s got to be costing us money or it’s got to be costing us efficiency.” The impact of privacy safeguards brings out a balance issue that is of high concern to healthcare leaders. This section includes the analysis of the influence of four facets of negative impacts: (1) unavailability of information, (2) workflow disruptions, (3) usability issues, and (4) operational feasibility.

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

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

Several healthcare leaders discussed the ways in which implementing privacy safeguards influenced the availability or accessibility of patient information. Not having 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 lab tests, but may not need to see a progress note on a psychiatric condition or a psychotherapy note. The desire to balance the implementation of privacy programs and the healthcare delivery appeared to have created a serious issue for clinicians trying to provide care for their patients, which ended up opening doors for potential unauthorized access and impacting their privacy compliance. As was noted by one of the healthcare executives:

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

Another healthcare executive noted that:

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

There are potential impacts to privacy compliance with the Imbalance Challenge. When healthcare leaders described the challenges of information availability and accessibility of data, they connected it to their compliance with healthcare regulations. There is a worrisome aspect of compliance concerning the law and its impact on privacy compliance. One of the privacy officers described it well: “We have lots of policies and everybody else has lots of policies, but we can’t meet the regulations in the strictest letter of the law and offer clinicians the ability to practice in an efficient, cost-effective manner.”

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

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

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

Another example of workflow disruptions is password management. Healthcare is swamped with different applications, and employees have to log on to different systems to access information about their patients. One informant commented on the difficulty in managing different passwords: “I am using application A, application B and you get all these passwords you got to remember. Guess what? I am going to start writing them down.” Employees start writing down their passwords, which potentially makes the organizational network easily accessible to hackers or unethical co-workers. This
ultimately hinders privacy compliance instead of facilitating it as first intended by instating a password.

Organizations tend to consider these impacts in order to avoid push-backs and workarounds. A Chief Information Officer commented: “We try to take that into account, the workflow issues, when you are looking at a policy because there is no sense in establishing a policy that people will not adhere to.”

Although mitigation tools were put in place to bring the hospitals into compliance, in some cases, they ended up negatively impacting the hospitals’ adherence to regulations. In the case of workflow disruptions issues, employees found ways around these mitigations tools to accomplish their duties. This workflow disruption is illustrated by the nurses’ work practices that one of the study informant shared:

“40% of the work that a nurse does is to administer medication. 40% of her day, she is looking for pills and administering them . . . She is logging in and waiting, waiting, waiting, waiting. That is a problem; she is not going to get her job done. It’s hard enough to do the charting, administering medicine without the waiting, waiting, waiting. So what most hospitals do is they have these computers-on-wheels, and they wheel [such a computer] into the patient’s room and they leave it logged on and they administer the medicine and they wheel it out and they leave it logged on, and then they go into the next room and then leave it logged on. But when they go back to the medicine room it’s logged on and that’s a security risk.”
Usability Issues: The usability challenges that emerged from the data analysis include applications or systems of electronic health records (EHRs). The challenges arise from dealing with inherent difficulties associated with the task of using certain applications. Over the course of this study, healthcare executives explained that they had to take into consideration the usability of the privacy safeguards they put in place or embedded in their IT applications:

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

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

Operational Feasibility Issues: Many of the informants commented on the operational feasibility of the privacy safeguards implemented in their hospitals, which usually involves resources, time, and efficiency. As stated by one of the informants:
“So it does have an impact on resources and operation. You’re going to get to a point where people are going to have to have staff in place to just deal with that one situation, just to keep up with what they’re going to have to do to make sure they protect themselves. It’s got to be costing us money or it’s got to be costing us efficiency.”

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

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

4.4.2 Positive Impacts

Three factors—controlled access, deterrence effect, and tracking mechanisms—were identified with regard to the positive impacts of privacy safeguards.
**Controlled Access:** The enactment of technical privacy safeguards, such as role based access control (RBAC) mechanisms, allowed for better control of who is accessing the system. Filtering out users who have no business looking at patients’ data was a positive impact of enacting privacy safeguards. For example, environmental health workers might need access to parts of patients’ record to perform their jobs; however, they do not need full access. This ability to limit access based on the employees’ job function is illustrated by a healthcare executive: “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 components of your records that are important to the environmental health workers to do their job.”

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

“It is sort of user grisly analogy. Back in medieval England when they chopped people’s heads off, they would put [that] head on a pike, and they stick it on the London Bridge, and the idea was that it would allow you to see who had their head chopped off. It was a very public hanging. And so, it’s the same thing here, we can’t necessarily say who we fire, but you hope the word gets out, you hope the employee that gets fired almost says, I can’t believe they fired me for looking
at that. Well okay fine, I want you to tell your co-workers, because I want your coworkers to say, I am not going to do this again because I don’t want to have the same thing happen to me, or I don’t want to be suspended.”

Tracking Mechanisms: The ability to track the identity of the users who accessed specific information, along with when they accessed it, was perceived by organizational leaders as a major positive impact of privacy safeguard enactments. The ability to go back and investigate any questionable access was perceived by privacy leaders as a positive outcome. One Chief Medical Information Officer stated:

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

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

4.4.3 Imbalance Challenge

Capturing the Imbalance Challenge was a major finding in this study. The Imbalance Challenge is an analytical construct that was created to make sense of what
organizations reported they are faced with as a result of enacting information privacy safeguards. As shown in Figure 4-4, an Imbalance Challenge occurs when the negative impacts of enacting privacy safeguards outweigh the positive ones. The challenge resides in the organizations’ struggles in maintaining patient privacy and without inhibiting business processes. One privacy officer illustrated this Imbalance Challenge by stating:

“The biggest challenge with respect to privacy and health care in my mind is this notion that you have to err on the side of providing additional information access. You can’t afford to put a barrier in front of a physician or clinician when they need to have access to the information.”

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

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

The primary four dimensions of organizational context that emerged from this study include: (1) hospital size, (2) academic status, (3) leader’s educational background, and (4) leadership commitment.

4.5.1. Hospital Size

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

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

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

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

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

4.5.2 Organization’s Academic Status

Among the healthcare organizations interviewed, academic hospitals are associated with large hospitals and tied to medical schools and ongoing research about protected health information (PHI). These organizations have very well-established rules and IRBs with regard to PHI. Therefore, institutions with teaching hospitals have an
existing culture of privacy practices. Healthcare organizations with academic affiliations showed evidence of more awareness of privacy through stricter guidelines for medical students, resulting in expulsion from medical programs when patient’s privacy guidelines were not observed properly. Teaching and research hospitals are also more aware of the secondary use of patient data.

4.5.3 Professional Background of Privacy Officers

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

The above categories and representative data for each of them are presented in detail in Appendix F.
4.5.4 Leadership Buy-Ins

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

“If you don’t have that [buy-in from leadership], no matter what you implement, you are not going to have the resources in the first place”

4.6 Privacy Impact Assessment

The data analysis revealed a risk assessment rationale that privacy leaders undertake in the process of responding to information privacy threats. This risk assessment involves a few factors such as evaluating the appropriate processes and policies or listening to patients’ and clinicians’ needs. One Chief Privacy Officer commented on this assessment process:
“What I try to do is listen to both the clinicians, physicians, and patients . . . try to understand what the perspectives are and try to develop systems that, in processes and policies, are reasonable based upon our needs to access information as well as to allow our patients to feel comfortable that their information is being protected.”

Besides evaluating the privacy threats, organizations undertake a risk assessment in two major areas: influencing drivers and implications of privacy safeguards enactments. First, the analysis showed that healthcare organizations have to assess regulatory pressures, potential reputational damage, and available resources when responding to privacy threats. The privacy assessment involves evaluating each driver separately, then all drivers as they interact together. One Chief Privacy Officer commented on the assessment of available resources:

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

Another privacy leader commented on the risk assessment of all drivers combined:

“You always do what the law says. That’s a risk that’s not worth taking. But then you have to look at other kinds of risks, too, for what you may do or may not do and what the risk of reputational harm or financial harm or all those other kinds of things, how that comes into play.”
The second area of assessment included evaluating the actual outcomes of privacy safeguards in which organizations engage. Such assessments resulted in the emergence of the concept of Imbalance Challenge that healthcare organizations need to account for when responding to information privacy threats.

The concept of the Privacy Impact Assessment (PIA) emerged as a representation of how healthcare organizations respond to privacy threats in light of the different drivers (e.g., regulations, reputation, resources, and ethical considerations) and the implications of privacy safeguard enactments. The emergence of this analytical concept, which was created by the researcher to make sense of what organizations actually do, helped in understanding that responding to privacy threats is not as static and straightforward of a process as it seems, nor is it as simple as investing in few countermeasures. This process involves more well-thought processes, and it was effectively described by a consultant in healthcare privacy and security:

“*There were some that went out and bought an expensive tool thinking that would solve the problem for them. But because they didn’t understand the concept of risk analysis, having the tool is not going to help you . . . if you don’t understand the concepts of cabinetry or woodworking, going out and buying an expensive miter saw is going to be worthless, ‘cause you’re not going to know what to do with it.*”

At the early stages of analysis, the emergence of the PIA appeared to be important. Additional data were acquired using theoretical sampling until this category
was saturated (Urquhart et al., 2010). The study commenced tracking this concept’s development through attributes related to risk assessment, balance issues, and operational impacts. Subsequent interviews included a direct question about it, which led to some interesting comments. For instance, one privacy expert noted:

“Healthcare organizations and IT have to get used to identifying risks and managing risks. That’s what other organizations are doing, like banking and things like that. We need to take risk assessments to heart. I think the industry as a whole has been lacking in following that . . . it is hard to do when you’re getting started, when you’re learning the process, but once you have it figured out and you’ve got it where it should be integrated in your environment, it’s going to do nothing but help you. When we looked at vendors coming, bringing products in again by being involved early on, we could do that risk assessment up front.”

The emergence of the PIA concept facilitates understanding the processes healthcare organizations have to undertake to respond to privacy threats. These processes take into consideration the different drivers influencing the organization’s actions, but also account for the implications of information privacy safeguard enactments.
Chapter 5

Discussion and Theoretical Framework

This chapter presents the theoretical framework grounded by the findings from the empirical study with support from the relevant extant literature. First, I elaborate upon the categories from Chapter 4—Privacy Threats, Privacy Drivers, Privacy Safeguards, Privacy Impact Assessment, Imbalance Challenge, Privacy Compliance, and Leadership Commitment—and discuss their relationships that led to the emergence of the two core themes, the PIA and the Imbalance Challenge. These major categories are found within the IS, organizational behavior, and health informatics communities, yet they are very seldom interconnected in the literature. Next, the study presents a theoretical framework that unifies these concepts and thereby contributes to the explanation of organizational responses to information privacy threats. Finally, this chapter examines the study in light of existing research and evaluates the proposed theoretical framework using various evaluation criteria (outlined in Chapter 3) for judging interpretive research.

5.1 Shaping the Theoretical Framework

The constant analysis of the data led to the emergence of major categories—Privacy Threats, Drivers, Privacy Safeguards, PIA, Imbalance Challenge, Privacy Compliance, and Leadership Commitment. Close analysis of the data revealed interrelations among these categories and allowed for their integration into a theoretical framework (Strauss et al., 1998).
The analytical process undertaken in this chapter aims at finding patterns and interrelationships among the categories. Indeed, a higher level of abstraction is used to identify the conceptual relationships between the categories. As a result, the two core themes—the PIA and the Imbalance Challenge—which form the theoretical framework emerged.

5.1.1 The First Emerging Theme: The PIA

The first emerging theme focuses on a risk assessment approach, which encompasses the identification and assessment of privacy. This theme focuses on privacy threats and privacy drivers as the reasons why organizations respond to privacy threats. It also reflects on different approaches organizations take to respond to these threats. Therefore, this theme seeks to address the following research questions: Why do healthcare organizations respond to privacy threats (drivers)? What are the mechanisms used by healthcare organizations to mitigate information privacy threats? Furthermore, this theme shapes the first core category named the PIA.

When considering the process of PIA, I found that the organization’s proactive or reactive strategic approach was categorizing drivers into two clean-cut groups: facilitating drivers and inhibiting drivers. Before moving forward with this analysis any further, both proactive and reactive type of strategies within healthcare organizations will be clarified.
- **Proactive type of organizations.** Proactive organizations exhibited very
distinct behaviors regarding their approaches to responding to privacy threats.
These behaviors consisted of having foresight and looking for patterns to
anticipate issues or opportunities for changes, developing well thought-out
strategies, and taking effective actions. Prospectors are considered proactive
strategies by seeking new products and markets and by seeking to protect core
competences (Miles et al., 1978). In the present study, healthcare
organizations exhibited proactive strategic behaviors: (1) by developing
privacy audit plans that have not yet been made available by the regulatory
body, (2) by seeking feedback from key representatives of each department
before rolling out their privacy safeguards, and (3) by revisiting their plans to
incorporate better alternatives. Such proactive behavior was also exhibited
when healthcare organizations contacted their State legislature representatives
and/or professional organizations to lobby for better laws to protect patient
privacy without hindering healthcare delivery.

