HIPAA Compliance: An Examination of Institutional and Market Forces[1,2]

Ajit Appari[*] (Ajit.Appari@Dartmouth.edu)
Denise L. Anthony[**] (Denise.L.Anthony@Dartmouth.edu)
M. Eric Johnson[***] (M.Eric.Johnson@Dartmouth.edu)

[*] Research Fellow – Center for Digital Strategies, Tuck School of Business, and Institute for Security, Technology, and Society at Dartmouth College, Hanover NH 03755
[***] Chair - Department of Sociology, and Research Director - Institute for Security, Technology, and Society, Dartmouth College, Hanover NH 03755
[**] Professor of Operations Management, and Director – Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover NH 03755

Abstract

One would think that the enactment of the HIPAA, with its mandates on data security and privacy, would have brought a major shift in the security management practices within the US healthcare. Unfortunately, recent industry reports indicate low levels of regulatory compliance, thus raising security concerns for the US health IT infrastructure. This research develops a regulatory compliance model by drawing insights from the institutional theory literature to identify the key drivers influencing HIPAA compliance, both institutional and market forces (e.g., variability in state-level privacy laws comprehensiveness, interdependency between privacy and security rules, pressure from compliance leaders in the region, compliance officer's functional background, and the consumer concern for privacy). We validate the model using a national sample of acute-care hospitals and find partial support. The primary contribution of this research lies in the novel application of institutional theory to explain the variability in regulatory compliance prevalent in the US healthcare sector.

Keywords: Information Privacy, Information Security, HIPAA Compliance, Institutional Theory

The 8th Workshop on Economics of Information Systems (WEIS 2009), University College London, England, 24-25 June 2009

1. This research was supported through the Institute for Security, Technology, and Society at Dartmouth College, under awards 60NANB6D6130 from the U.S. Department of Commerce and U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001. The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the National Institute of Standards and Technology (NIST), the U.S. Department of Commerce, or U.S. Department of Homeland Security.

2. We acknowledge the Health Information and Management Systems Society Foundation for sharing the 2003 annual survey data on the state of HIPAA implementation among US hospitals.

HIPAA Compliance: An Examination of Institutional and Market Forces

1 Introduction

The Health Insurance Portability and Accountability Act (HIPAA) [1] was enacted in 1996 with the intent of leveraging information technology (IT) to reduce costs, improve quality, and ensure portability and continuity of health insurance coverage (OCR 2006)[2]. An implication of the growing dependence on IT to manage health information is the increased information security and privacy concerns. Recent anecdotal evidence suggests that a lack of adequate security measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish, and possible social stigma (Health Privacy Project 2007). Moreover, over 75% of consumers who use health websites are wary of those web sites sharing their information for secondary purposes without their permission (Raman 2007). The US Congress, foreseeing precisely such concerns, incorporated provisions of Privacy Rules and Security Rules as part of HIPAA (Hoffman and Podgurski 2006). Yet, studies of publicly reported data breaches show that medical data disclosure is the second highest breach category (e.g. Hasan and Yurcik 2006).

Managing information security risks is a "balancing act between maintaining security and not inhibiting the business." As customers and business partners demand greater levels of security the investments in information security have moved from "reactive add-ons to proactive initiatives that are aligned with the company's strategic goals" (Johnson and Goetz 2007). An extensive body of research has drawn attention to the technical, behavioral, process, and policy issues concerning information security and privacy, yet relatively little has been focused on the unique managerial, regulatory, and policy challenges found in healthcare (Appari and Johnson 2009). HIPAA and associated mandates on data portability, security, and privacy have brought a major shift in management policies and IT investments across healthcare organizations. Unfortunately, recent industry reports suggest low level of HIPAA compliance related to data portability, security, and privacy among US hospitals (AHIMA 2006). From a policy perspective, we lack a systematic investigation of such phenomenon, especially a rigorous and well-grounded empirical study (Kotulic and Clark 2004). More importantly, the lack of compliance could reflect a lackluster state of cyber security in healthcare organizations. Furthermore, while HIPAA imposes an overarching regulatory mandate, healthcare organizations are also expected to meet state-level privacy regulations, which often vary significantly between states creating confusion (Langenderfer and Cook 2004).

