8-5-2011

Healthcare Information Privacy Research: Iusses, Gaps and What Next?

Rachida Parks
The Pennsylvania State University, rfp127@ist.psu.edu

Chao-Hsien Chu
The Pennsylvania State University, chu@ist.psu.edu

Heng Xu
The Pennsylvania State University

Healthcare Information Privacy Research: Issues, Gaps and What Next?

ABSTRACT

The proliferation of e-health holds great promises in sharing medical data, improving healthcare quality, saving patient lives and reducing costs. However, these potential benefits also bring much attention to the issues of information privacy. Given that medical data disclosure is the second highest reported breaches, it is imperative to understand both information privacy and its context in healthcare. Just as lack of appropriate privacy measures might cause economic harm or denied service from insurance or employers, tight privacy can prevent care providers from accessing patient information in time to save lives. This paper takes an integrated look into the area of healthcare information privacy from both MIS and health informatics perspectives. Based on the literature review and our personal communication with health informatics experts, we identified and presented four major themes: 1) scope and definition of privacy and electronic health records, 2) the information privacy issues and threats, 3) the countermeasures used to address and manage information privacy and 4) why privacy responses matter. This paper provides a unique perspective to privacy in the context of healthcare by focusing on the issues, the matching countermeasures and the drivers behind organizational behaviors into how they manage these threats.

Keywords

Information privacy, E-health, Health Informatics, Electronic Health Records (EHRs)

INTRODUCTION

With the support from the highest level of the federal government (Bush 2004; Obama 2009), e-health and more specifically electronic health records (EHRs), has grown considerably over the past decade. However, in spite of its potential benefits such as sharing medical data, improving healthcare quality, saving lives and reducing costs (Appari et al. 2010; Fernando et al. 2009; Kluge 2007), EHRs proliferation is hampered by patient information privacy issues (Chen et al. 2010; Chiang et al. 2003). As a result of privacy threats and breaches, patients might be subject to harassment, discrimination, economic harm or denied service from insurance or employers (Neubauer et al. 2011; Ohno-Machado et al. 2004; Sadan 2001); and thus the issue of how and what measures need to be incorporated to address and protect personal health records was raised (Pear 2009).

The notion of privacy issues and threats vary depends on several influences such as industry sectors, regulatory laws and cultures (Malhotra et al. 2004; Milberg et al. 1995). Several countries, such as Australia, Canada, New Zealand and countries in the European Union, have embraced an omnibus law that address all issues related to data collection, use and dissemination (Smith 2004; Zwick et al. 2001). In the United State, privacy laws are sectoral with industry specific regulatory rules (Culnan et al. 2009), for example, in healthcare there is the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH). Thus, information privacy as a concept holds different definitions or expectations across industries. Consequently, privacy issues and threats will be better understood when they are bounded by a specific context (e.g., healthcare industry) (Bansal et al. 2008; Johns 2006). Therefore, integrating health informatics research findings to MIS literature in information privacy seems pertinent in order to gain in-depth insights.

Recent research underscores the significance of privacy threats on information collection and uses (Culnan et al. 2009; Greenaway et al. 2005; Mishra 1996). Examining privacy threats in the healthcare environment is difficult, because such environment is complex, changeable and has stricter regulations and policies (Garfinkel et al. 2002; Thatcher et al. 2000). Congress' recognition that advances in e-health could erode the privacy and confidentiality of health information led to the adoption of privacy regulations for protecting individual identifiable health information. The HIPAA act of 1996 lays out a broad set of specifications for privacy at the federal level and defines the regulatory requirements for protected health information (PHI) with override capabilities at the state level (Appari et

al., 2009). This created variability in state-level and federal regulations that some scholars are considering as a major impediment to healthcare organizations to comply with regulations (Hodge Jr. 1999; Langenderfer and Cook 2004).

In the presence of increasing penalties for non-compliance (Fernando et al. 2009; Mohan et al. 2004) and privacy operational challenges (Croll 2010), organizations are facing challenges on how to respond appropriately to privacy threats while not impeding health care workflows. This paper provides a unique perspective to privacy in the context of healthcare by focusing on the issues, the matching countermeasures and the drivers behind organizational behaviors into how they manage these threats.

The rest of the paper is organized as follow. In the following section, we present our research methodology, briefly discussing the journal selection, time span and the review process. Next, we discuss in details the four themes identified from our literature analysis. We conclude with future research directions in healthcare information privacy.

REASEARCH METHODOLOGY

The objective of this paper is to examine major research issues in information privacy in healthcare and identify gaps and opportunities for future directions through an extensive literature review. The literature search was based on the keywords "privacy," "information privacy", and "healthcare" within the MIS and health informatics communities. Each article was fully reviewed and was excluded if it did not relate to information privacy. Although our search was not exhaustive, it constitutes a reasonable coverage for a sectoral focus on information privacy in healthcare.

For MIS publications, we selected MIS Quarterly, Information Systems Research, Journal of the Association for Information Systems, Organization Science and ICIS proceedings as the outlets for review. We chose 1990 as a starting date for the MIS literature search. This is because, according to Smith (1996a), it was then that the preliminary research on information privacy began to emerge (Culnan 1993; Milberg et al. 1995; Smith 1994). We believe therefore, that early 1990s might be considered as a starting point of information privacy research in MIS.