- **Reactive type of organizations.** Reactive behaviors consisted of behaviors
opposite to the ones pertaining to proactive type organizations. For instance,
when asked about the effectiveness of their actions (e.g., implementing
privacy safeguards), a proactive organization would have revealed a set of
measurements, while a reactive organization’s common response would be to
wait for complaints to be reported before undertaking any actions.
Therefore, in considering the proactive and reactive approaches, there is a need to distinguish between two different drivers: (1) facilitating drivers that act as catalysts for undertaking the assessment of threats, capabilities, and shortcomings, and (2) inhibiting drivers that act as barriers to undertaking effective privacy solutions.

With regard to the relationship between proactive strategy and enabling drivers, an organization with a proactive approach evaluates the impact of each driver. In other words, it assesses if it is worth paying penalties for non-compliance with healthcare regulations. It also evaluates the potential reputational harm in case of a privacy breach. The analysis revealed a relationship between high levels of institutional and ethical considerations with higher intentions to assess these drivers. However, if these drivers were associated with a reactive type approach, the organization would be less likely to perform a PIA and would instead be “responding inappropriately to environmental change and uncertainty, performing poorly as a result, and then being reluctant to act aggressively in the future” (Miles et al., 1978, p. 557). Based on the study findings, these drivers acted as facilitators when the organization exhibited a proactive type of organizational strategy in which it was demonstrating attitudes toward responding to privacy threats beyond seeking regulatory compliance.

Similarly, there was a relationship between reactive strategy and inhibiting drivers. The data showed that, regardless of the organization’s strategy, resources were a major handicap with respect to what a hospital could or could not do. While proactive organizations would undertake a limited assessment, reactive type organizations would wait because “they could not afford to” — a possible reason for not undertaking any
assessment. Therefore, the reactive type strategy, coupled with the lack of resources and the lack of leadership commitment, acts as an inhibitor to undertaking a PIA.

![Diagram of Enabling and Inhibiting Drivers]

Figure 5-1 Enabling and Inhibiting Drivers

The central role of PIA is emphasized by integrating the dynamics of the drivers (via organizational proactive or reactive approach) and identifying the threats toward effective organizational privacy safeguards. These relationships are further discussed in the propositions section.

5.1.2 The Second Emerging Theme: Imbalance Challenge

The second emerging theme, which is named the *Imbalance Challenge*, relates the categories of privacy safeguards to privacy compliance. This theme is focused on the intended and unintended consequences (positive and negative impacts) of enacting
privacy safeguards and their implications on privacy compliance. Therefore, this theme seeks to address the third research question of this study: “How does the implementation of privacy safeguards impact healthcare workflow and processes?”

This theme is focused on the outcomes rather than the antecedents of privacy safeguards and emerged as a result of the negative impacts overpowering positive impacts. In this study, the term “impact” emerged when investigating the changes in operational healthcare workflow and work practices after privacy safeguards were implemented. Indeed, enactment of privacy safeguards impacted healthcare activities and was reflected through positive and negative impacts. In this study, the term “impact” is used to describe the challenges organizational leaders identified from their operational processes and work practices after the enactment of privacy safeguards.

When considering the relationship between privacy safeguards and privacy compliance, the study revealed that the implementation of privacy safeguards does not necessarily lead to positive impacts. In the presence of negative impacts, employees find ways to work around privacy practices that could be harmful to their privacy compliance.

In using grounded theory, Urquhart (2010) emphasized leveraging a systematic and iterative approach to theory conceptualization. Embracing this approach for this study enabled further analysis of the negative impacts. I pursued a theoretical sampling in an attempt to increase my knowledge of the implications of privacy safeguards’ enactment, their impact on business practices, and their implications for privacy compliance. Accordingly, this research was focused on answering a question: “What are the implications of privacy safeguards?” The data analysis revealed that the tension and
strain due to negative impacts causes a state of imbalance, termed the *Imbalance Challenge*, where negative impacts are overpowering positive impacts.

Further analysis revealed distinction between: (1) organizations in which leaders were not aware of the negative impacts and (2) organizations that were aware of the negative impacts and accounted for the Imbalance Challenge in how they responded to privacy threats. In fact, when asked how they measured the effectiveness of their safeguards, the former organizations indicated that there were no formal metrics in place to assess the impacts, positive or negative, of their privacy safeguards’ implementation. Instead, they relied on the number of complaints, or reported breaches, as an indication of the effectiveness of their safeguards. Once these organizations became aware of the negative impacts, they considered revisiting their safeguards to account for the Imbalance Challenge. In these instances, awareness only happened when privacy compliance became an issue. If the organizations’ privacy compliances were not in jeopardy, would they ever become aware of other negative impacts? Additional analysis revealed that organizations that were aware of the negative impacts had performed a PIA. Such initiatives allowed organizations to look out for these impacts, sometimes to prevent them or at least to minimize them. Ultimately, a proactive assessment versus a reactive approach seems to distinguish these two types of organizations and further explains the Imbalance Challenge. Indeed, organizations with a proactive approach are trying to develop their metrics to assess negative impacts. Relationships between the Imbalance Challenge, privacy safeguards, impacts, and privacy compliance are depicted using propositions in the next section.
5.1.3 The Entwined Relationship between the Themes

Both the PIA and the Imbalance Challenge emerged as distinct but mutually linked themes. In fact, they are complementary. The integration of both the PIA and the Imbalance Challenge contribute to a more elaborate theoretical framework portraying the dynamics of how organizations respond to privacy threats in healthcare.

The entwined relationship between the PIA and the Imbalance Challenge themes is apparent *in the iterative relationship* between the PIA and the Imbalance Challenge. That is to say, when the Imbalance Challenge is identified, the organization re-evaluates its PIA to account for this challenge. As a result, an adapted privacy safeguard is implemented that could positively or negatively impact work practices which lead to starting the iterative cycle again. For example, the enactment of a privacy safeguard such as role-based access control may not allow a physician access to a patient admitted in another department, which could be harmful in an emergency situation. As a response to this Imbalance Challenge, organization leaders implement the “break the glass” utility. “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. The access must be appropriate to avoid disciplinary procedures. Therefore, accounting for the implication on work practices allows organizations to provide exceptions to their standard privacy responses in order to reduce the negative impacts of the lack of availability of information. This iterative relationship between the PIA and the Imbalance Challenge
might not always be obvious, especially in organizations where leadership commitment is minimized.

The relationship between the PIA and the Imbalance Challenge is also apparent through organizational privacy compliance. For instance, the Imbalance Challenge that results from non-usability of privacy safeguards, or from disruption of workflows, generally leads to employees’ workarounds. These workarounds, such as bypassing privacy policies or ignoring encryption requirements, can result into data landing in the wrong hands and negatively impacting privacy compliance. It is apparent that even when the Imbalance Challenge is not acted upon, the correlation between both themes still exists. The relationship between both themes is discussed in more detail in the following section.

5.2 Formulating the Theoretical Framework

The emerging theoretical framework is based on the interactions of the core themes previously identified: the PIA and the Imbalance Challenge. These themes are entwined to form the theoretical framework of *Organizational Responses to Information Privacy Threats*. In this section, I will provide an explanation of the emerging theoretical framework and discuss its propositions.

The theoretical framework developed from this work is stated below:

*The Privacy Impact Assessment (PIA) within healthcare organizations is shaped by a dynamic interplay between privacy threats, organizational drivers, and the Imbalance Challenge. Responding to privacy threats without accounting for the
Imbalance Challenge causes potential negative operational impacts to outweigh positive impacts. Therefore, the PIA is characterized by the iteration between undertaking a risk assessment of privacy threats and existing drivers, management of privacy safeguards, and evaluation of their impacts. In order to manage this process, healthcare leaders are driven to act proactively and to apply appropriate strategies to accurately assess privacy threats while handling the impact of privacy safeguard enactments on healthcare workflow and work practices.

A diagrammatic representation of this dynamic interplay is represented in Figure 5-3 with a set of theoretical propositions.

Figure 5-2 The Emerging Theoretical Framework
5.2.1 Discussion of the PIA

The study identified four major threats that healthcare organizations and hospitals in particular, have to deal with: (1) unauthorized access, (2) unintended data disclosures, (3) loss of hardware, and (4) misuse of ubiquitous technologies such as mobile devices, wireless technologies, and social media. Privacy threats are generated from both internal and external sources. For fear of financial losses, breaches of privacy, or damage to their reputation, organizations tried to understand and assess the risks associated with these threats. The study findings show that organizations assessed the potential outcomes of each threat and acted upon the ones associated with higher negative outcomes (Wallace et al., 2004).

In this study, four major drivers emerged as the influential factors behind organizational responses to privacy threats. In the findings section, I provided a detailed description of (1) regulatory pressures; (2) financial, human, and technical resources; (3) competitive advantage via reputation and image; and (4) ethical considerations and best practices. This study further links these drivers, along with the organizations’ proactive or reactive strategic approaches with the facilitating and inhibiting drivers.

Organizational strategy can emerge for different reasons, whether by simply springing from frequently launched new initiatives (proactive approach) or in the aftermath of long experience of a maintenance approach that “goes with the flow” (reactive approach) (Van Maanen et al., 1979). Proactive organizations exhibit a variety of behaviors, including feedback seeking (Ashford et al., 1985; Crant 2000), courageous
acts (Hornstein, 1986), strategic prospecting (Miles et al., 1978), and task revision (Staw and Boettger, 1990). Based on the study findings, these drivers act as facilitators when organizations exhibit a proactive type of organizational strategy that supports decision-makers’ attitudes toward proactively responding to privacy threats beyond seeking regulatory compliance. As a result, proposition one was developed:

**Proposition 1:** With the proactive type of privacy strategy, organizations are more likely to leverage their threats and drivers to undertake a PIA when responding to privacy threats.

Similarly, a reactive type of organization exhibits a “drift-threat-reaction” attitude, which means that an organization’s privacy safeguards tend to “drift” until they are confronted by an external “threat,” and then such organizations “react” with formalized policies and interventions (1993). For example, due to a lack of resources, organizations may delay implementation of privacy safeguards until mandated by law. As a result, proposition two states the following:

**Proposition 2:** With the presence of the reactive type of strategy, organizations are less likely to embrace a PIA when responding to privacy threats.

The findings suggest that PIA was very important because it impacted the types of safeguards organizations would implement to mitigate privacy threats. On paper, a combination of technical safeguards, physical safeguards, human safeguards, and organizational processes makes sense. Yet, organizations continue to face breaches, which suggest that “existing compliance programs are not effective” (Culnan and
Williams, 2009, p.678). This data clearly demonstrates that when organizations assess different drivers and threats, they are more likely to enhance the likelihood that effective privacy safeguards will be implemented. This evidence leads to the following proposition:

**Proposition 3:** Embracing a PIA enhances the likelihood of effective privacy safeguards to be implemented.

### 5.2.2 Implications of the Enactment of Privacy Safeguards

In healthcare, the need to implement the appropriate privacy safeguards is as unquestionable as the need to protect patient privacy, confidentiality, and the integrity of electronic health records. However, defining how privacy safeguards can be effective and what their implications are is a far more complex task. This study explores the implications of information privacy safeguard enactments on healthcare workflow and work practices.

As shown previously, different types of information privacy safeguards contribute to the possibilities which allow organizations to respond to privacy threats and achieve compliance. However, some of the major challenges faced by healthcare organizations is establishing safeguards in harmony with the “actual day-to-day procedures” (Choi, Capitan, Krause, & Streeper, 2006).

Organizations implement privacy safeguards with the purpose of mitigating information privacy threats and ensuring compliance. While only positive impacts were expected by privacy leaders, negative impacts were also identified. The data showed
evidence of four negative factors: (1) unavailability of information to provide adequate care to patients, (2) workflow disruptions, (3) usability issues of privacy applications and processes, and (4) operational feasibility issues.

