Organizational Privacy Responses in Healthcare:
A Conceptual Framework

Completed Research Paper

Rachida F. Parks
University of Arkansas at Little Rock
rfparks@ualr.edu

Rolf T. Wigand
University of Arkansas at Little Rock
rtwigand@ualr.edu

ABSTRACT
With rising unpredictability and continued changes in the healthcare environment, organizational responses to information privacy threats are unclear, needing better classification and precision. This paper presents an innovative approach by combining the pressures of the healthcare environment and its internal context by extending two organizational typologies: Oliver’s (1991) strategic responses to institutional processes, a motivational framework for examining privacy responses in light of institutional pressures, and Miles’ and Snow’s (1978) organization strategy, structure, and process framework providing a perspective on proactiveness. The findings based on in-depth interview data of executive-level healthcare information privacy decision makers highlight both the dimensions of resistance (resistance to institutional pressures) and proactiveness (the degree to which the strategy is proactive in protecting PHI (Protected Health Information). The resulting framework generates theoretically different but sound explanations for differences in information privacy strategic behaviors. The authors offer suggestions, implications and recommendations to researchers and practitioners.

Keywords
Information privacy, Healthcare Information Technology (HIT), organizational privacy responses, Electronic Health Records (EHRs), qualitative study.

INTRODUCTION
The use of information technology (IT) in healthcare is a core strategic issue for healthcare organizations in their efforts to reduce cost and improve healthcare quality. However, advances in healthcare IT are posing potential threats to the privacy and confidentiality of patient information. These threats have materialized for several healthcare organizations (hereafter referred to as ‘organizations’) as demonstrated by the increasing number of breaches reported to the Department of Health and Human Services (HHS)\(^1\) and other entities.

Defining privacy has been notoriously difficult (Tsai et al., 2010) because of its multidimensionality (Culnan and Williams, 2009). In healthcare, the notion of protecting patients’ privacy in the physician-patient relationship goes back to the Hippocratic Oath, which states in its modern version, “I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know” (Lasagna 1964). At the organizational level, information privacy refers to the right to determine when, how, and to what extent information is communicated to others (Claerhout and DeMoor, 2005). For Greenaway and Chan (2005), organizational information privacy refers to how firms treat their customers’ personally identifiable information. This study adopts Greenaway and Chan’s (2005) definition, thereby focusing on how healthcare organizations treat their patients’ protected health information (PHI).

Since 2007, nearly sixty health IT-related laws have been enacted in 34 states (Appari and Johnson, 2010) with their primary focus on defining the scope and boundaries of all different stakeholders which ultimately have to be integrated. Thus, healthcare organizations face external 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. Federal (e.g., HIPAA and HITECH) and state laws and regulations are among 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

\(^1\) http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
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.

In an environment of healthcare regulations, high levels of medical privacy breaches (Hasan and Yurcik 2006), and increasing penalties for non-compliance (Fernando and Dawson, 2009), organizations are facing difficult and complex decisions on how to respond to these threats and regulations. Moreover, recent research emphasizes the lack of research at the organizational level (Belanger and Crossler, 2011; Pavlou, 2011; Smith, Dinev, and Xu, 2011). Thus the research questions examined in this study are:

- How do healthcare organizations strategically respond to privacy threats?
- What factors influence healthcare organizations in developing their privacy strategies?
- Which organization theories can be used to provide a theoretical understanding of organizational privacy responses?

Rather than drawing on a single theoretical lens, we combine and extend two organizational typologies – Oliver’s (1991) framework and Miles’ and Snow’s (1978) typology – to answer these questions. The proposed theoretical framework is novel in the sense that no prior studies combined these different but sound concepts to illuminate differences in information privacy behaviors in the context of healthcare. This study aims to develop a better theoretical understanding that identifies alternative ways in which organizations define their responses, strategies and mechanisms to pursue these strategies. The proposed framework is based on the interpretation of existing literature with a special focus on the healthcare industry.