The purpose of this research is to investigate the variability in firm-level information privacy and security behavior among US hospitals in response to enactment of HIPAA. Greenway and Chan (2005), in their exposition of firms' information privacy behavior, contend that information security research could leverage socio-organizational theory, such as institutional theory

[1] HIPAA regulation is applicable to 'covered entities' including hospitals, hospice, clinics, insurance, payer organizations, employers, regional health information organizations who manage patient information in electronic form. In this study, we focus only on acute care hospitals.

[2] Recent studies show that the adoption of IT is having significant impact on care quality improvement (see Garg et al. 2005). However, IT spending in healthcare, trails many other industries, typically 3-5% of revenue - far behind industries like financial services where closer to 10% is the norm (Bartels 2006).

(DiMaggio and Powell 1983, Meyer and Rowan 1977), to frame inquiries. In this research we build a regulatory compliance model by drawing insights from literature on institutional theory. In particular, our focus is to identify the key drivers of hospitals' compliance to HIPAA regulation in terms of several institutional and market forces that may influence the dynamics of hospitals' adoption of information privacy and security safeguards (e.g. coercive pressure arising from mix of state and federal privacy regulations, mimetic pressure arising from compliance leaders in the region, and market pressure arising from consumer demand for privacy).

The primary contribution this research lies in novel application of institutional theory to explain variability in regulatory compliance prevalent in US healthcare sector. More specifically, our findings offer insights on the major drivers influencing the current state of cyber security behavior in healthcare as measured by hospitals' HIPAA compliance. Moreover, we expect our findings may inform policy decisions, particularly in reference to HIPAA compliance.

The rest of this paper is structured as follows. First we briefly review past research on information security and privacy in healthcare Next we present our theoretical model and the research methods applied to validate the model. We also present preliminary summary statistics and describe our plans to test our theoretical model. Finally we conclude with remarks on limitations and future steps for this research.

2 Information Security in Healthcare

2.1 Background

The healthcare sector is experiencing a tectonic shift in the enablement of care services through IT -in particular, the internet and mobile technologies such as remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access, and asset tracking (Kalorama 2007). Increasing adoption of IT systems, though beneficial in terms of improving productivity and service quality, also raises major concerns for information security threats. In the internet age, security risks to health information could arise from various sources including accidental disclosure, data breach by insider, data breach by outsider with physical intrusion and/or intrusion of network system (NRC 1997; Rindfleisch 1997). Moreover, healthcare organizations, striving to become HIPAA compliant, face significant challenges in meeting regulatory norms (Choi, et al. 2006). As personal health information is digitized, transmitted and mined for effective care provision, new forms of threat to patients' privacy are becoming evident (Mercury 2004). For example, recent empirical research studying the growing trend of "data hemorrhages" demonstrates the resulting vulnerability and security threats to health sector, specifically financial risks to firms and medical risks to patients (Johnson 2009), highlighting the need to "enact better monitoring and information controls to detect and stop leaks." (p. 18).

Information security and privacy issues have been brought to the forefront of managements' attention with the enactment of the HIPAA, which set compliance dates for Privacy Rules (April 2003), and for Security Rules (April 2005). The security standard released under HIPAA specifies five categories of security measures including administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information; organizational requirements governing contractual agreements; and policies, procedures and documentation governing overall information security policy management (NIST 2005). Despite the time since the regulations became active, recent industry surveys present a

bleak picture of HIPAA compliance status among US hospitals. According to a recent survey of about 1100+ hospitals and health systems in the 2006, only 39% are fully compliant with privacy regulation, and 25% are fully compliant with security regulation (AHIMA 2006).

Compliance with HIPAA is not only a technological issue; it also requires effective organizational change management by institutionalizing new structures and processes to maintain and protect sensitive data (Huston, 2001). Silverman (2008) note "regulatory compliance and its enforcement produce an ever-changing environment […] *and* organizations struggle to understand and manage within this maelstrom of rules and regulations." (p. 33) HIPAA compliance requires organizations to relentlessly assess their internal controls across all business units and functional areas, including data security (Huston, 2001), real time availability (Peterson et. al., 2005), encryption and authentication techniques (Chao, et al. 2005), network communications (Huston, 2001), and disaster recovery techniques (Dynes 2009). Additionally, organizations must maintain audit trails which are subject to external evaluation (Peterson et al., 2005), implement adequate privacy policies and appropriate controls at all data access points to maintain data integrity (Mercuri, 2004).