This study further suggests that the level of negative and positive impacts have to be considered if an organization was proactive or reactive in its PIA. Whereas proactive organizations are capable of identifying and acting upon the negative impacts of enacting privacy safeguards, reactive organizations become aware much later (i.e. when privacy complaints or breaches are reported). A priori awareness of potential negative impacts allows leaders to implement the appropriate safeguards, to minimize the negative impacts, and to maximize the positive impacts. Therefore, the following proposition was reached:

**Proposition 4:** In the absence of a proactive approach, the implementation of privacy safeguards is more likely to lead to: (1) a higher degree of negative impacts, and (2) a lower degree of positive impacts.

With regard to the research questions RQ3a and RQ3b, “What are the intended consequences (positive impacts) of privacy safeguards?” and “What are the unintended consequences (negative impacts) of privacy safeguards?” the findings identified more factors than those exhibited by the literature. Healthcare leaders provided many examples in terms of how they implemented privacy protective safeguards and how they were mindful of the negative impacts associated with these safeguards. But in discussing the negative impacts on practices, factors that were positively impacting healthcare practices were also identified.
5.2.3 Effect of Positive and Negative Impacts on Imbalance Challenge

Organizations implement privacy safeguards for the purpose of mitigating information privacy threats and ensuring legal compliance. However, the emergence of negative impacts was also an important concept. Indeed, much of the research on privacy safeguards assumes a positive impact where the sequels of post implementation (e.g., negative impact) are often overlooked. The Imbalance Challenge is impacted by positive and negative impacts.

These types of impacts tend to negatively shift the desired balance organizations are targeting. As such, we expect the unavailability of information needed to treat a patient to create an environment of Imbalance Challenge between protecting patient information and treating the patient. Similarly, disruptions in workflow, usability, and operational issues could slow down healthcare deliver. Based on these findings, it is conceivable to suggest that the negative impacts lead to a higher degree of the Imbalance Challenge. The following proposition was developed:

**Proposition 5:** A higher degree of negative impacts leads to a higher degree of the Imbalance Challenge.

Healthcare organizations seek to achieve protection of both patients’ information and regulatory compliance. In doing so, they implement privacy safeguards pertaining to minimizing privacy breaches and abiding by regulatory pressures. While the negative impacts of adopting privacy safeguards lead to a state of imbalance, organizations
leverage the positive impacts of adopting privacy safeguards to further minimize the negative impacts. Therefore, the following proposition is presented:

**Proposition 6:** A higher degree of positive impacts leads to a lower degree of the Imbalance Challenge.

### 5.2.4 Effect of the Imbalance Challenge on Privacy Compliance

The findings suggest that the issues surrounding the organizational struggles to meet the ever-increasing privacy constraints and to comply with regulatory requirements have become a central concern to healthcare leaders. In particular, the Imbalance Challenge emerged as the key concept with regards to these struggles. If unattended, the Imbalance Challenge has the potential to become harmful to the organization’s compliance. This study provides evidence that healthcare professionals may see a need to improvise or to work around their privacy safeguards. Existing health informatics literature defines workarounds as clever alternative methods developed by the users to accomplish what the system does not easily allow them to do (Ash et. al., 2004). Morath and Turnbull (2005) define workarounds as ‘‘work patterns an individual or a group of individuals create to accomplish a crucial work goal within a system of dysfunctional work processes that prohibits the accomplishment of that goal or makes it difficult’’ (p. 52). The workaround phenomenon has been recognized in both IS and health informatics literature (Pollock 2005); however, limited studies theorize this concept (Halbesleben et al., 2008) especially with regards to information privacy.
This study provides three themes with regard to workarounds: (1) conditions leading to workarounds, (2) evidence of these workarounds, and (3) concerns surrounding the potential consequences of these workarounds. These themes are summarized in Figure 5-3.

<table>
<thead>
<tr>
<th>Conditions Leading to Workarounds</th>
<th>Evidence of Workarounds</th>
<th>Potential Consequences of Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Information Unavailability</td>
<td>- Ignoring Encryption</td>
<td>- Intercepted Unencrypted Records</td>
</tr>
<tr>
<td>- Workflow Disruptions</td>
<td>- Borrowing Password</td>
<td>- Inability to Track Actual Users</td>
</tr>
<tr>
<td>- Usability Issues</td>
<td>- Unattended Logged on Computers</td>
<td></td>
</tr>
<tr>
<td>- Operational Feasibility</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5-3 Model of Workarounds

Healthcare professionals seek to balance privacy demands with the need to provide care for their patients, all in an efficient manner. The study provides evidence of the struggles that privacy leaders face to the effect of the Imbalance Challenge. A striking example was provided by a Chief Privacy officer who stated that clinicians sometimes bypass privacy safeguards to do their job, which involves saving lives. He emphasized that he would rather explain the office of civil right why one of the hospital’s employee inappropriately accessed information (e.g., used someone else’s log in credentials) rather than having to explain to a family that he could not save their loved one because of privacy safeguard enactments. The concern surrounding such action is that the same access that saved lives could also hinder privacy compliance. The same Chief Privacy officer referred to the case of Arizona Representative who was admitted to a hospital
after being shot and how several employees lost their jobs for inappropriately looking up her medical records.

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

**Proposition 7:** The stronger the Imbalance Challenge, the higher the frequency of workarounds occurred.

**Proposition 8:** The higher the frequency of workarounds occurred, the lower the degree of organizational privacy compliance.

With regards to the research question RQ3c, “What are the implications of these opposing impacts on privacy compliance?” the data revealed that the implementation of information privacy protective safeguards is influencing healthcare work practices
through positive and negative impacts and thus is creating an Imbalance Challenge. Achieving a balance in privacy and utility by maximally reducing negative impacts was 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, and workforce needed at unexpected times and locations, often conflicted with privacy role-based access safeguards (Boxwala et al., 2011) and therefore made the Imbalance Challenge even more important. The positive impact of privacy protective safeguards may function as a facilitator to privacy compliance while negative impact may function as inhibitors. Identifying these impacts is not enough. In fact, healthcare leaders must also address the Imbalance Challenge that ultimately defines their compliance.

Top management support emerged as an essential element impacting privacy compliance. As a result, there seems to be a significant positive correlation between having the appropriate management support in handling the Imbalance Challenge and the privacy compliance. The role of leadership commitment is discussed in the next section.

5.2.6 Iterative Relationship between the PIA and the Imbalance Challenge

The iterative relationship between the PIA and the Imbalance Challenge is apparent in how organizations responds to threats and follow up on the implications of information privacy safeguard enactments. This iterative relationship starts with assessing the privacy risks and enacting the appropriate privacy safeguards, followed by monitoring the consequences of these safeguards for any positive and negative impacts. When the
Imbalance Challenge is identified, the organization re-evaluates its PIA to account for these challenges. As a result, an adapted privacy safeguard is implemented, and the lifecycle starts again.

Assessing regulatory pressures, resources, competitive advantages, and best practices is very important when responding to information privacy threats. However, the PIA must be capable of assessing the negative and positive impacts of privacy safeguards. The findings suggest that organizations that integrated an iterative approach of re-evaluating their PIA in light of the Imbalance Challenge have greater chances of developing more appropriate privacy safeguards. Therefore, mitigating information privacy threats while accounting for the Imbalance Challenge leads to better information privacy responses.

**Role of Leadership Commitment in Pursuing PIA**

The entwined relationship between the PIA and the Imbalance Challenge is supported by support from top management. Recognizing the importance and implications of the leadership support reflects broader impact in organizational beliefs and attitudes. Having this support is seen as an asset in undertaking a PIA Securing patient privacy is no small task (Choi, 2006), and having the leadership commitment constitutes a proactive approach to appropriately securing patient confidentiality.

Top management support includes funding support, technological support, and experience support. In terms of funding support, it is clear that several initiatives and protective safeguards could not have been implemented. The data provided evidence of the importance of funding. Funding support was not always a handicap for smaller
hospitals, as they were able to be more creative in certain instances. For example, small hospitals cannot afford outside consultants for audits and social engineering, so in one case, the compliance officer performed tours and walkthroughs, talked to employees, and even checked trash cans for possible record violations. In terms of technological support, top management played a critical role, particularly in allocating central IS resources to facilitate the implementation of privacy safeguards and technical tracking mechanisms. In terms of experience support, the top management was crucial. By attending several executive functions and meeting with peers at social and professional events, the top management developed a deeper understanding of the capabilities of different tools and strategies being used. This allowed management to invest in those resources with stronger potential that may be less expensive.

**Effect of Leadership Commitment in Handling the Imbalance Challenge**

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

**Proposition 9:** With stronger leadership commitment, the iterative relationship between the Privacy Risk Assessment and the Imbalance Challenge will be stronger.

5.3 Relating to the Literature

The emergent theoretical framework of organizational responses to information privacy threats indicates a set of drivers, organizational factors, and outcomes that is relevant to its context. This section attempts to compare these categories and relationships with those from related literature.
5.3.1 Relating to the Literature on Risk Management

In Chapter 2, an argument was made for a new theory that handles the significant gaps in the literature on organizational privacy responses and their outcomes. Existing theories separately point to a need to understand the processes by which organizational privacy responses unfold. Yet, absent from the literature is how organizations assess the dynamics of these theories taken together. Therefore, a call has been made for a risk assessment approach through the PIA.

When relating the PIA to the literature, I started by approaching this concept simply as an extension of security risk management. However, the PIA is different from security risk management. First, the concepts of information privacy and information security hold different meanings, as one respondent pointed out:

“Security is a technology-centric activity, whereas privacy really isn’t. You could put a lot of security stuff in place, but you are not going to solve your privacy problems . . . you can’t solve a privacy problem by implementing more security; you can’t improve security by improving privacy. They are really different, distinct, unique disciplines, and people want to lump them together, not realizing that they are really dramatically different, and how you have to approach them is dramatically different. You can use technology to help support privacy, like using login tools, but it is still processes; it’s a lot of other things.”

This comparison is also supported by the literature, in which information privacy concerns refer to control over access to information, while security refers to all measures that protect information privacy (Fernando et al., 2009). Security risk management was
traditionally a technology-driven approach using different computing technology assets to handle known threats (Gerber et al., 2005). However, current research has embraced a more business-driven approach to account for employees’ awareness, participation, and behaviors (Bulgurcu et al., 2010a; Siponen et al., 2010; Spears et al., 2010).

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

Since privacy safeguards encompass a plethora of IT safeguards, it is worth comparing privacy risk assessment to IT risk management. IT risk management pertains to anticipating, preventing, and mitigating problems arising from the implementation of IT projects, including issues with personnel, communication, and coordination (Mohtashami et al., 2006). Due to its focus on technology and IT projects, IT risk management presents only a limited perspective compared to PIA.

It can be concluded that the existent IS literature supports the findings of the present study. What distinguishes the PIA from the existing literature is the fact that it serves as an assessment bridge between the threats, privacy safeguards, and their drivers, as well as the implications of privacy safeguard enactments. The PIA assesses the threats and their impacts as well as the privacy safeguards and the implications of their enactments. As such, the PIA is developed to ensure that the organizations’ practices are
consistent with the FIPs regarding the collection, use, and dissemination of information. The PIA maintains this consistency while also using the appropriate safeguards, using best practices, and embracing a sense of moral responsibility through a privacy culture (Culnan and Williams, 2009).

5.3.2 Relating to the Theory of Balance

When relating the Imbalance Challenge to the literature, this study applies the lens of balance theory to seek an explanation for the contradictory positive and negative impacts and the Imbalance Challenge. According to Heider (1946) and Lewin (1951), Balance Theory is viewed as a structural arrangement between social actors and affective ties. If these arrangements create an imbalance (tension or strain), actors will attempt to reduce the imbalance. For example, as a result of a discomfort in a relationship, an actor may take a detachment action. Contrary to the balance theory’s expectation of detachment, the data from this study reveal that once healthcare leaders become aware of the negative impacts, they work on resolving the negative impacts rather than distancing themselves. In situations where privacy safeguards are in the way of healthcare delivery, healthcare leaders increase their involvement rather than reduce it. For example, when clinicians could not access the records they needed, leaders reviewed policies and a “break the glass” escape mechanism was created to allow clinicians to bypass access controls. Also, because of the penalties associated with breaches, organizations could not afford to avoid taking actions.
5.3.3 Relating to Privacy Calculus

The opposing concepts of negative and positive impacts of the Imbalance Challenge led us to consider the privacy calculus theory in the privacy literature (see Culnan & Bies 2003 for a review). This theoretical framework has been applied at the individual level (e.g., Dinev & Hart 2006; Xu et al., 2010) and provides insights that are worth taking into account at the organizational level. Privacy calculus considers two sets of opposing factors: inhibitors and facilitators to behavioral intentions (such as willingness to conduct online transaction or intention to disclose information). A user’s decision to transact online is based on the outcome of weighing both sets of factors: if the effects of the facilitating factors (i.e., trust and control) are greater than those of inhibiting factors (i.e., privacy concerns and perceived risk), the user is more likely to engage in an eCommerce transaction. While the individual user has to make a priori decisions, the Imbalance Challenge in this study pertains to consequences of these decisions at the organizational level. Moreover, the privacy calculus allows the individual user to “calculate” if it is beneficial or not to engage in an online transaction. In the theoretical model in this study, organizations do not “calculate,” but rather deal with the consequences, which is the Imbalance Challenge. The Imbalance Challenge results from negative impacts outweighing positive impacts.