We first present both theoretical explanations for organizational privacy responses through the framework of Oliver (1991) and the typology of Miles and Snow (1978), discussing the value and benefits of integrating both perspectives. Then, we present our framework of Organizational Privacy Responses where we demonstrate the relationship between the two frameworks. After presenting the method section, we analyze the findings based on in-depth and extensive interview data of executive-level healthcare information privacy decision makers. We conclude with a discussion of theoretical and practical implications, and directions for future research.

THEORETICAL EXPLANATIONS FOR ORGANIZATIONAL PRIVACY RESPONSES

The ultimate purpose and utility of a theory is that it enables the researcher to describe, relate, explain and predict in a systematic and coherent framework the phenomena under study. Scientific works typically aims at one (or both) of two things: (1) the precise, accurate and parsimonious description of some phenomena, and/or (2) the explanation of some phenomena, i.e. why does a phenomenon take place? It is our intent to improve on existing theoretical privacy conceptualizations to offer improvements when explaining and predicting privacy phenomena.

Oliver’s Framework:

This research’s conceptual model departs from and extends Oliver’s (1991) framework of strategic responses to institutional pressures. We explicitly drew this theoretical framework to provide a foundation for identifying factors that influence the strategic responses to institutional pressures and specifically explored organizational responsiveness to privacy issues in healthcare.

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 (Oliver, 1991, p. 151) (see Table 1). First, organizations may embrace an acquiescence strategy and comply with institutional pressures. Through compromise, organizations can partially comply with institutional pressures. The third possible approach is avoidance by concealing compliance or escaping. Fourth, organizations may challenge the institutional requirements through defiance. And finally, organizations may attempt to manipulate regulators through alliances, control or influence. Oliver’s framework also includes a set of factors driving the strategic responses. They are cause, constituents, content, control, and context. Each of these factors is expected to affect an organization’s strategic response.
Table 1: Strategies for resistance and accommodation to institutional pressures
(Adapted from Oliver (1991, p. 152)

<table>
<thead>
<tr>
<th>Oliver’s Strategies</th>
<th>Oliver’s Tactics</th>
<th>Oliver’s Examples</th>
<th>Healthcare Privacy Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquiescence</td>
<td>Habit • Imitate • Comply</td>
<td>Following invisible, taken-for-granted norms. • Mimicking institutional models. • Obeying rules and accepting norms.</td>
<td>Adopting and complying fully with HIPAA(^2) privacy and security rules.</td>
</tr>
<tr>
<td></td>
<td>Balance • Pacify • Bargain</td>
<td>Balancing the expectations of multiple constituents. • Placating and accommodating institutional elements. • Negotiating with institutional stakeholders.</td>
<td>Negotiating through healthcare chapters such as HIMSS(^3) and CHIME(^4) to meet the external requirements at a reduced cost.</td>
</tr>
<tr>
<td>Compromise</td>
<td>Conform • Buffer • Escape</td>
<td>Disguising nonconformity. • Loosening institutional attachments. • Changing goals, activities, or domains.</td>
<td>Writing policies that do not reflect organizations’ actual enactments of privacy.</td>
</tr>
<tr>
<td>Avoidance</td>
<td>Dismiss • Challenge • Attack</td>
<td>Ignoring explicit norms and values. • Contesting rules and requirements. • Assaulting the sources of institutional pressure.</td>
<td>Opposing to HIPAA privacy and security rules by healthcare organizations.</td>
</tr>
<tr>
<td>Defiance</td>
<td>Co-opt • Influence • Control</td>
<td>Importing influential constituents. • Shaping values and criteria. • Dominating institutional constituents and processes.</td>
<td>Influencing and or controlling healthcare regulations through lobbying.</td>
</tr>
<tr>
<td>Manipulation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Oliver’s framework (1991) received widespread attention and several studies provided empirical evidence to her conceptual framework (Clemens and Douglas, 2005). Both Goodstein (1994) and Ingram et al. (1995) confirmed Oliver’s framework in their research. However, they both tested only the first four strategic responses, disregarding manipulation, the last strategy. Goodstein’s study was among the first to empirically validate Oliver’s framework that examined the strategies organizations adopted in response to institutional pressures. Etherington and Richardson (1994), in their study of institutional pressures on accounting education, applied Oliver’s five strategies based on two dimensions: passive/active responses and positive/negative responses. With acquiescence being passive and neutral, Etherington and Richardson (1994) grouped avoidance and defiance under active-negative strategies, compromise and manipulation under active-positive strategies. Recent applications of Oliver’s framework expands across a variety of sectors (e.g., banking, fashion) (Munir, Perera and Baird, 2011; Pedersen, and Gwozdz, 2013).