For Health informatics publications, we considered the Journal of American Medical Informatics Association (JAMIA), Journal of Biomedical Informatics, and International Journal of Medical Informatics. In the healthcare environment, data protection has been addressed from the earliest days of computer storage (Griesser 1980). With the proliferation of EHRs to over half of the hospitals in the US (Anderson 2000) and the introduction of the Internet and other networking capabilities, together with media reports on violations (Ohno-Machado et al. 2004), privacy issues started arising to the forefront. Various state and federal regulations, such as HIPAA Act of 1996, started mandating the protection of patients' privacy. Thus, retrieving for information privacy articles in health informatics backs to year 2000 seems reasonable.

Papers were classified based on the privacy definition, privacy threats, countermeasures and the factors driving organizations' responses. This classification helped identifying and analyzing relevant issues and gaps in the literatures. Our second approach that led this classification was through the analysis of ten semi-structured interviews with consenting key informants in healthcare organizations such as chief information officers (CIO), chief privacy officers (CPO), and chief medical information officers CMIO. The interviews, conducted as part of a an ongoing project, were transcribed and analyzed using Strauss and Corbin's (2008) constant comparative approach. Quotes from the healthcare experts were used throughout this paper to support our literature classification.

RESEARCH ISSUES AND CLASSIFICATION

We classify the review of healthcare information privacy issues into four broad categories: Scope and definition of privacy and EHRs; the privacy threats and vulnerabilities; the measures used to address and manage privacy; and why privacy matters (see Figure 1). This classification, based on the What, Why and How logic, is for the purpose of more comprehensive understanding of existing research in order to provide a clear picture for further research in healthcare information privacy. The "What" logic allows us to define information privacy from communities as well

as what privacy issues and threats organizations are facing? How organizations are addressing these threats is handled through the "How" logic by providing a taxonomy of privacy measures; and finally "Why" organizations are responding depict the drivers influencing their responses.

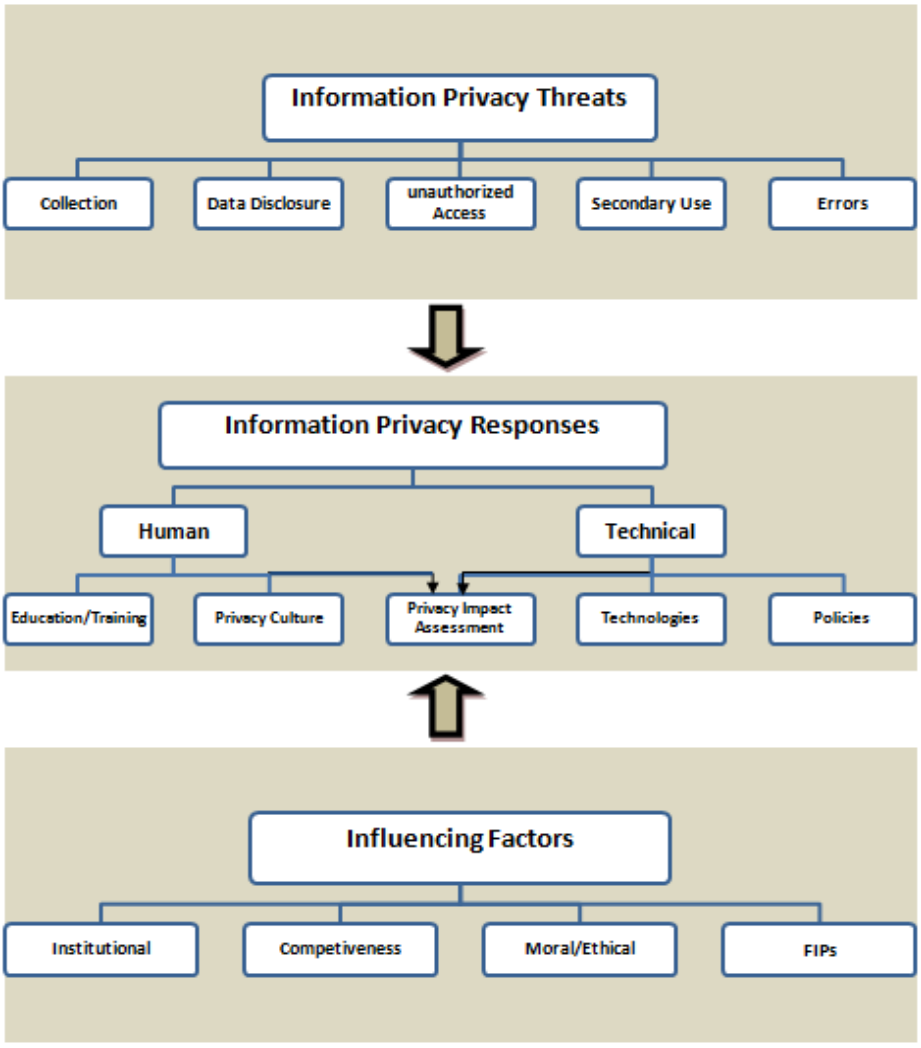

Figure 1. Classification of Information Privacy Research Issues

Theme 1: Definition and Scope of Information Privacy and EHRs

Information Privacy

Defining privacy has been notoriously difficult (Tsai et al. 2010) because of its multidimensionality (Culnan et al. 2009) and its broadness (Smith 1993). In certain countries, the concept of privacy was not even previously defined (Ishikawa 2000). The scope of this research pertains specifically to information privacy and it 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 over how personal information is acquired and used has been embraced by several scholars (Culnan et al. 2009; Peleg et al. 2008; Smith et al. 1996a).