5.3.4 Relating to Organizational Behavior Literature

This study revealed the organization’s strategic type as an important factor for enabling or inhibiting embracing the PIA. Therefore, exiting theoretical framework with
regard to proactive and reactive approaches will be compared with those typologies of Oliver (1991) and Miles and Snow (1978).

Drawing on the resource dependence and institutional literature, Oliver (1991) posited that organizations may pursue five broad strategies in responding to institutional pressures. With respect to the level of resistance to these pressures, these responses varied on a continuum from passive conformity to active manipulation: acquiescence, compromise, avoidance, defiance, and manipulation (Oliver, 1991, p. 151; see Table 1). First, organizations may embrace an acquiescence strategy and comply with institutional pressures. As a second approach, and through compromise, organizations can partially comply with institutional pressures. Avoidance is the third possible approach, as organizations can conceal or escape compliance. Fourth, organizations may challenge the institutional requirements through defiance. Oliver’s conceptual framework (1991) received widespread attention and several studies provided empirical evidence (Clemens et al., 2005; Ingram et al., 1995). The present study agrees with Oliver’s different strategies (as indicated in Table 6-1). However, these strategies are viewed more as behaviors that can be exhibited separately or jointly. For example, an organization can embrace acquiescence and manipulation by fully complying with the HIPAA privacy and security rules and, at the same time, can influence and/or control healthcare regulations through lobbying. Moreover, Oliver only accounts for resources dependence and institutional pressures as drivers. In the healthcare environment, the best practices are critical. For instance, healthcare organizations cannot exhibit a defiance strategy to HIPAA privacy and security rules, because it is in the patients’ best interest to have safeguards to protect their health information.
Miles and Snow (1978) offer a theoretical framework that considers three interrelated problems: the entrepreneurial pertaining to the organization’s definition of a product-market domain, the engineering related to the technologies and processes in relationship with the engineering solution, and the administrative problem pertaining to ways the organization implement its strategies. Miles and Snow (1978) developed an adaptive cycle topology of four strategic types of organizations: the prospector, the analyzer, the defender, and the reactor. While the adaptive cycle refers to the dynamic approach of organizations’ continuous adjustment to their environment topology, the strategic types represent alternative forms, each of which has its own adaptive strategy (Miles et al., 1978). In comparison to the typology proposed by Miles and Snow (1978), the present study aligns with two organizational strategy types: the prospector and defender (proactive) and the reactor (reactive) (Table 5-1).

In summary, this chapter introduced a theoretical framework of organizational responses to information privacy threats and discussed the relationships between the major categories. This theoretical framework was initially limited to explaining a phenomenon (responding to privacy threats) in the area studied (healthcare) (Glaser et al., 1967; Strauss et al., 2008). However, by integrating insights from the related literature, this study concludes with a stronger theoretical framework.
Table 5-1 Strategies for Resistance and Accommodation to Institutional Pressures

<table>
<thead>
<tr>
<th>Oliver Strategies</th>
<th>Oliver Tactics</th>
<th>Oliver Examples</th>
<th>Healthcare Privacy Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquiescence</td>
<td>• Habit</td>
<td>• Following invisible, taken-for-granted norms.</td>
<td>Adopting and complying fully with the HIPAA privacy and security rules.</td>
</tr>
<tr>
<td></td>
<td>• Imitate</td>
<td>• Mimicking institutional models.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Comply</td>
<td>• Obeying rules and accepting norms.</td>
<td></td>
</tr>
<tr>
<td>Compromise</td>
<td>• Balance</td>
<td>• Balancing the expectations of multiple constituents.</td>
<td>Negotiating through healthcare chapters such as HIMSS(^{11}) and CHIME(^{12}) to meet the external requirements at a reduced cost.</td>
</tr>
<tr>
<td></td>
<td>• Pacify</td>
<td>• Placating and accommodating institutional elements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bargain</td>
<td>• Negotiating with institutional stakeholders.</td>
<td></td>
</tr>
<tr>
<td>Avoidance</td>
<td>• Conceal</td>
<td>• Disguising nonconformity.</td>
<td>Writing policies that do not reflect organizations’ actual enactments of privacy.</td>
</tr>
<tr>
<td></td>
<td>• Buffer</td>
<td>• Loosening institutional attachments.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Escape</td>
<td>• Changing goals, activities, or domains.</td>
<td></td>
</tr>
<tr>
<td>Defiance</td>
<td>• Dismiss</td>
<td>• Ignoring explicit norms and values.</td>
<td>Opposing the HIPAA privacy and security rules by healthcare organizations.</td>
</tr>
<tr>
<td></td>
<td>• Challenge</td>
<td>• Contesting rules and requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Attack</td>
<td>• Assaulting the sources of institutional pressure.</td>
<td></td>
</tr>
<tr>
<td>Manipulation</td>
<td>• Co-opt</td>
<td>• Importing influential constituents.</td>
<td>Influencing and/or controlling healthcare regulations through lobbying.</td>
</tr>
<tr>
<td></td>
<td>• Influence</td>
<td>• Shaping values and criteria.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Control</td>
<td>• Dominating institutional constituents and processes.</td>
<td></td>
</tr>
</tbody>
</table>

\(^{11}\) Healthcare Information and Management Systems Society. [http://www.himssconference.org](http://www.himssconference.org)

5.4 Evaluating the Study

This study is evaluated through (1) Lincoln and Guba (1985) criteria for trustworthiness and (2) Strauss and Corbin (1998) and Corbin and Strauss (2008) evaluative criteria for the empirical grounding and the research process.

Trustworthiness in this interpretive study is ensured by attending to four criteria (Lincoln & Guba, 1985): credibility (equivalent to internal validity), transferability (equivalent to external validity), dependability (equivalent to reliability), and confirmability (equivalent of objectivity). Several steps were employed throughout the research to guarantee that the above criteria are met.

To address credibility, the study used multiple methods and sources to ensure triangulation of the findings, such as single interviews, group interviews across different sources (e.g., hospitals, government, consultants and IT designers). Triangulation was also achieved by supplementing workshops, round tables, and documentation. Moreover, the researcher had several years of industry experience in healthcare IT, in addition to being an active member of a healthcare research center and a national healthcare professional association (e.g., involved in several conferences with sessions on privacy and security).

To ensure transferability, the study provided a detailed first-order analysis of the phenomenon and context which is supposed to provide enough background for the readers to judge the plausibility of the findings and their applicability beyond the bound of this project (Van Maanen 1979).
Dependability and confirmability were achieved as follows. First, rather than conducting an inter-rater reliability, an inquiry audit was conducted. This is because interpretive research assumes each researcher will have a unique interpretation of the findings, therefore inter-rater reliability cannot be applied (Lincoln & Guba, 1985). An inquiry audit was performed by one professor of organizational behavior (committee member) and a senior graduate student (trained in qualitative research) to examine and assess the process of inquiry and review the interview transcripts, coding sheets, and data analysis. Second, to measure how the findings are supported by the data collected; the study was shared with professors, two graduate students, and two healthcare professionals, in order to get critical feedback. Consensus suggests that this research analysis and theoretical model accurately reflect the data.

An evaluation of the empirical grounding component of the study is accomplished using Strauss and Corbin’s eight criteria is represented in the following table.
### Table 5-2 Empirical Grounding of the Study

<table>
<thead>
<tr>
<th>Evaluative Criteria</th>
<th>Description</th>
<th>Goal</th>
<th>What to look for in this study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion 1</td>
<td>Are concepts generated?</td>
<td>Assess if the concepts used in the research are grounded in the data.</td>
<td>The concepts used in the research are grounded in the data. Therefore, the study could be viewed as fitting with the first criterion.</td>
</tr>
<tr>
<td>Criterion 2</td>
<td>Are the concepts systematically related?</td>
<td>Check if there is a linkage between concepts.</td>
<td>The study shows how the concepts have been interwoven into more coherent themes and categories.</td>
</tr>
<tr>
<td>Criterion 3</td>
<td>Are there many conceptual linkages and are the categories well developed? Do they have conceptual density?</td>
<td>Check if categories and subcategories are tightly linked.</td>
<td>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.</td>
</tr>
<tr>
<td>Criterion 4</td>
<td>Is much variation built into the theory?</td>
<td>Check for variations in the theoretical model and different conditions and consequences.</td>
<td>This research presents a hybrid of process and variance in the theoretical framework (Figure 5-2) that aims to depict the interrelations of categories influencing the process of responding to privacy threats. The variance component derives from the organizational strategy (proactive or reactive) and leadership buy-ins/lack of commitment, which occurs during the process of organizational privacy responses.</td>
</tr>
<tr>
<td>Criterion 5</td>
<td>Are the broader conditions that affect the study built into its explanation?</td>
<td>Incorporate the micro and macro conditions.</td>
<td>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.</td>
</tr>
<tr>
<td>Criterion</td>
<td>Question</td>
<td>Check Criteria</td>
<td>Conditions.</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Criterion 6</td>
<td>Has process been taken into account?</td>
<td>Check if process has been considered.</td>
<td>This study focuses on understanding how organizations respond to privacy threats. This translates into the processes undertaken to handle these threats. Therefore, the criterion of identifying process in research has been achieved.</td>
</tr>
<tr>
<td>Criterion 7</td>
<td>Do the theoretical findings seem significant and to what extent?</td>
<td>Check for imagination and insights.</td>
<td>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.</td>
</tr>
<tr>
<td>Criterion 8</td>
<td>Does the theory stand the test of time and become part of the discussions and ideas exchanged among relevant social and professional groups?</td>
<td>Check if the theoretical framework is able to withstand future testing and research.</td>
<td>Given that this study has been developed based on a specific context, it is my hope that the insights of the emerging theory can make it withstand future applications and research.</td>
</tr>
</tbody>
</table>

An evaluation of the grounded theory research process is completed using Strauss and Corbin’s (1998) and Corbin and Strauss’s (2008) seven criteria for judging a grounded theory research process. Table 5-3 presents a summary of where these criteria have been reflected in this study.
### Table 5-3 Research Process Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluative Criteria</th>
<th>Description</th>
<th>What to look for in this study</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 1</strong></td>
<td>How was the original sample selected? On what grounds?</td>
<td>Interviewing informants has been initiated in the hospitals. However, after initial data analysis, this target was revisited to include other healthcare organizations and entities (e.g., the U.S. Department of Health and Human Services, healthcare professional associations, healthcare IT providers, and healthcare privacy consultants). This sample was originally based on privacy leaders only in hospitals and ultimately included privacy leaders from other healthcare-organizations who impact the process by which hospitals respond to information privacy threats.</td>
</tr>
<tr>
<td><strong>Criterion 2</strong></td>
<td>What major categories emerged?</td>
<td>The study led to the emergence of major categories – Privacy Threats, Drivers, Privacy Safeguards, Privacy Risk Assessment, Imbalance Challenge, Privacy Compliance, and Leadership Commitment.</td>
</tr>
<tr>
<td><strong>Criterion 3</strong></td>
<td>What were some of the events, incidents, or actions (indicators) that pointed to some of these categories?</td>
<td>Categories emerged as a result of first and second order analysis.</td>
</tr>
<tr>
<td><strong>Criterion 4</strong></td>
<td>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?</td>
<td>Theoretical sampling was driven by the concepts that emerged. The categories of privacy risk assessment, hospitals’ size and the Imbalance Challenge created a need to collect further data. Ultimately, some categories sustained (e.g., the PIA and the Imbalance Challenge) and others did not hold up (e.g., hospital size).</td>
</tr>
<tr>
<td>Criterion 5</td>
<td>What were some of the hypotheses pertaining to conceptual relations (i.e., among categories), and on what grounds were they formulated and validated?</td>
<td>As a qualitative researcher, I came up with hypotheses in their initial form in early analysis. These hypotheses were formulated and based on the interpretations of the data collected. Examples of these hypotheses include proactive type organizations who exhibited very distinct behaviors regarding their approaches to responding to privacy threats, while reactive type organizations’ behaviors were opposite to the ones described above.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Criterion 6</td>
<td>Were there instances in which hypotheses did not explain what was happening in the data? How were these discrepancies accounted for? Were hypotheses modified?</td>
<td>As the coding continued, I improved categories and themes. Some did not hold up. For instance, at early stages of data analysis, I formulated the hypothesis that larger hospitals with more resources would thrive to achieve higher degree of privacy compliance and better address the imbalance issues. I further analyzed this pattern to discover that, while the hospital size matters because it is often closely linked with resources, it is the commitment of top managers that prevails. This hypothesis eventually was modified to account for the role of leadership commitment.</td>
</tr>
<tr>
<td>Criterion 7</td>
<td>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?</td>
<td>The PIA and the Imbalance Challenge gradually emerged as the core themes of this study. While the PIA emerged first, the Imbalance Challenge theme emerged as further analysis of the PIA and theoretical sampling was undertaken. The final analytics decisions were made and validated with the empirical data.</td>
</tr>
</tbody>
</table>
In summary, from the analysis of the data collected, two core themes emerged that contribute to the theoretical model. The interaction between those themes, privacy risk assessment and the Imbalance Challenge, was moderated by strategic types of healthcare organizations as well as the leadership commitment. Contrasting the core themes with relevant literature on risk management, the theory of balance, and different organizational strategic types contributed to understanding the critical importance of embracing privacy risk assessment in different healthcare environments. As a result, this study offers well-supported answers to all the research questions presented in Chapter 1.
Chapter 6

Conclusion

This interdisciplinary study of IS, Health informatics, and organizational behavior started with a broad question—*How do healthcare organizations respond to information privacy threats?*—and concluded with a theoretical framework that explains the processes by which organizations respond. This chapter concludes this study by presenting a summary of this research, revisiting the research questions, and discussing the key contributions, implications, and limitations for both theory and practice. Finally, suggestions for future research opportunities are provided.