Miles’ and Snow’s Typology:

While Oliver’s framework considered institutional pressures when studying organizational responses, several of her follow-up empirical studies called for integrating other lenses (Clemens and Douglas, 2005). Considering the integration of Miles’ and Snow’s (1978) typology is not an arbitrary decision. Miles and Snow (1978) offer another theoretical framework that considers three interrelated problems, the entrepreneurial problem pertaining to the organization’s definition of a product-market domain, the engineering problem related to the technologies and processes in relationship with an engineering solution, and, finally, the administrative problem pertaining to ways the organization implements its strategies. Miles and Snow 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 typology, the strategic types represent alternative forms, each of which has its own adaptive strategy (Miles and Snow, 1978).
The prospector is the most dynamic and proactive type of strategies. This type of organization identifies opportunities for developing new products or markets that are critical to their success. The defender enacts and responds to their environment in a less dynamic form. Moreover, the defender focuses on establishing a productive and stable environment. The analyzer is a unique combination of prospector and defender types (Miles and Snow, 1978) seeking to minimize risk and maximizing profits. The fourth type, the reactor, lacks consistency and clarity.

Miles’ and Snow’s typology has stimulated numerous empirical investigations. For a review, see (Zahra and Pearce, 1990) with a call to pursue industry specific studies. The healthcare industry was used as one setting for developing Miles’ and Snow’s theoretical typology (Miles and Snow, 1978, p. 214). Several studies applied Miles’ and Snow’s typology in the healthcare context (Shortell and Zajac, 1990; Zahra 1987; Zajac and Shortell, 1989). Recent research encompasses several sectors including the retail industry (Parnell, 2013), hospitality (Köseoğlu, Topaloglu, Parnell and Lester, 2013) and healthcare (Zinn, Spector, Weimer and Mukamel, 2008). Collectively, these studies provide important insights into Miles’ and Snow’s perspective especially in the healthcare industry.

**Taxonomy of Organizational Responses:**

Oliver’s work has inspired several empirical studies. While these empirical studies confirm Oliver’s contribution, they raised discussion on potential regrouping of resistance strategies (Clemens et al. 2008, Clemens and Douglas 2005). We extend Oliver’s framework to encompass responsiveness to institutional pressures into three main responses: Avoidance, manipulation and compliance as a mid-point. First, organizations may embrace an avoidance strategy through disguise of conformity or defiance of the regulations. Second, they may fully cooperate and comply with institutional pressures. Third, organizations may attempt a compromise response through negotiation or manipulation (e.g., lobbying and influencing regulators). The above three responses are not exclusive (Clemens and Douglas, 2005) as organizations may comply with institutional pressures but may still negotiate with regulators where enactment of privacy measures are conflicting with business operations.

We further expand the compliance response to incorporate three different levels using Miles’ and Snow’s (1978) typology of reactors, defenders, analyzers and prospectors. The analyzer strategy has been interpreted sometimes as a combination of the prospector and the defender (Doty, Glick and Huber, 1993). Therefore, we will only consider the reactor, defender, and prospector within the compliance strategy (see Figure 1).

![Figure 1: Taxonomy of Organizational Privacy Responses](image-url)
A PROPOSED FRAMEWORK OF ORGANIZATIONAL PRIVACY RESPONSES (OPR)

The need for integrating theoretical frameworks rises when significant gaps on organizational privacy responses exist in the literature. Existing organizational research has used a limited repertoire of theories to explicate organizational behavior in responding to privacy issues and threats (Greenaway et al., 2005). Combining both frameworks yields a conceptual richness that would not have been achieved separately by each of them individually.