In healthcare, the notion of protecting patients' privacy from a 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, patient information privacy definition has its basis on confidentiality, integrity, availability and accountability (Ishikawa 2000). When asked to define information privacy, a 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 MIS 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 such environment is complex, changeable and has stricter regulations and policies (Garfinkel et al. 2002; Thatcher et al. 2000). Federal regulations are usually overridden by state healthcare regulations and by 2007, nearly 60 Health IT related laws have been enacted in 34 states (Appari et al. 2010). The focus is on defining the scope and boundaries of all different stakeholders which ultimately has to be integrated. Thus future research should address healthcare information privacy with an integrative focus rather than an isolated one.

Electronic Health Records

Although the terms of electronic medical record (EMR) and EHRs describes two different concepts, they have been used interchangeably (Garets et al. 2006). In what follow, we will provide definition of EMR and EHRs from the MIS and health informatics communities.

In MIS and medical informatics literature, EMR refers to electronic patient records that are created and maintained by one care delivery organization (CDO) and include patient medical history, clinical documentation, medications, laboratory and radiology test results (Tong et al. 2009). This definition is supported by the Institute of Medicine report (IOM 1991) defining 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 patient information in digital format and make the information available to other healthcare stakeholders (Angst et al. 2009). EHRs represent the primary mechanism through which interoperability of health information can take place (Agarwal et al. 2007). This definition aligns with the one from the medical informatics community as Garets stated that "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, in our literature review we will focus on the EHRs.

Theme 2: Privacy Issues & Threats

In MIS literature, problems and challenges surrounding privacy have been originally centered around four dimensions of individuals' concerns on organizational information privacy practices: collection of personal information, unauthorized secondary access, errors, and improper access (Smith et al. 1996a; 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 et al. 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 arise include data ownership (van der Linden et al. 2009), complexity of the evolving healthcare legislation (Croll 2010) and EHRs design (Kluge 2007).

Table 1 depicts a summary of relevant privacy issues and threats from MIS and medical informatics literature. The analysis of the literature highlights several key privacy issues and threats:

Privacy Issues and Threats	MIS References	Medical References
Data Collection	(Culnan et al. 2009; Malhotra et al. 2004; Smith 1993; Smith et al. 1996b; Solove 2006; Stewart et al. 2002)	(Croll 2010)
Data Use and Disclosure	(Dinev et al. 2006; Li et al. 2010a; Malhotra et al. 2004; Solove 2006)	(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)
Unauthorized Access	(Culnan et al. 2009; Smith et al. 1996a; Solove 2006; Stewart et al. 2002)	(Chen et al. 2010; Croll 2010; 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)
Secondary Use	(Culnan et al. 2009; Culnan 1993; Smith et al. 1996a; Solove 2006; Stewart et al. 2002)	(Aberdeen et al. 2010; Chiang et al. 2003; Croll 2010; Ishikawa 2000; Neubauer et al. 2011; Quantin et al. 2000)
Errors	(Smith et al. 1996a; Stewart et al. 2002)	(Croll 2010; Mohan et al. 2004; Reni et al. 2004)
Ownership of the Data		(Sadan 2001; van der Linden et al. 2009)
Balance between Privacy Policies, Clinical Users and Patient Expectation		(Croll 2010; Mohan et al. 2004)
Awareness of Privacy Practices	(Malhotra et al. 2004)	(Croll 2010)
EHRs Design and Lack of Standards		(Kluge 2007)

Table 1. Summary of Privacy Issues and Threats

Data Collection: Organizations should only collect for the purpose identified as essential (Croll 2010; Culnan et al. 2009). However individuals perceptions on the fairness of data collected by organizations vary (Malhotra et al. 2004) and brings up a number of concerns associate with data collection (Smith et al. 1996a).

Unauthorized Access: Health and medical data is privileged information and should be accessed based on need to know (Croll 2010; 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. 1996a). This type of threats include abuse by authorized personnel when browsing records for curiosity purposes (e.g. access family members) or ulterior motives (e.g., celebrities medical information) (Culnan et al. 2009). It also includes hacking by external entities which results in harms such as data breaches.

Secondary Use: Information secondary use involves new uses for the information collected by organizations (Culnan et al. 2009). Smith (1996) differentiated between internal secondary use and external secondary use when information collected for one purpose is used for another weather within the same organization or disclosed to an external organization (Croll 2010; Ishikawa 2000).

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 can also be disclosed to outside entities (Ohno-Machado et al. 2004). Patients' data disclosure could lead to patients' harassment, discrimination, economic harm or denied service from insurance or employers (Neubauer et al. 2011; Ohno-Machado et al. 2004; Sadan 2001).

Errors: Organization 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 consumers information either subject to incorrect information or even mistaken identity (Smith 1993).

As can be seen from the summary, MIS literature focused more on data collection issue; while medical informatics literature is more concerned on issues related to data use and disclosure, unauthorized access, secondary use and errors. Recent medical informatics studies are focusing 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 balance between privacy policies, clinical users and patient expectation (Croll 2010).

Theme 3: Protecting and Managing Information Privacy

Individuals and organizations face a plethora of privacy issues and threats. It might be expected that such a wide variety of privacy issues and threats, and its associated breaches would have produced an abundance of empirical research studies on how to address them. Our literature review revealed that it is not the case (Smith et al. 2011) and the theories to address these problems remain also underdeveloped (Greenaway et al. 2005).

While several research provided a categorization of privacy problems and issues (Smith et al. 1996a; Solove 2006), very few attempted to categorize the countermeasures to address these threats (Culnan et al. 2009; Greenaway et al. 2005). In this paper, we endeavor not only to provide a taxonomy of privacy measures but to map the technical measures to the appropriate threats (See Table 2).