6.1 Summary of the Study

The purpose of this dissertation was to develop a theoretical framework based on the grounded data and the researcher’s understanding of the opinions and attitudes of healthcare privacy leaders. This study capitalizes on a great interdisciplinary research opportunity provided by prior studies in IS, health informatics, and organizational behavior on the topic of information privacy.

The IS literature points to a lack of theories explaining how organizations respond to privacy threats and calls for qualitative research to further explore this area. Moreover, recent literature reviews on privacy call for further studies at the organizational level (Belanger et al., 2011; Pavlou 2011; Smith et al., 2011). The health informatics literature focuses on technology-driven privacy safeguards and the dynamics of the healthcare
environment; furthermore, it presents the issues of balance challenges between implementing privacy safeguards and protecting patient information (Buckovich et al., 1999; Coiera et al., 2004; Weber et al., 2012). The organizational behavior literature reveals that organizational contexts and organizational strategies are significant in the explanation of organizational behaviors (Miles et al., 1978; Oliver 1991).

The need for generating a new theory rises when significant gaps in the literature are considered together. A grounded theory methodology is adopted that accounts for and uncovers organizational activities and behaviors with regard to healthcare information (Strauss et al., 2008). Grounded theory approach is becoming increasingly common in the IS research literature because the method is extremely useful in developing context-based descriptions and explanations of the phenomenon (Orlikowski 1993). This methodology also enables one to “produce theoretical accounts which are understandable to those in the area studied and which are useful in giving them a superior understanding of the nature of their own situation” (Turner 1983, p. 348).

Chapter 4 presented the research findings and introduced major emerging themes. Two core themes, the Privacy Impact Assessment (PIA) and the Imbalance Challenge are further discussed in Chapter 5 and led to the shaping of the theoretical framework of the organizational responses to privacy threats. This theoretical framework is compared with existing literature and evaluated against major interpretive judgment criteria (Strauss et al., 1998; Corbin et al., 2008).
6.2 Revisiting the Research Questions

The research has met its objective, which was to create a theoretical foundation for guiding healthcare organizations through responding to information privacy threats. The first research question asked, “Why do healthcare organizations respond to information privacy threats?” In response, the study:

- Defined a taxonomy of threats faced by healthcare organizations. Indeed, the study identified four major threats that healthcare organizations and hospitals in particular, have to deal with: (1) unauthorized access, (2) unintended data disclosures, (3) lost hardware, and (4) misuse of ubiquitous technologies such as mobile devices, wireless technologies, and the use of social media. Figure (4-3) in Chapter 4 provides a visual representation of this taxonomy.

- Developed a taxonomy of drivers. In this study, four major drivers emerged as influential factors affecting organizational responses to privacy threats. In the findings section, detailed descriptions were provided for (1) regulatory pressures; (2) financial, human, and technical resources; (3) competitive advantage via reputation and image; and (4) ethical considerations through the best practices. This study further links these drivers with the organizations’ strategic approaches (proactive or reactive) by identifying them as facilitating or inhibiting drivers. While facilitating drivers act as a catalyst into undertaking a thorough assessment of threats, capabilities, and shortcomings, inhibiting drivers act as a barrier to undertaking effective privacy solutions.
The second research question pursued was, “What are the safeguards and mechanisms used by healthcare organizations to mitigate information privacy threats with two sub-questions: “What are the different types of safeguards implemented?” and “What are the mechanisms undertaken to apply the appropriate safeguards?” Healthcare organizations implement a variety of safeguards to mitigate the impact of the privacy threats with which they are faced. Figure 5-3 illustrates the four types of privacy safeguards: (1) technical safeguards, (2) human safeguards, (3) physical safeguards and (4) administrative processes.

The study findings provide evidence that the issues surrounding the mechanisms of selecting and implementing the appropriate privacy safeguards and their impact (last research question) were of high priority to healthcare privacy leaders. Understanding the dynamics between the threats, the drivers, and the operational impacts appeared to be critical to understanding the processes by which organizations respond to privacy threats. Doing so allows organizations to assess these elements and respond appropriately. The findings from this qualitative study indicate that the process by which organizations respond to information privacy threats, named the Privacy Impact Assessment (PIA), is central to responding effectively to information privacy threats. Based on the findings and analysis of this study, the PIA involves protecting patient health information by implementing organizational safeguards that (1) account for the dynamics of different factors influencing how organizations respond to information privacy issues and (2) assess the implications of such responses.
This definition of the PIA emerged from the data analysis of informants’ integration of assessment processes for more informed decisions about information privacy safeguards. In this study, the concept of the PIA is considered to be both simple and profound. Assessing each driver (institutional, resources, competitive advantage, and the best practices) while simultaneously accounting for the dynamics of how complying with one driver may impact another driver or outcome, constitutes a strong conceptual foundation for organizational privacy responses.

The third research question in this study was, “How does the implementation of privacy safeguards impact healthcare workflow and processes?” with three sub questions: “What are the intended consequences (positive impacts) of privacy safeguards?” “What are the unintended consequences (negative impacts) of privacy safeguards?” and “What are the implications of these opposing impacts on privacy compliance?” The data revealed that the implementations of information privacy protective safeguards is impacting healthcare work practices through positive and negative impacts and thus creates the Imbalance Challenge. Achieving a balance in privacy and utility by maximally reducing negative impacts was challenging because of the dynamic environment surrounding healthcare delivery. The dynamics inherent in medical practices such as scheduled and unscheduled patient visits, clinicians’ unscheduled shifts, and workforce needed at unexpected times and locations, often conflicted with privacy role-based access safeguards (Boxwala et al., 2011) and therefore made the Imbalance Challenge even more important. The positive impact of privacy protective safeguards may function as a facilitator to privacy compliance while negative
impact as inhibitors. Identifying these impacts is not enough. Healthcare leaders must also address the Imbalance Challenge that ultimately defines the level of their privacy compliance. Top management support emerged as an essential element impacting the privacy compliance. As a result, there seems to be a significant positive correlation between having the appropriate management support in handling the Imbalance Challenge and privacy compliance.

The Imbalance Challenge allows organization leaders to understand that the implementation of privacy safeguards does not necessarily lead to positive impacts and that it is important to account for negative impacts and act accordingly in order to prevent undesirable shortcomings in their privacy compliance.

In summary, the emerging theoretical framework was able to answer the research questions formulated in this thesis (Chapter 1). Moreover, it points to several future research projects covered in the future research section (6.6).

6.3 Contributions and Implications for Research

This study aims to contribute to existing privacy research in several ways. First, the primary contribution is to respond to the compelling call for research investigating information privacy at the organizational level of analysis. This research provides new theoretical insights in understanding privacy management through a grounded theory approach. In the IS field, Smith et al. (2011, p. 1006) have made an explicit call for research on studying information privacy at the organization level:
“Indeed, most rigorous studies of organizational privacy policies and practices would likely include a set of exhaustive interviews with an organization’s members and stakeholders, and some amount of deep process tracing would also likely be involved. Such studies are the best approach to uncovering the somewhat subtle organizational dynamics that drive privacy policies and practices.”

This research responds to a theoretical challenge and introduces a theoretical framework of organizational responses to privacy threats. The concept of the PIA emerged as a proactive solution to handle the privacy threats. The PIA allows organizations to simultaneously assess privacy risks and the implications of information privacy safeguard enactments. As a result, organizations will be able to better assess the threats and the impact on workflow, and ultimately will be able to achieve better compliance without impeding healthcare practices.

Second, this research provides new theoretical insights by investigating the consequences of enacting privacy safeguards (Belanger & Crossler, 2011). To date, most studies on privacy focus on designing and implementing the appropriate safeguards to mitigate information privacy threats, and there has been a notable lack of research on the outcomes of privacy safeguards enactments. The emerging theoretical framework highlights the importance of the analytical construct I developed—the Imbalance Challenge—to capture the unintended consequences caused by the situation where the negative impacts of privacy safeguards outweigh the positive ones. Analyzing these opposing impacts is important because it enables us to assess and account for their implications for work practices and for privacy compliance.
Third, methodologically, using a grounded theory provides a rich lens through which to understand the consequences of privacy safeguards enactments and their implications on privacy compliance. Grounded theory methodology was selected because of the lack of existing theories to explain how organizations understand the implications of privacy safeguard enactments, the contextualization of the healthcare domain, practical relevance, and suitability to study healthcare processes. Based on a grounded theory study spanning over 16 months in which I was able to interview thirty privacy leaders from several healthcare organizations including the government, the study uncovered subtle organizational dynamics that would not have emerged through quick data collection techniques such as online surveys. The ability to revisit the interview questions and the target population to include more pertinent questions and participants was crucial to reaching saturation where all concepts were well defined and no new concepts emerged (Corbin & Strauss, 2008).

Fourth, this interdisciplinary study has contributed to the recent needs of cross-pollination of insights and perspectives to advance knowledge. This contribution converges the research streams of IS and health informatics. Based on this study, more interdisciplinary research opportunities in IS, organizational behavior, and health informatics can be achieved through systematic studies of concepts discovered in this study.

It is important to consider what the proposed theoretical framework has to offer to the academic disciplines of IS and health informatics, as well as to healthcare
practitioners. The theoretical framework of organizational responses to information privacy threats has significant implications that expand to other fields of research:

- Risk Management. This research presents significant issues of privacy relating to the Imbalance Challenge that are important to research on risk management. Risk assessment and management account for the potential negative impact of threats, but neglect to account for the implications of privacy safeguards enactments. Future research could leverage this concept to support the continuous development of Risk Management literature.

- Health Informatics. This study is a response to the lack of theory in health informatics literature. Proposing a theory that is in complete synergy with practice can further support future research by extending and testing the emerging concepts.

- Organizational Behavior. Based on this study, organizational behavior researchers could pursue research opportunities to expand upon the behavioral patterns of healthcare organizations in light of the Imbalance Challenge. This could be accomplished by a detailed and controlled research based on concepts that emerged in this study.

6.4 Contributions and Implications for Practice

The findings of this study have significant contributions and useful practical implications for healthcare organizations in general and hospitals in particular.
The study provides an analysis of how healthcare organizations respond to information privacy threats that goes beyond security risk management to include assessing the negative impacts of privacy safeguards. Such an analysis is accomplished by identifying and explaining the different categories and their relationships, thereby producing a framework that is parsimonious and practical.

The emergence of the Imbalance Challenge provides a clearer understanding of the unintended consequences of privacy safeguard enactments and their implications for the organization’s overall privacy compliance.

The study provides an analysis and a taxonomy of information privacy threats faced by healthcare organizations. This taxonomy goes beyond general threats to include specific issues related to the healthcare industry, such as the use of social media and the use of ubiquitous technologies by clinicians and business associates.