Existing theoretical models have examined either the resistance perspective (Oliver, 1991) or the proactivity perspective (Miles and Snow, 1978) with regards to organizations’ privacy behaviors but not both. Oliver’s framework, based on the institutional resource dependence theories, distinguishes among five types of strategic responses which represent increasing levels of resistance to institutional pressures. What seems to distinguish mainstream institutional theory from the privacy literature is that the latter is open to responses beyond conformity and resistance (Culnan and Williams, 2009). Recent research, not limited to privacy, has called for more studies on how organizations respond to institutional pressures while adopting a proactive strategy (Peng and Chen, 2011). With regards to reactive-proactive strategies, Miles’ and Snow’s typology present four strategic types of organizations: the prospector, the analyzer, the defender, and the reactor. By combining both lenses, this study offers a theoretical framework that transcends the institutional theory that has been demonstrated to be inadequate in explaining differences in organizational responses (Delmas and Toffel, 2008) and the moving beyond resistance behaviors to include proactive behaviors in responding to information privacy threats. Therefore, the reasoning for this grouping is the combination of both institutional and organizational strategy lenses while accounting for differences in internal factors specific to each organization as depicted in Figure 2.

![Figure 2: Framework of Organizational Privacy Responses](image-url)

**Reactor Response:**

Most organizations’ information privacy behaviors are primarily responses to external pressures and ‘having to do what the law requires’ (Greenaway et al., 2005; Milberg et al., 2000). This type of behavior is reactive to either negative publicity (e.g., medical records breaches) or to legislative pressures. Smith (1993) referred to this process as “drift-threat-reaction” meaning that organizations’ privacy measures tend to “drift” until facing an external “threat”, and then the organization would “react” with formalized policies and interventions. The reactive response has been defined in Miles’ and Snow’s adaptation typology as “responding inappropriately to environmental change and uncertainty, performing poorly as a result, and then being reluctant to act aggressively in the future” (Miles and
Snow, 1978, p. 557). By definition these reactive strategies act only when there is a data breach or legislative pressure. In healthcare, organizations adopting this reactive approach will develop technical measures or policies as a reaction to an unauthorized data access, data breach or other threats. This reaction is driven by compliance to external pressures such as experienced with HIPAA and HITECH.  

**Defender Response:**

The compliance mind-set or the defender type strategy “deliberately enacts and maintains an environment for which a stable form of organization is appropriate” (Miles and Snow, 1978, p. 550). Therefore organizations embracing this type of strategy are a bit more proactive than the previous strategy but their processes focus on achieving efficiency through technical compliance and appropriate policies. Technical responses include tools such as privacy enhancing technologies to support the business objectives to handle the privacy threats. However, little consensus has been reached in the privacy research community concerning the technological requirements to be integrated into systems to assume privacy protections (Spiekermann and Cranor, 2009).

Within security measures by the United States Government Accountability Office (GAO, 2007), a GAO report identified authentication, authorization and access control, encryption, information protections, and information audits. With the use of electronic medical records, different stakeholders are accessing patient data for different contextual purposes. To manage access to and prevent unauthorized access to patient data, several researches focused on contextual role-based information access (Kalam, Baida, Balbiani, Benferhat, Cuppens, Deswarte, Miege, Saurel and Trouessin, 2003; Motta and Furrie, 2003). Under the compliance strategy, organizations focus on strengthening their technical security measures to insure the stability of their operations with emphasis on efficiency, and prevent any unauthorized data access.

**Prospector Response:**

Unlike the defender strategy that thrives to achieve stability thorough compliance, prospector response undertakes a more dynamic approach (Miles and Snow, 1978). This type of organization invests on current and future capabilities. Therefore, their proactive response includes integrating a culture of privacy and governance processes (Culnan and Williams, 2009). Proactive response calls for policies that are personalized to the organizations, its customers and users (Greenaway and Chan, 2005).