Privacy Measures	MIS References	Medical References
Technical	(Tsai et al. 2010)	(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)
Policy	(Greenaway et al. 2005; Smith 1993; Tsai et al. 2010)	(Anderson 2000; Ishikawa 2000; Mohan et al. 2004)
Training and Education	(D'Arcy et al. 2009; Yeh et al. 2007)	(Fernando et al. 2009; Ishikawa 2000; Mohan et al. 2004; Patel et al. 2000)
Culture of privacy	(Culnan et al. 2009)	(Ishikawa 2000; Mohan et al. 2004)
PIA Privacy Impact Assessment	(Culnan et al. 2009)	(Croll 2010)
Disciplinary actions	(Herath et al. 2009; Straub et al. 1990)	(Fernando et al. 2009; Mohan et al. 2004)
Physical measures		(Mohan et al. 2004)

Table 2: Summary of Privacy Countermeasures

Organizations are expected to have safeguards in place against these threats of privacy (Culnan et al. 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). These responses are summarized by a healthcare expert as an internal-external approach

> *"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 that get adjusted based upon both internal and external information. So if we would identify something internally where we had a risk, we would address that whether it is a technological fix, or education or process fix. We would do that. If an external pressure like HIPAA or HITECH would come by, we will of course gonna need to adjust where we at based upon additional information or additional requirements."*

Our review revealed a variety of ways in which organizations attempt to address and manage these privacy problems and threats (See Table 3). Our literature analysis distinguishes between different protection mechanisms ranging from technical, to physical, policies, training and awareness programs, and privacy impact assessment (PIS).

Technical Approach

As a reaction to data breaches, unauthorized data access or other threats, healthcare organizations react by developing technical measures (Chen et al. 2010; Ohno-Machado et al. 2004) or drafting policies (Mohan et al. 2004; Smith 1993). This reaction is usually driven by compliance to external pressures such as HIPAA and HITECH. 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.

Various technologies have been used to address health information privacy threats (See Table 3). The proposed mapping has been developed based on the literature review as well as interviews with privacy experts (See Figure 2). A conventional approach to addressing access issues as well as data use and disclosure is access control mechanisms. This approach focuses on designing access roles and policies to handle 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 it needs to balance between control to information and operational activities for healthcare providers (Lovis et al. 2007).

Privacy Threat	Matching Technical Countermeasure	MIS and Medical References
Data Collection	Anonymization	(Claerhout et al. 2005)
Use & Disclosure	Anonymization	(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)
	Cryptographic	(Quantin et al. 2000)
	Access Control	(Chen et al. 2010; Haas et al. 2011)
Unauthorized Access	Access Control Mechanism	(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; van der Linden et al. 2009)
	Encryption	(Kluge 2007)
	Anonymization	(Boyd et al. 2007; Neubauer et al. 2011)
Secondary Use	Anonymization	(Aberdeen et al. 2010; Neubauer et al. 2011)

Table 3. Mapping of Privacy Threat to Its Countermeasure

The extent and breadth of these technologies varies depending on the issue and the context. Several technologies have been used to achieve protecting patients' privacy 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).

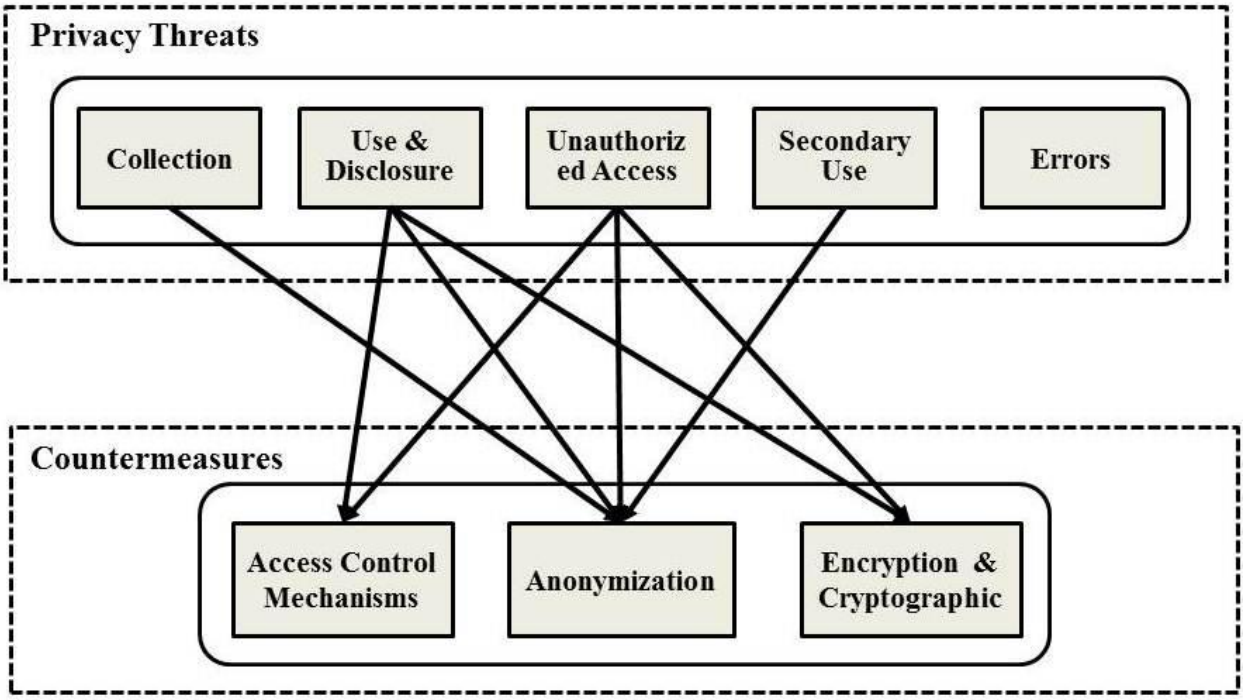

Figure 2. Mapping of Privacy Threats to Technical Countermeasures

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 faced with an external threat, and then the organization would react with formalized policies and interventions. Smith concluded with alternative approaches to incite better protective approaches from corporations to include 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).