The theoretical framework of the organizational responses to information privacy threats generated in this study represents why, how, and what healthcare leaders strive to accomplish in response to information privacy threats. An appropriate practical implication for this research would be to seek how they could implement the PIA. Indeed, this study seeks to relate research and practice “by producing relevant theories that can advance the academic knowledge and, at the same time, can be applied in practice” (Fernandez et al., 2002, p. 111). This study demonstrated the need for conducting a PIA for a successful mitigation of privacy threats. Future studies can achieve this synergy by developing specific guidelines that can be put forward with step-by-step instructions for
how to conduct a PIA in healthcare settings given the categories identified in this research.

6.5 Limitations

In this study, limitations related to the literature, data collection, data analysis, generalizability, and internal validity must be considered. This section lists the limitations of this study, both real and potential.

With regard to the literature, this study investigated information privacy from a vast amount of relevant literature from different disciplines: IS, organizational behavior, and health informatics. It cannot be claimed that the literature review is exhaustive. Moreover, because of the inductive nature of this study, the literature review was conducted throughout the course of research and was driven by the emerging theoretical framework.

With regard to data collection through interviews, there was a possibility of interviewer’s bias. Walsham (1995, p. 77) distinguishes between the “outside observer” and the “involved observer.” My role in this study can be described as that of an outside observer. Consequently, potentially relevant knowledge might have been not captured. However, my industry experience in a hospital environment coupled with my involvement with a healthcare professional association (HIMSS) and a center for integrated healthcare delivery systems (CIHDS) alleviated some of these potential limitations.
With regard to validity of the emerging theory, it is worth referring to
generalizability, which is “the validity of a theory in a setting different from the one
where it was empirically tested and confirmed” (Lee et al., 2003, p. 221). Lee and
Baskeville (2003) clarified that the appropriate type of generalizability (not just
statistical) should be applied to the particular study. The purpose of this study was not to
achieve statistical validation but rather to discover patterns for the purpose of theory
building and gaining a better understanding of the main issues in its context. For the
theory building type of studies, Strauss and Corbin (1998) define assessing the
explanatory power as being more appropriate than its generalizability. Strategies and
criteria in checking the explanatory power are presented in section 5.4. Therefore,
generalizability is not a limitation in this study.

The issue of internal validity could be a limitation since this study was conducted
by a single researcher. Yet, it is hardly a major concern because the study used grounded
theory inductive methodology to develop the theoretical model, so it is more likely to be
internally valid (Eisenhardt 1989a). Moreover, this potential limitation is allayed by using
different sources, conducting single and group interviews, member checkings, and
seeking advisors’ and committee members’ feedback throughout the process.

6.6 Future Research

This study provides opportunities for future research. First, this study was
conducted with the objective of creating a theoretical foundation for guiding healthcare
organizations in their privacy responses. The proposed theory explains how healthcare
organizations respond to privacy threats under certain circumstances in certain areas (Strauss et al., 1998; Strauss et al., 2008). Hence, there is an opportunity to further engage with the existing theoretical framework and extend it to other domains. During the course of this study, other areas emerged as under-researched:

- The study helped to identify the factors that impact the Imbalance Challenge at the organizational level. Hence, there is an opportunity to research this imbalance impact from an individual level of analysis. Indeed, employees have different stakes in the organization based on their employment status (full-time/part-time, contract/permanent, staff/management) that could impact how receptive they are to privacy safeguards (D'Arcy et al., 2011).

- The findings show that hospitals, based on their top management commitment, take different attitudes toward the Imbalance Challenge. Therefore, another opportunity for research is to further examine the correlations among resources and leadership style with negative impacts. Doing so could facilitate the development of programs supported by executives to effectively act on the Imbalance Challenge.

- The findings are based on US hospitals. IS researchers have demonstrated that there are differences in information privacy issues across countries and cultures (Bellman et al., 2004; Milberg et al., 2000). Therefore, a third opportunity for future research is a comparative study of the factors impacting this imbalance while taking the cultural influences into consideration.
The emerging theoretical model was able to answer the research questions by explaining and predicting. Moreover, the theory can be translated into a more practical methodology for defining the guidelines and constructing PIA frameworks that are more efficient and effective.
References


Bulgurcu, B., Cavusoglu, H., and Benbasat, I. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security


Culnan, M.J. ""How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* 1993, pp 341-363.


DHS "Privacy Office- Privacy Impact Assessments (PIA).


Gritzalis, S., Lambrinoudakis, C., Lekkas, D., and Deftereos, S. "Technical Guidelines for Enhancing Privacy and Data Protection in Modern Electronic Medical


IOM, I.o.M.s.C.R. "The Computerbased Patient Record: An Essential Technology for HealthCare."


Lewin, K. "Field Theory in Social Science: Selected Theoretical Papers (Edited by Dorwin Cartwright.),") 1951.


Appendix A

Semi–Structured Interview Protocol for Information Privacy Experts

The purpose of this study is to gain a better understanding of the influencing factors and the appropriate measures used by healthcare organizations as a response to privacy issues.

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

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

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

4. Privacy Implementation Issues/ Practices/Enactment
   a. How is privacy practiced? Is it different from one setting (clinical) to others?
   b. What type of business conflicts (workflow conflicts) does your organization face in developing and enacting these privacy programs?
   c. What do you do when there is a conflict between your medical clinical workflow and mandates from regulations?
   d. How does your organization balance between its day-to-day operations and privacy policies’ implementation?
   e. How does training and education align with routing activities? Does it support actual practices or is it informational (awareness)?
   f. Are you a part of any HIMSS or CHIME chapters? Do you ever use your associations with these chapters to raise privacy mandates that are in conflict with your workflow processes? Has it ever been lobbied?
   g. Under what scenario, would an organization not comply with regulations?
   h. How do you balance privacy with convenience (for employees and for patients)

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

6. Concluding Questions
   a. Are there other issues related to privacy programs that we haven’t discussed but that would be important for me to know?
Appendix B

Illustrative Supporting Data for Privacy Threats

<table>
<thead>
<tr>
<th>2nd Order Themes</th>
<th>Illustrative 1st Order Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Access</td>
<td>“The biggest single problem is not the 14-year old hacker who is going to try to break into a hospital system, but someone who has legitimate access to the system but not for the use that they are using it for.”</td>
</tr>
<tr>
<td></td>
<td>“The fact of the matter is a lot of difficulties go back to this idea of access.”</td>
</tr>
<tr>
<td></td>
<td>“There are a lot of high profile patients that come through this facility and we have to be on guard; because of those high profile patients we don’t have employees that are curious about medical records and things alike, so we audit some high profile records.”</td>
</tr>
<tr>
<td></td>
<td>“It was about two years ago George Clooney was in a car accident and taken to a local hospital. And before you knew it, 20 people had access to his records. Is George Clooney really here in our hospital? Let me see.. And they think nobody is checking on them.”</td>
</tr>
<tr>
<td></td>
<td>“We’ve had situations where people have looked up other people’s records and they shouldn’t have.”</td>
</tr>
<tr>
<td></td>
<td>“We have to make sure they are only accessing what is appropriate for whatever they need to provide care for that patient and not going and looking at other patients medical records.”</td>
</tr>
<tr>
<td>Data Disclosure &amp; Secondary Use</td>
<td>“There are many times when a clerical person will hit the wrong number on the fax machine and fax a lab result for Ms. Jones to a Sheetz store. That happens all the time.”</td>
</tr>
<tr>
<td></td>
<td>“If another hospital requests our record from us through an exchange, we have to assume that the hospital needs that information, and they are entitled to that information, that they are caring for a patient for whom information relates.”</td>
</tr>
<tr>
<td></td>
<td>“The area where I’m most uncomfortable with is the third parties that have to handle our data because they are a business associate that provide service to us.”</td>
</tr>
</tbody>
</table>
"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."

"How do you secure information that is being used for secondary purposes for research, for research, for quality, for billing and coding"

<table>
<thead>
<tr>
<th>Lost &amp; Stolen Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Reasons reported for the breaches = loss 34%&quot;</td>
</tr>
<tr>
<td>&quot;There is vulnerability that if you put the device out, with a person, which means they can lose them, they can be stolen, they can be just and not making good decisions with them.&quot;</td>
</tr>
<tr>
<td>&quot;We don’t have a hundred percent security, you can have somebody who has records on a laptop that gets lost at Panera. It is going to happen.&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ubiquitous Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Everybody has a cell phone now or a Droid or a smart phone. It’s really hard, from an information security and privacy standpoint, how much do you let employees use them, especially with the video and picture taking abilities. We have policies on taking pictures and videos, but it’s very hard to control when everybody’s got a video camera in their pocket.&quot;</td>
</tr>
</tbody>
</table>
| "There’s a big movement under foot now in the industry to set up public clouds and host private clouds for organizations to use and to share their data. In other words, move it from localized data centers that are costly to build and maintain, shift that to kind of privatized businesses in the cloud that are available through the Internet. So there’s a lot of that taking place and it’s great for some business models, I think, healthcare is going to have to work to find its place. It’s going to require a lot of controls to be put into place to give us an assurance that the information is as protected as we want it to be."
| "How we get in trouble on Facebook and how a lot of guys get in trouble. A lot of the marketing teams like using that now for marketing. So people get in there and say some..." |
good things without asking. I had this great experience. But then you could also say bad things about our hospital and say bad things about manager or certain things going on. That’s when our privacy comes in. So we could get that stuff taken down. We have to have controls. And who’s going to monitor and filter every time somebody says something about an individual?
## Appendix C

**Illustrative Supporting Data for Drivers of Privacy Safeguards**

<table>
<thead>
<tr>
<th>2nd Order Themes</th>
<th>Illustrative 1st Order Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Institutional Pressures</strong></td>
<td>“I think a lot of it is still regulatory. I would say more often than not, our decisions are often forced. We are forced to say what does regulation allows us to do.”&lt;br&gt;“We follow the state guidelines and, and make sure that we deal with everything so it, we don’t get sanctioned because part of the thing is protecting ourselves so that we don’t get sued or don’t get fined.”&lt;br&gt;“There are various state laws that also guarantee patient privacy and so, you have to, you follow whichever law is more restrictive and stringent, whether is the federal, or the state. Basically I think most of the HIPAA laws are probably the most restrictive at this point that offer the most privacy to the patients.”&lt;br&gt;“Privacy will always win this because of the fine associated, the loss of reputation associated.”&lt;br&gt;“It’s well reputational damage if there is a lack of privacy. If they are not treating individuals’ information with the respect, not safeguarding individual health information, then of course the repercussions from that can be really damaging. And the first thing is the reputational damage. Who wants to go to a hospital that’s been in the news four times for having lost patient information or put it in the dumpster without bothering to eradicate any types of shreds of evidence as to who it belonged to.”</td>
</tr>
</tbody>
</table>
| **Resources**              | “You got to constantly be on top of that. Financial resources could limit that and, like I said, my human resources do limit my ability to get to where we could be right now “<br>“We don’t have the financial resources to pay for consultants to come in”<br>“We don’t have the resources to do all those things.”<br>“Those things cost a lot of money. If I have to protect it
with virtualization but I have a chance of buying this real fancy clinical application that’s going to help me, which do you think I’m going to do? I’m going to buy that real fancy clinical application. Then I’ll think about security last on it due to funding. “

“It’s up to you to figure out how to comply so a lot of things could be based upon money as in resources and people, the ability to install it and support it.”

“From process based to time spent developing but it’s also and again back to capital and resources. It’s a huge commitment.”

“Major problem for me now is that you install a lot of safeguards and technical solutions and having the ability to continue to support them you just don’t put them in and walk away. it becomes an ongoing resource issue or an ongoing expense issue.”

<table>
<thead>
<tr>
<th>Competitive Advantage</th>
</tr>
</thead>
</table>
| “I think no one wants to be the poster child, no healthcare organization wants to be the one that makes New York Times today. Back to that trust when, where I said we’re very similar to financial institutions because you want to maintain that trust with your consumer, whoever your consumer is. If your consumer is a patient, you’ve got to have that trust or you lose your brand, you lose your reputation.”

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

‘I think in the privacy officer’s function, we would always recommend what we see as what’s legally required, what does the individual consumer want and expect, and what’s the ethical thing to do? And we would look at those things and make that recommendation, here's what we think “

if you don’t see to your patient information, patients don’t want to go there.

“Our senior management really understands the issues. They want to protect [our hospital] brand and they understand that protecting privacy and implementing security are the two components that will you know help the
most in that situation in keeping those two front and center.

“We need to get the information out, we need to get it in people’s hands and there’s a lot of trust there that’s traditionally been put on our workforce’s hands and their responsibility is to keep it secure.”