A significant number of studies has focused on technological solutions (Agrawal and Johnson, 2007; Blobel 2004) and legal compliance through policies (Culnan and Williams, 2009; Greenaway and Chan, 2005) but rarely into multiple responses. Because of the mismatch and gap between policies and actual practices and the call for a proactive role in acting on privacy concerns, we considered further options within the proactivity level in our framework. The prospector response focuses on aligning these policies and technologies along with implementation practices through governance and operational processes (Baker et al., 2008); in other words, translating policies into feasible and measurable actions that fit the prospector business type strategy (Miles and Snow, 1978). With regards to privacy culture, returns on investments on privacy programs are not obvious thus making key executives’ commitment as a major driver of adopting a culture of privacy (Culnan and Williams, 2009).

**METHOD**

To answer our research questions we conducted a multiple case study of privacy threats in the U.S. hospital industry, using a holistic case research design (Yin, 1999). The multiple case study research method is particularly appropriate for answering how and why research questions in settings in which the phenomenon of interest, i.e. privacy threats, cannot easily be distinguished from its context, i.e. interrelations among organizations in an industrial community (Yin, 1999). Our questions, concerning how and why privacy threats, specifically organizational privacy responses to privacy threats, in hospital industry-specific settings arise and can be successfully resolved, meet Yin’s criterion. The unit of analysis in our research questions is the organizational privacy response effort—an organization-level phenomenon. We chose a multiple case design in order to being able to generalize our findings back to hospital organizations after intensive data collection. Our research design involves holistic, rather than embedded units of analysis; that is, although we necessarily examine the interests and resources of the organizations making up the industry as they contribute to organizational privacy responses (OPR), our

---

outcome of interest and explanation then may be inferred back to the hospital industry specifically and the healthcare industry generally.

Our research context is healthcare IT with a focus on healthcare organization behaviors with regards to privacy issues related to the use of electronic health records (EHRs). In this study, we interviewed healthcare organization decision makers in small, medium and large hospitals. Also included were representatives from healthcare nonprofit associations and healthcare consulting firms.

The data on organizational privacy responses reported here were collected from 30 healthcare executives in 21 healthcare organizations. Semi-structured interviews were conducted as part of a larger project and are presented in support of our framework of organizational privacy responses. Interviews were conducted with healthcare executives such as chief information officer, chief privacy officer, chief medical information officer, and an HIPAA security officer. Interviews were one-on-one as well as group interviews and lasted between 40 and 100 minutes and were all audio-recorded. To analyze our data, we leverage both inductive and deductive coding. This hybrid approach allows creative insights to be generated using existing concepts from the literature (Fereday and Muir-Cochrane 2006).

FINDINGS AND ANALYSIS

Due to the limited space in these proceedings, we are presenting only high level themes supporting our OPR framework.

Types of Healthcare Organizational Privacy Responses

Answering the first research question, we sought to document the variations in responses to privacy issues in the complex and challenging environment of healthcare. Accordingly we asked direct questions about the informants’ privacy strategies and indirect questions about their enactment of privacy. Asking these questions was important as it allowed us to align their perceived strategies with their enactment of privacy. We found evidence of three major responses categories to privacy issues in healthcare: Avoidance, compliance and compromise.

Avoidance has been portrayed as the only response option for rural hospitals with a less lucrative payer mix, implying a higher percentage of Medicare and Medicaid patients. This high percentage translates quickly into financial issues and thus an inability to afford the appropriate infrastructure to comply with these regulations. An informant provided the name of a rural hospital that closed its doors because of inability to keep up with the operating costs. While it may sound reasonable to make the assumptions that lack of resources in rural hospital stands against fully complying with the regulations, further data collection from this type of hospital would be recommended to shed further light on this response type.

One of the major factors influencing healthcare organizations to develop and implement privacy responses are the institutional pressures from HIPAA and HITECH. One dominating response to these pressures is compliance. With the fear of hefty penalties and costly processes of informing patients whose information has been compromised, healthcare organizations are adopting a compliance strategy to protect their patient protected health information (PHI). They are developing policies and processes that are in alignment with healthcare regulations as one informant stated “we have to understand the legislation and will have to abide by the rules and to then have an infrastructure to be able to do those things.”