Human Approach

Information privacy issues and threats cannot 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 enough because "breaches continue to occur, suggesting that existing compliance programs are not effective" (Culnan et al. 2009, p.678). With medical data disclosure being the second highest reported breaches (Hasan et al. 2006), privacy issues in healthcare sector is moving to the forefront. These worries of information security and privacy in healthcare have prompted the federal government to fund initiatives such as funding 3-year $17.3 million to develop state-level solutions to the privacy and security challenges (Miller et al. 2009) in order to transcend the dominating reactive approaches to privacy (Culnan et al. 2009). Though, a perfect privacy program does not exist, organizations can initiate a proactive attitude by creating a culture of privacy that involves buy-ins from the leaders (Culnan et al. 2009; Ishikawa 2000) and an ongoing commitment by all stakeholders to safeguard patient health information (Mohan et al. 2004) using a human-technology equation (Patel et al. 2000).

Education and training started emerging as an important tool because it provides awareness of potential risks and the organization's practices (Ishikawa 2000; Mohan et al. 2004). However, training sessions tend to be informational and 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 an appropriate and effective training.

Another proactive measure which has been mentioned in a limited number of papers is the privacy impact assessment (PIA). 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 new application is developed" (Culnan et al. 2009, p.684). Identifying a priori these key PIA leads to addressing potential privacy issues and threats (Croll 2010) and complying with fair information practices (Culnan et al. 2009).

Not only robust privacy programs are difficult and costly (Culnan et al. 2009) but also more challenging in healthcare. Healthcare organizations are expected to have safeguards in place against these threats (Liginlal et al. 2009) and thus a need of business model specific for the healthcare industry (Appari et al. 2010, p.281). Despite the consensus among multidisciplinary research reviews that research on privacy breaches and responses at the organizational level is under-researched (Appari et al. 2010; Culnan et al. 2009; Greenaway et al. 2005; Smith et al. 2011), there are limited theoretical guidelines on how organizations develop their responses to information privacy threats (Greenaway et al. 2005) and what 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).

Theme 4: Why Privacy Responses Matters?

What factors explain consumer privacy valuation? Several research has investigated individual behaviors through the concept of trust (Culnan et al. 1999; Malhotra et al. 2004) and how organizations are handling their information according to fair information practices (Culnan et al. 2009). Thus, 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, how organizations handle consumers information can mitigate the fears and concerns of their consumers. Therefore, the important question is what factors influence organization into how they respond to privacy issues and threats?

Despite interest in information privacy, the information privacy literature provide limited insights and explanations about factors explaining organizational responses and behaviors (Greenaway et al. 2005). Only a limited number of research provides a theoretical explanation of the measures undertaken by organizations (see Table 4). Three major themes are prevalent when considering the influencing factors: legitimacy (Agrawal et al. 2007; Greenaway et al. 2005; Neubauer et al. 2011), competitive advantage (Greenaway et al. 2005; Smith 2000); and moral and ethical considerations (Culnan et al. 2009; Kluge 2007; Mohan et al. 2004). A very limited number of researchers (Greenaway, 2005) combine more than one theme to provide a richer understanding of organizational responses.

Factors	MIS Literature	Medical Informatics
Legitimacy (Institutional Forces)	(Greenaway et al. 2005)	(Agarwal et al. 2007; Kluge 2007; Neubauer et al. 2011; Smith 2000)
Fair Information Practices	(Culnan et al. 2009; Greenaway et al. 2005; Smith 1993)	
Competitive Advantage	(Greenaway et al. 2005; Smith 1993)	(Smith 2000)
Moral/ ethical Considerations	(Culnan et al. 2009; Smith 1993; Stewart et al. 2002)	(Kluge 2007; Mohan et al. 2004)

Table 4. Summary of Drivers to Privacy Responses

Legitimacy and Institutional Forces

With regards to organizational responses to privacy, the institutional approach provides a great perspective of how organizations respond to external pressures (Greenaway et al. 2005). Institutional theory posits that organizations respond to institutional pressures and adopt behavioral and structural changes in order to achieve legitimacy (DiMaggio et al. 1983; Meyer et al. 1977).

An example of institutional pressures in healthcare is the regulatory environment which comprises many different regulations and rules. HIPAA and HITECH define the federal regulatory requirements for handling patients' privacy in U.S. (Appari et al. 2010; Neubauer et al. 2011). Prior research has used institutional theory in organizational research; however institutional theory has received only limited attention from MIS researchers (Mignerat et al. 2009; Orlikowski et al. 2001). Institutional theory seems to offer a lens to examine the regulatory effects on information technology management (Mishra et al. 2008) and information privacy in healthcare (Appari et al. 2009).