“Even if the regulations were not there, it may be a little more lacks because you wouldn’t have nothing to refer back to, but … you have to have best practicing and you have to have good practices.”

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

“I would say that when the HIPAA privacy rule came out, because it was a mandate organizations did comply because they knew they needed to. However, I don’t think that’s the only thing, because most organizations that I’ve come in contact with either because I’ve worked there or I know their privacy officers or whatever, they do compliance because it’s a good thing to do.”

“I do think that there are a number of motivating factors for confine. 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.”

“we are going to put together what we think are reasonable, fair information practices.”

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

Illustrative Supporting Data for Privacy Safeguards

<table>
<thead>
<tr>
<th>2nd Order Themes</th>
<th>Illustrative 1st Order Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Controls</td>
<td>“We are working through role based security, and we are not there yet. So we are identifying every position within the hospital, and we are identifying what they [employees] should have access to.”</td>
</tr>
<tr>
<td></td>
<td>“There are lots of tools that we can use to help us create these access levels and what not. And we are implementing them, one by one, but it’s really complicated”</td>
</tr>
<tr>
<td></td>
<td>“The electronic security of it is a whole another ball game in regards to firewalls and remote access to the information, redundancy of that information, who has the sign in security to see pieces of information.”</td>
</tr>
<tr>
<td></td>
<td>“We have all our laptops encrypted. We have all kinds of rules around PDAs’.”</td>
</tr>
<tr>
<td></td>
<td>&quot;You can’t necessarily prevent somebody from breaking into your office and stealing your stuff. But if you have encrypted it, you can prevent him from using it and accessing it.”</td>
</tr>
<tr>
<td></td>
<td>“We track everything that gets looked at. So if I am logged on and I look at your record, that’s tracked in every application. So we do that now if you were to come back in two years, and say, I think my next door neighbor looked at my records while I was in the hospital, we would probably be able to find that transaction.”</td>
</tr>
<tr>
<td></td>
<td>“We are not just 8 hours a day, 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.”</td>
</tr>
</tbody>
</table>
**Human controls**

“We also educate the staff about HIPAA, orientations plus ongoing annual training regarding HIPAA laws and HIPAA issues and how extremely important it is for patients’ right to privacy.”

“We have what we call education-on-the-go and on an annual basis. We all log on to our computers, and we read the education material and then we answer some questions to make sure that we understand that education and then we track that information. So all these people are educated. The information is really basic information.”

“HIPAA requires us to train our workforce on policies and procedures associated with the privacy. We are supposed to retrain our work force if those policies change, that’s all HIPAA says. So the question really is, how often do you train people. We have trained on a number of occasions since HIPAA became effective.”

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

“There are other lesser forms of discipline and we have also taken further steps to limit access in various ways. We go through and periodically look whether an employee or a nurse working in one unit does not have access to patients in another unit. We have taken those additional steps to do things like that.”

“We have a progressive discipline policy based both upon whether somebody has done something the first time, or second time, but it’s also based on severity.”

“We actually have people that are hired to oversee those things in the institutions, patient privacy officers, so there are people who live and breathe this every day.”
| Physical Controls | “You have to worry about physical. We do have a data center today, you remember you walked through it. It looks like a real mess, it’s really full with equipment and I have an offsite data center also. That’s in a bunker hidden, and protected and very few people know where it’s at and seriously that’s true.”  
“We do rounding to look at the place in the computers to see if a screen is visible. We have put in nurse stations, one-way glass in certain areas so the public cannot walk by and look in and see a computer.”  
“There is badge access everywhere, it is recorded in this thing that tells me who I am. They are also have a proxy card inside that tells me that I am in the indoors or outdoors and records it.”  
“Work stations are set up appropriately to protect privacy. Are patient carriers protected enough? Are there areas for folks to be able to go and have a private conversation with a provider?”  
“Well, we have security on the data center. I mean, you don’t get in the data center unless you know certain codes and stuff like that.”  
“We look at physical barriers that we could put in.”  
“We make sure they [patients’ charts] not visible to anyone, make sure they’re covered, they’re turned upside down “  
“We try to take as many safeguards within our own department. We are also a secure department and we use keypad access” |
| Administrative Processes | “We have a lot of policies on security and privacy. And that goes in line with again government regulations too. If the regulations have a lot of policies, you have to put policies and procedures you in place. You may find healthcare workers as very policy oriented. They really truly are.”  
“Privacy of health information is a priority and we have policies and procedures and infrastructure that support that approach to patient information.”  
“When we developed our security policies especially our
internet policy people really struggled and spent a lot of time cause we wanted to make it reasonable.”

“We have revised our confidentiality statement to make it more detailed and to address Facebook and social networking. So we added a lot to the confidentiality statement that all employees, students, physicians, all the work, workforce have to sign.”

“We have different policies depending upon what your relationship is with [our hospital]. Not necessarily who you are, don’t get me wrong. If a physician looks at something inappropriate, we will discipline the physician the same we will discipline a nurse or a dietitian.”

“We have policies, training and education and some sort of procedures that we put in place. What drives into having these measures in place? You don’t want to mess with [the regulations].”
### Appendix E

**Illustrative Supporting Data for Imbalance Impacts**

<table>
<thead>
<tr>
<th>2nd Order Themes</th>
<th>Illustrative 1st Order Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative Impact (Information Unavailability)</td>
<td>“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.”</td>
</tr>
<tr>
<td></td>
<td>“One of the challenges with my area is when we try to secure the information but yet our healthcare providers need quick access to it. So there’s always kind of a fine line there. We try to make it as accessible as possible but yet have security measures in place to protect those assets.”</td>
</tr>
<tr>
<td></td>
<td>“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.”</td>
</tr>
<tr>
<td></td>
<td>“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”</td>
</tr>
<tr>
<td>Negative Impact (Workflow Disruption)</td>
<td>“if the security is too hard, people wouldn’t do it. If it is beyond their work flow much, they won’t do it. “</td>
</tr>
<tr>
<td></td>
<td>“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”</td>
</tr>
<tr>
<td></td>
<td>“Do you want me not to administer that medication because everything didn’t line up in the security behind the scenes?”</td>
</tr>
<tr>
<td></td>
<td>“Once I log in, I don’t want the system to log me out automatically. I don’t like it “</td>
</tr>
<tr>
<td></td>
<td>“Time out features. There’s times out in all our system end….”</td>
</tr>
</tbody>
</table>
this is something we have to work around. You know we have some key systems in the emergency department and what they’re saying … We have a twenty minute time out feature … if I’m a doctor in the emergency room and my system times out on me while I am critically working on a patient … I have to [enter] my password, that’s not a good thing.”

“I’m using application A, application B and you get all these passwords you got to remember. Guess what? I’m going to start writing them down.”

“40% of the work that a nurse does is to administer medication. 40% of her day, she is looking at pills and administering them. … she is logging in and waiting waiting waiting waiting that’s a problem she is not going to get her job done. It’s hard enough to do the charting, administering medicine without the waiting waiting waiting waiting, 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”

<table>
<thead>
<tr>
<th>Negative Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Usability Issues)</td>
</tr>
</tbody>
</table>

“It comes from EHR usability and access to information. I mean in certain scenarios, I would like to walk in from purely a clinician hat on, I like to walk into to room and see that patient’ information, talk with that patient and provide the care. but somehow I have to be acknowledge as being allowed to see that information. So, that one of the conflicts. I have to log in or else I have to use an RFID tag or swipe something to get into that record. “

“With the privacy and security in healthcare it’s the need for speed. I don’t want to log in twice. I don’t want to log in this, I don’t want to that.”

“If it is not usable to them, they won’t use it. and the things that are very usable to them, that they are used to, they can, I’ve seen this all the time “
Negative Impact
(Operational Feasibility)

“My biggest concern time again comes down to operational feasibility and weather what’s being asked is either can be operationalized or is it going to be detrimental to the patient best interest.”

“It really comes down to practice”

“There is a lot of indirect impact that you have to be careful of its operational efficiency you know you have to really look at, you will never get a number you look and say oh my God. It’s got to be costing us money or it’s got to be costing us efficiency.”

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

“Let’s just say for example, your brother is Don Parks and you are a physician, and you are looking up Don Parks records for no reason what so ever. An alert is triggered and will be sent to someone who actually sponsors your account. It is going to say Rachida Parks looked at Don Parks’ record. The person that sponsors you will need to get with you and say who is that? You might say that is my brother, and one might say, why did you look at that record? You would say he was not looking good at the family dinner last week, so I looked up his record, which will be totally inappropriate. Or you could say, Don parks is not related to me, but is a patient of mine. The alerting provokes the next level of inquiry. If you were to say the former where you were looking up at you brother’s record and you didn’t really have a reason to, then that gets referred to the human resources for discipline”

“We got to make sure the things are operationally supportable and I have to say that there are aspects of HIPAA that are very difficult to operationalize and they really often don’t have a lot of meaning either”.

“We have lots of policies and everybody else has lots of policies but we can’t meet the regulations in the strictest letter of the law and offer clinicians their ability to practice
in an efficient cost effective manner.”

“My biggest concern time again comes down to operational feasibility and weather what’s being asked is either can be operationalized or is it going to be detrimental to the patient best interest and there is balance, it really is”

<table>
<thead>
<tr>
<th>Positive Impact (Controlled Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“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.”</td>
</tr>
<tr>
<td>“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.”</td>
</tr>
<tr>
<td>“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.”</td>
</tr>
<tr>
<td>“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.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Positive Impact (Deterrence Effect)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“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 gonna happened. 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.”</td>
</tr>
</tbody>
</table>
| “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 coworkers, because I want your coworkers to say, I am not going to do this again because I don’t want to have the same thing happen to me, or I don’t want to be suspended.”

“We need to discipline them, we need to make sure that people understand that we take this seriously, and hopefully, there is a deterrent effect that occurs from other people seeing the fact that people have lost their jobs over. Now the fact that only three people in that hospital lost their jobs over it, probably it says to me only good thing, because it says to me only three people were dumb enough to look at the record.”

““We have alerts built in to things, there are alerts for certain people when there is a perceived attack or perceived breach so to speak…”

“We have software which goes through every PC in the house every day looking for things on PCs. so we have software in place on emails that look for certain patterns of information of people are trying to send out here it will block it.”

“our system is all doing very advanced logging, and if I decided that I wanted to see who looked at your record, I would know everybody who looked at your record”

“So anybody who goes in and looks at a record of same, the same last name that’s, that’s a flag. It doesn’t mean it’s inappropriate. It just means that we need to look at those a little bit closer.”

“A system behind the scenes looking at these audit models that are being generated continuously and let’s look for patterns or let’s look for, let’s look for trends or patterns that you know doesn’t appear to be right and they need to be investigated on.”
## Appendix F

### Illustrative Supporting Data for Organizational Context

<table>
<thead>
<tr>
<th>2nd Order Themes</th>
<th>Illustrative 1st Order Data</th>
</tr>
</thead>
</table>
| **Hospital Size** | “They [small hospitals] will be out of business and will not be compliant with HIPAA or HITECH, because they cannot afford to”  
“I have one (HIPAA officer) person to worry about 120 employees. If you had 12,000 employees, to get that same ratio you’d have to have 100 HIPAA officers.”  
“I’m thinking of Hospital X and you’ve been in that hospital probably. I mean there’s so many points of access there, so many people and so many work stations and so much happening and paper everywhere. It may be more of a challenge for them to adhere to the standards than here at this little hospital.”  
“I’d imagine in a big organization trying to control that is a daunting task so while we may not have the, the, the resources for the IT and the sophisticated systems and all that, from a HIPPA privacy standpoint we probably could do better than the big places.”  
“I think if you were a little hospital, you couldn’t afford all these utilities.” |
| **Academic Status** | “We have a large teaching hospital which is actually in the heart of Columbus, Ohio.”  
“[We are] medical school and a major research institution”  
“we have teaching hospitals” |
| **Educational Background** | “I have an undergraduate degree in computer science, and I also have a degree in history, and then I have my JD, jurist doctor, I am an attorney”  
“I have an associate’s degree in biomedical engineering and a bachelor’s degree in electronic engineering and a” |
“I have a medical degree”

“I went to medical school and became an internist. I became convinced that we will never be able to provide high quality efficient care without using computers effectively … so started to get interested at the end of my residency and became one way and another involved [the hospital] implementation of EHR “

“I have a diploma in professional nursing, a bachelor’s of business and finance and a Master’s in organizational development.”
Appendix G

Illustrative Supporting Data for PIA

<table>
<thead>
<tr>
<th>2nd Order Themes</th>
<th>Illustrative 1st Order Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment of Drivers and Impact</strong></td>
<td>“You have to do a risk assessment in each of the areas and apply the appropriate mitigation tools to prevent those things from happening.”</td>
</tr>
<tr>
<td></td>
<td>“I think ultimately a lot of this is done around risk too. And so you know that’s, that’s the unfortunate or fortunate, I’m not sure where that fits in, but there is no such thing as zero risk. But I think a lot of people expect that, but the truth is, everyone is constantly in the back of their minds measuring risk all the time. So I think that’s why you always do what the law says. That’s a risk that’s not worth taking. But then you have to look at other kinds of risks too for what you may do or may not do and, and what the risk of reputational harm or financial harm or all those other kinds of things, how that comes into play.”</td>
</tr>
<tr>
<td></td>
<td>“A lot of the regulations are rather large and some of it is not practical.”</td>
</tr>
<tr>
<td></td>
<td>“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.”</td>
</tr>
<tr>
<td></td>
<td>“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.”</td>
</tr>
<tr>
<td></td>
<td>“It’s a balance, you need to have role based access, but you’ve got to be careful about being too prescriptive in terms of limits. You have to err on the side of more access, understanding that people very well may you know, look at something that they shouldn’t be, but hopefully you catch it on the back end by log in and monitoring”</td>
</tr>
<tr>
<td></td>
<td>“The opposing concept is you have hospital operations trying to take care of patients and stuff like that but you have federal, federal regulations that try and make it as...”</td>
</tr>
</tbody>
</table>
difficult as they can to do that. And then the other issue you deal with is, is the discrepancy between the agencies as to what, what’s the level of security you should have.”