The third type of response is compromise through negotiation and the manipulation of the law. Most healthcare organizations are members of nonprofit healthcare associations such as HIMSS and CHIME. Through the local chapters of these organizations, hospitals communicate and exchange their disagreement with current regulations. These disagreements are lobbied through national chapters as one informant stated “we have to understand the legislation and will have to abide by the rules and to then have an infrastructure to be able to do those things.”

Different Levels of Compliance

Our data analysis distinguishes between different levels of compliance through the countermeasures being used.
Hospitals with a Reactor Strategy

This type of organizational behavior is reactive to either negative publicity (e.g. medical records breaches) or by legislative pressures. One privacy officer stated that they have to:

“abide by the rules, comply with healthcare regulation” and “we have to understand the legislation and will have to abide by the rules and to then have an infrastructure to be able to do those things.”

While we suspect this type of approach as being the dominant among healthcare organizations, we cannot confirm it through this qualitative study.

These reactive strategies act only when there is a data breach or a legislative pressure. 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 to avoid civil and criminal penalties as expressed by one informant:

“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.”

Hospitals with a Defender Strategy

This type of organization demonstrates compliance with healthcare regulations. One security officer shared that they focus on achieving efficiency:

“You do your due diligence, you don’t overspend, you don’t underspend, you make the case for what is needed and how it matches up with laws and pick one security to protect your data and patients’ rights.”

This type of hospital also engages in social engineering for the purpose of measuring employees’ privacy awareness, and proceeding to termination of employees or business associates who are not abiding by privacy policies and agreements.

Hospitals with a Prospector Strategy

On the other side of the spectrum, organizations with a built-in culture for patient privacy are embracing a proactive approach and have invested in patient privacy even before the enactment of HIPAA and HITECH. One informant stated:

“It is not like we did not care about information before, now all of the sudden the legislation make you compliant with this, which is a poor assumption. We clearly value patient, health information security at the highest level.”

Hospitals with this type of response showed a more dynamic approach by investing on current and future capabilities. Therefore, a chief privacy officer response includes investing in proactive measures and integrating a culture of privacy as justified by a chief privacy officer:

“Because we are proactive in that we are on constantly monitoring and testing ourselves for breach.”

These hospitals focus on aligning these policies and technologies along with implementation practices through employees’ buy-ins and user centered programs. One informant stated:

“It is very important that when you develop a process that you get buy in from the staff and they understand the reason for it... those are the users we have these policies and procedures work for... worse than not having a policy, is having policies that are not followed.”

External Environment and Internal context

Our review of the literature probed our awareness of the concept of institutional pressures. We therefore asked questions about healthcare regulations and other possible factors impacting how they design and develop their privacy programs and processes. One informant revealed internal and external perspectives to how privacy responses might be affected:

“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 get adjusted based upon both internal and external information.”
Concerning the second research question addressing factors that influence healthcare organizations in developing their privacy strategies, we summarize these factors into internal and external pressures (Table 2).

<table>
<thead>
<tr>
<th>External/Internal</th>
<th>Description</th>
<th>Exemplary Quotations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External Pressures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory pressures</td>
<td>Complying with HIPAA and HITECH</td>
<td>“There are hefty fines and penalties for organizations. You can be fined up to 1.5 million dollars by the federal government if you have an egregious breach.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“All the work that goes into contacting these patients and sending letters if there is a breach”</td>
</tr>
<tr>
<td>Competitive Pressures</td>
<td>Hospitals may attempt to invest in privacy measures to avoid breaches and create sustainable advantage over their competitors</td>
<td>“There is the business driver where as 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”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“There are a lot of high profile patients that come through this facility and we have to be on guard that we don’t have employees that are curious about their medical records”</td>
</tr>
<tr>
<td><strong>Internal Context</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resources/Payer Mix</td>
<td>Establishment of privacy programs requires significant resources to support the privacy measures. Payer Mix refers to a mix of who is paying the hospital billing claims: major insurance carriers, self-pay and government for Medicaid and Medicare plans.</td>
<td>“It is not cheap. We spend a lot of money every year on security and I have a person in place right now who is does nothing but security “</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“The different firewalls and antivirus systems, they are all very expansive.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“I do not what percentage at the budget is goes into this but I can probably find a rough estimate. But it is significant”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“If you have a big payer mix as Medicare or Medicare, a lot of rural hospitals do. If you do not meet these regulations … they will start reducing money”</td>
</tr>
<tr>
<td>Best Practices</td>
<td>Overall organization strategy of how reactive/proactive they are toward certain business practices</td>
<td>“Even if the regulations were not there ... you have to have best practicing and you have to have good practices. “</td>
</tr>
<tr>
<td>Education/Culture of Privacy</td>
<td>Programs that promote awareness of enacting privacy, and a culture of privacy that includes buy ins from staff</td>
<td>“The biggest challenge is making sure people know the rules. “</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Educate the staff about HIPAA, orientations plus ongoing annual training regarding HIPAA laws and issues.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“It is very important that when you develop a process that you get buy-in from the staff ad they understand the reason for it. “</td>
</tr>
</tbody>
</table>
| | | “I think the culture is changing and everyone really
understands the right to privacy””