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 compliance being the major goal for organizations to protect patient PII, organizations are developing policies and processes that are in alignment with healthcare regulations, as one industry expert stated:

> "*We have to understand the legislation and will have to abide by the rules and then have an infrastructure to be able to do those things".*

While complying with healthcare regulation is inescapable in order to avoid penalties, organizations with a built-in culture for patients' privacy are embracing a proactive approach and have valued and invested in patient privacy before the enactment of HIPAA and HITECH, as stated by an industry expert:

> *"It is not like we did not care about information before, now all of the sudden the legislation make you compliant with this that is a poor assumption. So, we clearly value patient, health information security at the highest level".*

Competitive Advantage

Resource-Based View (RBV) has been explored as a theoretical explanation for organizations seeking competitive advantage through their privacy programs (Greenaway et al. 2005). Organizations investing in privacy programs can gain competitive advantage (Bowie et al. 2006; Smith 1993). In the light of HIPAA, healthcare organizations have to notify and report in the media data breaches. Such measures impact the reputation of the organization and potentially its competitive advantage as a healthcare CIO and HIPAA security officer explained:

> *"There is the business driver where you want to be viewed at, you want to be competitive, you need IT to be competitive, you need the safeguards to be competitive because if we have a breach, would you come here? No."*

Fair Information Practices

Fair information practices (FIPs) are a set of global standards which were originally developed by the US Department of Health, Education and Welfare (HEW 1973). In the context of information privacy, FIPs serve as guidance to organizations about responsible privacy behaviors (Smith 1993). In the United States, there is no omnibus law for organizations to adhere to FIPs, rather each domain adopted a sectoral approach (Culnan et al. 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 and responsibility over handling data collection and use (Greenaway et al. 2005).

Ethical Responsibility

Beyond legal compliance and legitimacy, organizations recognize the importance of moral responsibility and ethical considerations (Culnan et al. 2009; Mohan et al. 2004). Organizations that recognize moral and ethical

responsibilities will gain more buy-ins from their employees and customers (Culnan et al. 2009). In practice, ethics translates in having good business practices as a healthcare leader stated:

> *"Even if the regulations were not there, it may be a little bit more lacks because you won't have anything to refer back to, but as things change, you have to have best practicing, you have to have good practices… I mean you need to be efficient; you need to provide the best practice. Because eventually, somebody will ask for, somebody will know…. I think again is just best practice, is best practice. No matter where I have ever worked, is still always best practice".*

FUTURE RESEARCH AND CONCLUSION

Achieving privacy in healthcare is not a destination but a journey with a crucial mission of achieving the most appropriate balance between access to patient records and their right to privacy. The lack of appropriate privacy measures might cause economic harm or denied service from insurance or employers; while tight privacy can prevent care providers from accessing patient information in time to save lives. Our analysis of information privacy literature from MIS and health informatics perspective provided a grounded lens in the context of the challenging domain of healthcare. This study is not without limitations. In particular, our study suffered from limited journal selection and time frame covered.

Research to date shows a dominant reactive approach to privacy with high level solutions that do not address the operational aspects of privacy measures effectiveness. Having the technical safeguard and policies is not sufficient to protect against the threats of data breaches. A human-technical equation is needed and requires the establishment of legal, technical, social and ethical requirements for a prosperous e-health environment. These requirements and solutions have to be defined beyond a narrative way and must support the implementation and enforcement processes. Our contribution consists not only of identifying different privacy countermeasures but also in mapping the technical measures with the classified threats and thus identifying new areas for further development.

From a practical perspective, this study shows that institutional pressures and competitive advantage heavily influence how organizations respond and manage their information privacy responses. However, ethical, responsibilities and best practices remain key elements to cultivate a culture of privacy and favorably distinguish the operationalization of privacy practices, as stated by an industry expert:

> *"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"*

In conclusion, there are many competing claims about how EHRs and e-health in general impact the privacy of patients' medical information. This study contains the first significant study of the practical and theoretical causes and measures of privacy threats and vulnerabilities within its relevant industry and research community. These findings can contribute to more useful empirical studies in both MIS and health informatics disciplines. Applying reactive and proactive measures impact the business operation of healthcare delivery (Fernando et al. 2009) whose goal is to provide efficient care. Future research should focus on the impact of information privacy measures on operational aspects of privacy measures effectiveness as well as answering how and what tools can organizations use to test and measure that they achieve maximum privacy without impeding business operations.

Moreover, future research of healthcare information privacy should be more grounded in its context which would help support the theoretical explanations as well practitioners' responses and actions. The results of this study provide an important although limited snapshot of current research in information privacy. First the journal selection was based on academic journals mainly and thus might not be exhaustive, however we believe it was comprehensive. The second limitation is the time period. We used only a 10 year time span in the health informatics literature. Our future work will complement the results of this study by expanding the scope of both our IS and health informatics literature.

REFERENCES

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

Agarwal, R., Mishra, A., Angst, C., and Anderson, C. "Digitizing Healthcase: The Ability and Motivation of Physician Practices and Their Adoption of Electronic Health Record Systems," Proceedings of the 28th Annual International Conference on Information Systems (ICIS), Montreal, Canada, Paper 115, 2007.

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

Anderson, J.G. "Security of the Distributed Electronic Patient Record: A Case-Based Approach to Identifying Policy Issues," *International Journal of Medical Informatics* (60:2) 2000, pp 111-118.

Angst, C.M., and Agarwal, R. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2) 2009, pp 339-370.

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

Appari, A., Johnson, M.E., and Anthony, D.L. "HIPAA Compliance: An Institutional Theory Perspective," *AMCIS 2009 Proceedings*) 2009, p 252.

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

Blobel, B., Nordberg, R., Davis, J.M., and Pharow, P. "Modelling Privilege Management and Access Control," *International Journal of Medical Informatics* (75:8) 2006, pp 597-623.

Bowie, N.E., and Jamal, K. "Privacy Rights on the Internet: Self-Regulation or Government Regulation?," *Business Ethics Quarterly* (16:3) 2006, p 323.