“My biggest concern time again comes down to operational feasibility and weather what’s being asked is either can be operationalized or is it going to be detrimental to the patient best interest and there is balance, it really is”

“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.”
# Appendix H

## List of State Breach Notification Laws

<table>
<thead>
<tr>
<th>State</th>
<th>State Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>(ALASKA STAT. § 45.48.010 et seq.)</td>
</tr>
<tr>
<td>Arizona</td>
<td>(ARIZ. REV. STAT. ANN. § 44-7501)</td>
</tr>
<tr>
<td>Arkansas</td>
<td>(ARK. CODE ANN. § 4-110-101 et seq.)</td>
</tr>
<tr>
<td>California</td>
<td>(CAL. CIV. CODE § 1798.82)</td>
</tr>
<tr>
<td>Colorado</td>
<td>(COLO. REV. STAT. § 6-1-716)</td>
</tr>
<tr>
<td>Connecticut</td>
<td>(CONN. GEN. STAT. § 36a-701b)</td>
</tr>
<tr>
<td>Delaware</td>
<td>(DEL. CODE ANN. tit. 6, § 12B-101)</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>(D.C. CODE § 28-3851)</td>
</tr>
<tr>
<td>Florida</td>
<td>(FLA. STAT. § 817.5681)</td>
</tr>
<tr>
<td>Georgia</td>
<td>(GA. CODE ANN. § 10-1-911)</td>
</tr>
<tr>
<td>Hawaii</td>
<td>(HAW. REV. STAT. §§ 487N-1 et seq.)</td>
</tr>
<tr>
<td>Idaho</td>
<td>(IDAHO CODE ANN. § 28-51-104 et seq.)</td>
</tr>
<tr>
<td>Illinois</td>
<td>(815 ILL. COMP. STAT. ANN. 530/5, /10)</td>
</tr>
<tr>
<td>Indiana</td>
<td>(IND. CODE § 24-4.9)</td>
</tr>
<tr>
<td>Iowa</td>
<td>(IOWA CODE § 715C.1 et seq.)</td>
</tr>
<tr>
<td>Kansas</td>
<td>(KAN. STAT. ANN. § 50-7a01-02)</td>
</tr>
<tr>
<td>Louisiana</td>
<td>(LA. REV. STAT. ANN. § 51:3071 et seq.)</td>
</tr>
<tr>
<td>State</td>
<td>Code</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maine</td>
<td>(ME. REV. STAT. ANN. tit. 10, §1346 et seq.)</td>
</tr>
<tr>
<td>Maryland</td>
<td>(MD. CODE ANN., COM. LAW § 14-3501 et seq.)</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>(MASS. GEN. LAWS ANN. ch. 93H, § 1 et seq.)</td>
</tr>
<tr>
<td>Michigan</td>
<td>(MICH. COMP. LAWS ANN. § 445.72)</td>
</tr>
<tr>
<td>Minnesota</td>
<td>(MINN. STAT. § 325E.61)</td>
</tr>
<tr>
<td>Mississippi</td>
<td>(MISS. CODE § 75-24-29)</td>
</tr>
<tr>
<td>Missouri</td>
<td>(MO. REV. STAT. § 407.1500)</td>
</tr>
<tr>
<td>Montana</td>
<td>(MONT. CODE ANN. § 30-14-1701 et seq.)</td>
</tr>
<tr>
<td>Nebraska</td>
<td>(NEB. REV. STAT. § 87-801 et seq.)</td>
</tr>
<tr>
<td>Nevada</td>
<td>(NEV. REV. STAT. 603A.010 et seq.)</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>(N.H. REV. STAT. ANN. § 359-C:19 et seq.)</td>
</tr>
<tr>
<td>New Jersey</td>
<td>(N.J. STAT. ANN. § 56:8-163)</td>
</tr>
<tr>
<td>New York</td>
<td>(N.Y. GEN. BUS. LAW § 899-aa)</td>
</tr>
<tr>
<td>North Carolina</td>
<td>(N.C. GEN. STAT. § 75-65; see also SB 1017)</td>
</tr>
<tr>
<td>North Dakota</td>
<td>(N.D. CENT. CODE § 51-30-01 et seq.)</td>
</tr>
<tr>
<td>Ohio</td>
<td>(OHIO REV. CODE ANN. § 1349.19)</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>(OKLA. STAT. § 74-3113.1)</td>
</tr>
<tr>
<td>Oregon</td>
<td>(OR. REV. STAT. § 646A.600 et seq.)</td>
</tr>
<tr>
<td>Oregon</td>
<td>(OR. REV. STAT. § 646A.600 et seq.)</td>
</tr>
<tr>
<td>Oregon</td>
<td>(OR. REV. STAT. § 646A.600 et seq.)</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>(73 PA. STAT. § 2301 et seq.)</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>(P.R. LAWS ANN. tit. 10, § 4051 et seq.)</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>(R.I. GEN. LAWS § 11-49.2-1 et seq.)</td>
</tr>
<tr>
<td>State</td>
<td>Code Reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>South Carolina</td>
<td>(S.C. CODE ANN. § 39-1-90)</td>
</tr>
<tr>
<td>Tennessee</td>
<td>(TENN. CODE ANN. § 47-18-2107)</td>
</tr>
<tr>
<td>Texas</td>
<td>(TEX. BUS. &amp; COM. CODE ANN. § 521.001 et seq.; see also HB 2004)</td>
</tr>
<tr>
<td>Utah</td>
<td>(UTAH CODE ANN. § 13-44-101 et seq.)</td>
</tr>
<tr>
<td>Vermont</td>
<td>(VT. STAT. ANN. tit. 9, § 2430 et seq.)</td>
</tr>
<tr>
<td>Virginia</td>
<td>(Va. Code Ann. § 18.2-186.6)</td>
</tr>
<tr>
<td>U.S. Virgin Islands</td>
<td>(V.I. CODE ANN. tit. 14, §§ 2208, 2209)</td>
</tr>
<tr>
<td>Washington</td>
<td>(WASH. REV. CODE § 19.255.010)</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>(WIS. STAT. § 134.98)</td>
</tr>
<tr>
<td>Wyoming</td>
<td>(WYO. STAT. ANN. § 40-12-501 et seq.)</td>
</tr>
</tbody>
</table>
Appendix I

Informed Consent

Title of Project: Healthcare Organizations’ Privacy Strategies

Principal Investigator: Rachida Parks, Graduate Student
321 D IST Building
University Park, PA 16802
(814) 232-1920; rfp127@psu.edu

Co-Investigator: Dr. Barbara Gray
404 Business Building
University Park, PA 16802
(814) 865-3822; b9g@psu.edu

Advisors: Dr. Chao Chu
301 K IST Building
University Park, PA 16802
(814) 865 3822; chc42@psu.edu

Dr. Heng Xu
307 C IST Building
University Park, PA 16802
(814) 814 867 0469; hxx4@psu.edu

1. Purpose of the Study: The purpose of this research study is to explore the factors influencing the ways in which healthcare organizations are responding to privacy issues. Also of interest is to examine the differences in strategies across healthcare organizations.

2. Procedures to be followed: You will be asked to participate in an interview of about 15 questions. The interview will be audio taped.
3. **Benefits:** This research might provide a better understanding of how healthcare organizations develop their privacy strategies.

4. **Duration:** It will take about 60 minutes to complete the interview.

5. **Statement of Confidentiality:** Your participation in this research is confidential. The data and audio recordings will be stored and secured in the researcher’s office in a password protected file. Only the investigators and the advisor will have access to the data. In the event of a publication or presentation resulting from the research, no personally identifiable information will be shared. Any audio-recording will be destroyed by the end of 2013.

6. **Right to Ask Questions:** Please contact Rachida Parks at (814) 232-1920 with questions, complaints or concerns about this research.

7. **Voluntary Participation:** Your decision to be in this research is voluntary. You can stop at any time. You do not have to answer any questions you do not want to answer.

    You must be 18 years of age or older to take part in this research study. Completion of the interview implies your consent to participate in this research. Please keep this form for your records.
Appendix J

Example Solicitation Email

From: RACHIDA PARKS [rfp127@psu.edu]
To: xxxxx
Subject: Study about Healthcare Organizational Privacy Strategies

Dear XXXX

My name is Rachida Parks and I am a doctoral candidate at the Information Sciences and Technology College at Penn State University. As part of my dissertation, I am conducting a research study related to the understanding of healthcare organizations' privacy strategies with regards to EHRs and seeking to interview health care information leaders on the topic of privacy programs and processes.

With the support from the highest levels of the federal government, healthcare information technology has grown considerably within the past decade. However, in spite of its potential benefits, healthcare IT is facing serious issues of how to ensure the privacy of electronic medical records which are being reported as the second highest data breaches.

The purpose of this research is to explore the factors influencing the ways in which healthcare organizations are responding to privacy issues. Also of interest is to examine the differences in privacy strategies across healthcare organizations. With an enhanced understanding of how healthcare organizations' privacy responses are shaped, and what factors contribute to these types of responses, practitioners may be able to select the most appropriate privacy response to achieve their desired outcomes toward meaningful use of EHRs. This is beneficial to researchers who can further expand on the grounded theoretical knowledge.

Your participation is highly appreciated to further advance theoretical and practical understanding of healthcare organizations responses to privacy issues. I would like to meet with you at a date/location that is the most convenient for you. We can also conduct the interview over the phone. The interview should last between 45 minutes to one hour.

Your prompt response is highly appreciated to further advance research in this area. Should you have any questions about the study, please contact me at rfp127@psu.edu or at 814-232-1920
Appendix K

Sample Documentation

Risk Analysis

Regulation & Standards
- HIPAA Security Rule
- FISMA
- There are numerous methods of performing risk analysis and risk management

Risks and Impact

Risks
- Unauthorized system level access to the EHR data and system (A)
- Interception of information acquisition or delivery; Remote Access activities, such as "man in the middle attacks" (B)
- Access to data by someone impersonating patients or healthcare professionals or System professional (C)
- Modification of EHR data during transmission (D)

Impact
- Data Breach, The HITECH Act substantially expands the HIPAA Privacy and Security Rules and increases the penalties for violations of HIPAA
- Loss of Trust
- Fraud and Abuse
- Impact to Care

Mitigation
- Identification & Authentication (A,B)
- Access Control Procedures (A,C)
- Auditing (A,B)
- Multi Tier Architecture (A)
- Anti-Virus (A)
- Data Encryption (B,D)
- Data Integrity Checks (D)
- Media Security (C,D)
- Laptop Security (C)
- Training (C)
Curriculum Vita
Rachida F. Parks

EDUCATION

Doctor of Philosophy (Ph.D.) - Information Sciences and Technology (IST)
The Pennsylvania State University, University Park, PA, USA, August 2012

Master of Science - Management Information Systems
University of Central Florida, Orlando, FL, USA, December 2001

Bachelor of Science - Business Administration
Institut Superieure International de Tanger, Tangier, Morocco, July 1994

JOURNAL PUBLICATIONS


REFEREED CONFERENCE PROCEEDINGS