IT Infrastructure | From hardware to software capabilities to support healthcare IT including EMR implementation level. | “We are more advanced than a lot of the major hospitals in IT. I have over 1100 PCs out there. We’ve had an EMR for 13 years. A lot of the meaningful use stuff, we already meet”
        | “We have software which goes through every PC every day looking for things on PCs. so we have software in place that look for certain patterns of information of people are trying to send out here “
Balance | balancing day –to –day operations with privacy requirements | “It is a rough balance between maintaining privacy and not degrading the performance of the network”
        | “It impacts the day to day workflow of almost everybody here”

Table 2: Factors influencing Healthcare Organizational Privacy Responses

DISCUSSION AND IMPLICATIONS

We generated and tested a theoretical model of organizational privacy responses (OPR) to understand how and what factors influence these responses. External and internal factors are impacting how organizations fall under a resistance continuum ranging from compliance to avoidance and finally manipulation. It should be noted that in this research the authors mainly focused on organizations being exerted to external pressures, mainly in the form of regulatory pressures. When compliance is embraced, healthcare organizations undertake reactive, prospective or defender type strategies.

Our results elaborate on Oliver’s framework of strategic responses to institutional processes, which Etherington and Richardson (1994) argue could be grouped into three responses: acquiescence as passive and neutral response, avoidance and defiance were grouped under active-negative strategies, while compromise and manipulation under active-positive strategies. Our findings suggest a consensus with Clemens’ and Douglas’ (2005) empirical studies. Our data further expands Oliver’s framework by considering the dimension of proactiveness elaborated by and based upon Miles’ and Snow’s typology.

This study is not only beneficial to researchers who can further expand on the grounded theoretical knowledge but provide several insights for practitioners. With an enhanced understanding of how healthcare organizational 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 desired outcomes toward meaningful and proper use of EHRs.

CONCLUSION

Our research provides unique theoretical insights and sound explanations for differences in information privacy behaviors within the healthcare industry at the organizational level. Existing theoretical models have examined either the resistance perspective (Oliver, 1991) or the proactivity perspective (Greenaway and Chan, 2005; Miles and Snow, 1978) but not both. We have offered a theoretical extrapolation combining Oliver’s typology with Miles’ and Snow’s framework to form a new conceptual framework that is coherent, comprehensive and unifying. Moreover, it permits us to explain and predict OPR phenomena under study. This contribution demonstrates the gap of under-researched organizational levels as well as the overall lack of theory in privacy research. Our study embraces an interdisciplinary perspective including information systems, management and medical informatics communities and highlights the importance of internal and external factors in influencing how organizations respond and enact their privacy responses. Furthermore, this framework provides healthcare executives with the ability to envisage different privacy responses that align with their organizational strategy. We recommend that future research include examining empirically the above proposed theoretical OPR framework to further validate the resistance as well as proactive responses. We propose a mixed method approach through interviews of CIOs and CPOs of healthcare organizations as well as survey questionnaires to triangulate the findings.
REFERENCES