Boyd, A.D., Hosner, C., Hunscher, D.A., Athey, B.D., Clauw, D.J., and Green, L.A. "An 'Honest Broker' Mechanism to Maintain Privacy for Patient Care and Academic Medical Research " *International Journal of Medical Informatics* (76:5-6) 2007, pp 407-411.

Bush, G.W. "Executive Order 13335: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator ", 2004,

Chen, K., Chang, Y.C., and Wang, D.W. "Aspect-Oriented Design and Implementation of Adaptable Access Control for Electronic Medical Records," *International Journal of Medical Informatics* (79:3) 2010, pp 181-203.

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

Claerhout, B., and DeMoor, G.J.E. "Privacy Protection for Clinical and Genomic Data:: The Use of Privacy-Enhancing Techniques in Medicine," *International Journal of Medical Informatics* (74:2-4) 2005, pp 257-265.

Croll, P.R. "Determining the Privacy Policy Deficiencies of Health ICT Applications Through Semi-Formal Modelling," *International Journal of Medical Informatics*) 2010.

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

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.

Culnan, M.J., and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1) 1999, pp 104-115.

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

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

Dinev, T., and Hart, P. "An Extended Privacy Calculus Model for E-commerce Transactions," *Information Systems Research* (17:1) 2006, p 61.

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

Garets, D., and Davis, M. "Electronic Medical Records vs. Electronic Health Records: Yes, There is a Difference," *A HIMSS Analytics White Paper, Chicago, IL: HIMSS Analytics, 2006, http://www.healthstik.com/downloads/WP_EMR_EHR.pdf*) 2006.

Garfinkel, R., Gopal, R., and Goes, P. "Privacy protection of binary confidential data against deterministic, stochastic, and insider threat," *Management Science* (48:6) 2002, pp 749-764.

Greenaway, K.E., and Chan, Y.E. "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6:6) 2005, pp 171-198.

Griesser, G.G. *Data Protection in Health Information Systems: Considerations and Guidelines.* North-Holland Publishing Company, Amsterdam, 1980.

Gürses, S., Rizk, R., and Günther, O. "Privacy Design in Online Social Networks: Learning from Privacy Breaches and Community Feedback," Proceedings of the 29th Annual International Conference on Information Systems (ICIS), Paris, France, Paper 90, 2008.

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., and Müller, G. "Aspects of Privacy for Electronic Health Records," *International Journal of Medical Informatics* (80:2) 2011, pp e26 – e31.

Hasan, R., and Yurcik, W. "A Statistical Analysis of Disclosed Storage Security Breaches," Proceedings of the Second ACM Workshop on Storage Security and Survivability (StorageSS), ACM, Alexandria, Virginia, USA, 2006, pp. 1-8.

Herath, T., and Rao, H.R. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2) 2009, pp 154-165.

HEW "Fair Information Practices. U.S. Dept. of Health, Education and Welfare. http://www.privacyrights.org/ar/fairinfo.htm,") 1973.

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

Ishikawa, K. "Health Data Use and Protection Policy; Based on Differences by Cultural and Social Environment," *International Journal of Medical Informatics* (60:2) 2000, pp 119-125.

Johns, G. "The Essential Impact of Context on Organizational Behavior," *Academy of management review* (31:2) 2006, pp 386-408.

Kluge, E.H.W. "Secure e-Health: Managing Risks to Patient Health Data," *International Journal of Medical Informatics* (76:5-6) 2007, pp 402-406.

Kotulic, A.G., and Clark, J.G. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5) 2004, pp 597-607.

Lasagna, L. "Hippocratic Oath--Modern Version," *Retrieved June* (30) 1964, p 2006.

Li, X.-B., and Sarkar, S. "Protecting Privacy Against Record Linkage Disclosure: A Bounded Swapping Approach for Numeric Data," *Information Systems Research*), June 14, 2010 2010a, p isre.1100.0289.

Li, X.B., and Sarkar, S. "Data Clustering and Micro-Perturbation for Privacy-Preserving Data Sharing and Analysis," ICIS 2010 Proceedings. , 2010b.

Liginlal, D., Sim, I., Khansa, L., and Fearn, P. "Human Error and Privacy Breaches in Healthcare Organizations: Causes and Management Strategies," Proceedings of Americas Conference on Information Systems (AMCIS), San Francisco, CA, USA, 2009, p. 406.

Lovis, C., Spahni, S., Cassoni, N., and Geissbuhler, A. "Comprehensive Management of the Access to the Electronic Patient Record: Towards Trans-Institutional Networks," *International Journal of Medical Informatics* (76:5-6) 2007, p 466.

Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns(IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4) 2004, pp 336-355.

Meyer, J.W., and Rowan, B. "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2) 1977, pp 340-363.

Mignerat, M., and Rivard, S. "Positioning the Institutional Perspective in Information Systems Research," *Journal of Information Technology* (24:4) 2009, pp 369-391.

Milberg, S.J., Burke, S.J., Smith, H.J., and Kallman, E.A. "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM* (38:12) 1995, pp 65-74.

Miller, A.R., and Tucker, C. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science* (55:7) 2009, pp 1077-1093.

Mishra, A.K. "Organizational responses to crisis," *Trust in organizations: Frontiers of theory and research*) 1996, pp 261-287.

Mishra, S., and Chin, A. "Assessing the Impact of Governmental Regulations on the IT Industry: A Neo Institutional Theory Perspective," *Computer security, privacy, and politics: current issues, challenges, and solutions*) 2008.

Mohan, J., and Razali Raja Yaacob, R. "The Malaysian Telehealth Flagship Application: a National Approach to Health Data Protection and Utilisation and Consumer Rights," *International Journal of Medical Informatics* (73:3) 2004, pp 217-227.

Neubauer, T., and Heurix, J. "A Methodology for the Pseudonymization of Medical Data," *International Journal of Medical Informatics* (80:3) 2011, pp 190-204.

Obama, B. "American Recovery and Reinvestment Act of 2009. Washington, DC. Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf,") 2009.

Ohno-Machado, L., Silveira, P.S.P., and Vinterbo, S. "Protecting Patient Privacy by Quantifiable Control of Disclosures in Disseminated Databases," *International Journal of Medical Informatics* (73:7-8) 2004, pp 599-606.

Orlikowski, W.J., and Barley, S.R. "Technology and institutions: What can research on information technology and research on organizations learn from each other?," *MIS quarterly* (25:2) 2001, pp 145-165.

Patel, V.L., Arocha, J.F., and Shortliffe, E.H. "Cognitive Models in Training Health Professionals to Protect Patients' Confidential Information," *International Journal of Medical Informatics* (60:2) 2000, pp 143-150.

Pear, R. "Privacy Issue Complicates Push to Link Medical Data " in: *The New York Times*, http://www.nytimes.com/2009/01/18/us/politics/18health.html?_r=1, 2009.

Peleg, M., Beimel, D., Dori, D., and Denekamp, Y. "Situation-Based Access Control: Privacy Management via Modeling of Patient Data Access Scenarios," *Journal of Biomedical Informatics* (41:6) 2008, pp 1028-1040.

Quantin, C., Allaert, F.A., and Dusserre, L. "Anonymous Statistical Methods Versus Cryptographic Methods in Epidemiology," *International Journal of Medical Informatics* (60:2) 2000, pp 177-183.

Ravera, L., Colombo, I., Tedeschi, M., and Ravera, A. "Security and Privacy at the Private Multispecialty Hospital Istituto Clinico Humanitas: Strategy and Reality," *International Journal of Medical Informatics* (73:3) 2004, p 321.

Reni, G., Molteni, M., Arlotti, S., and Pinciroli, F. "Chief Medical Officer Actions on Information Security in an Italian Rehabilitation Centre," *International Journal of Medical Informatics* (73:3) 2004, pp 271-279.

Sadan, B. "Patient Data Confidentiality and Patient Rights," *International Journal of Medical Informatics* (62:1) 2001, pp 41-49.

Sinclaire, J.K. "Current Research in Information Security and Privacy," *Information Systems Management* (2004) 2003, p 8.

Smith, H.J. "Privacy policies and practices: inside the organizational maze," *Communications of the ACM* (36:12) 1993, pp 104-122.

Smith, H.J. *Managing privacy: Information technology and corporate America* Univ of North Carolina Pr, 1994.

Smith, H.J. "Information privacy and its management," *MIS Quarterly Executive* (3:4) 2004, pp 201-213.

Smith, H.J., Milberg, J.S., and Burke, J.S. "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly* (20:2) 1996a, pp 167-196.

Smith, H.J., Milberg, S.J., and Burke, S.J. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2) 1996b, pp 167-196.

Smith, J. "Towards a Secure EPR: Cultural and Educational Issues," *International Journal of Medical Informatics* (60:2) 2000, pp 137-142.

Smith, J.H., Dinev, T., and Xu, H. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (forthcoming) 2011.

Solove, D.J. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3) 2006, p 477.

Stewart, K.A., and Segars, A.H. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1) 2002, p 36.

Straub, D.W., and Straub, W. "Effective IS Security," *Information Systems Research* (1:3) 1990, pp 255-276.

Strauss, A.L., and Corbin, J. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques. 3rd Ed. Newbury Park, CA: Sage.*, 2008.

Sujansky, W.V., Faus, S.A., Stone, E., and Brennan, P.F. "A Method to Implement Fine-Grained Access Control for Personal Health Records Through Standard Relational Database Queries," *Journal of Biomedical Informatics*) 2010.

Thatcher, M.E., and Clemons, E.K. "Managing the Costs of Informational Privacy: Pure Bundling as a Strategy in the Individual Health Insurance Market," *Journal of Management Information Systems* (17:2) 2000, pp 29-57.

Tong, Y., and Teo, H.H. "Migrating to Integrated Electronic Medical Record: An Empirical Investigation of Physicians' Use Preference," Proceedings of the 30th Annual International Conference on Information Systems (ICIS), Phoenix, AZ, Paper 37, 2009, p. 37.

Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (forthcoming) 2010.

van der Linden, H., Kalra, D., Hasman, A., and Talmon, J. "Inter-Organizational Future Proof EHR systems: A Review of the Security and Privacy Related Issues," *International Journal of Medical Informatics* (78:3) 2009, pp 141-160.

Westin, A.F. *Privacy and Freedom*, Atheneum: New York, 1967.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," Proceedings of the 29th Annual International Conference on Information Systems (ICIS), Paris, France, Paper 6, 2008a.

Xu, H., Irani, N., Zhu, S., and Xu, W. "Alleviating Parental Concerns for Children's Online Privacy: A Value Sensitive Design Investigation," ICIS 2008 Proceedings, 2008b.

Yeh, Q.J., and Chang, A.J.T. "Threats and Countermeasures for Information System Security: A Cross-Industry Study," *Information & Management* (44:5) 2007, pp 480-491.

Zwick, D., and Dholakia, N. "Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right," *Electronic Markets* (11:2) 2001, pp 116-120.