2.2 Information Privacy Behavior in Health Service Providers

Recently Warkentin et al. (2006) undertook a study to characterize the compliance behavior among administrative staff and medical staff of public as well private-sector healthcare facilities. The authors observed that healthcare professionals at public hospitals have higher self efficacy, i.e. belief in their capability to safeguard and protect patient's information privacy, compared to their counterparts in private healthcare facilities. Further, on average, administrative staff exhibited higher self efficacy than medical staff across both public and private healthcare facilities. Moreover, the behavioral intent of healthcare professionals, including medical and administrative staff, was positively correlated to self efficacy and perceived organizational support. Another set of studies show that healthcare workers are highly concerned about maintaining accuracy of patient records, unauthorized access to patient data, and believe that patient data should not be used for unrelated purposes except for medical research (Baumer, et al. 2000; Earp and Peyton 2006).

Of course, patients' health information plays a major role in conducting medical research. The maelstrom of privacy regulations and rules directed toward health information has had some adverse effects on the conduct of medical research (e.g. Kaiser 2006). In a nationwide web-based survey of epidemiologists Ness (2007) report that nearly 68% of researchers perceived that HIPAA has made medical research highly difficult and only about 25% believed that it has increased patients' confidentiality or privacy. More importantly, about 39% of researchers believed HIPAA had increased research cost by a great deal, especially due to additional compliance related administrative cost, and over 50% of researchers believed HIPAA enforcement lead to delays in research. In a critical review of three cases of health research projects, Shen et al. (2006) report that several factors including the complexity of consent forms and privacy protection forms, and time consuming procedures often get in the way of patient recruitment. This adverse view of HIPAA is also reflected in lower adoption rate of health information systems such as EMR bolstering the perception that privacy laws may actually have negative effect on the ulterior goals of providing quality care at low cost. Recently, Miller and Tucker (2007), in a study of US hospitals, found that state-level privacy regulations are indeed moving away the hospitals from adopting interoperable EMR systems.

2.3 Information Privacy Behavior in Healthcare Consumers

A growing body of research examines key drivers of privacy and security concerns among patients, especially in the context of electronic health information (Bansal, et al. 2007; Campbell, et al. 2007). Bansal et al. (2007) developed a set of constructs based on utility theory and prospect theory as antecedents of trust formation and privacy concern that impact users' personal disposition to disclose their health information to online health services websites. In particular, this study reported that user's current health status, personality traits, culture, and prior experience with websites and online privacy invasions play a major role in user's trust in the health website and their degree of privacy concerns. Campbell, et al (2007), in a mail based survey with adult patients in England, found that about 28% to 35% of patients are neutral to their health information – such as age, gender, ethnicity, reason for treatment, medical history, personal habits impacting health, type of treatment obtained, side effects of treatment – being used by physicians for other purpose. Only about 5–21% of patients expected to be asked for permission to use their information by their physicians. Similarly only about 10% of the patients expected to be asked for permission for a wide variety of purposes including, combining data with other patients' data to provide better information to future patients, sharing how the treatment is working with other physicians in the hospital, teaching medical professionals, and writing research articles about diseases and treatments.

Perceptions of privacy and security vary depending on the technology involved in managing health information as well their own background. Recent empirical evidence suggest that patients' privacy and security concern increased with the level of technology(e.g. relative security and privacy concern for networked PHR is twice that of memory device based PHR, technologically advanced PHR systems are favored by highly educated patients (Angst, et al. 2006)).

3 Theoretical Background and Research Model

Institutional theory posits that organizations respond to normative pressures arising from both their external and internal business environments and adopt structures and practices that are socially accepted as appropriate organizational choices and considered legitimate by other organizations in their fields (DiMaggio and Powell 1983, Meyer and Rowan 1977; Zucker 1987). More precisely, these pressures could be classified into three archetypes that lead organizations to isomorphism, namely (a) *coercive pressure* that stems from political power exerted by the state; (b) *mimetic pressure* that arise from the need to respond to uncertainty, often by copying successful competitors; and (c) *normative pressure* which arise from the norms embedded in the profession (DiMaggio and Powell 1983). Although the overarching construct for institutional theory is isomorphism, it by no means suggests that organizations would not differ in their strategic responses to institutional forces in accordance with their contextual needs. Oliver (1991) suggests while organizations may acquiesce to the demands of institutional environment, they may as well choose to avoid, compromise, defy, and manipulate the institutional environment.

The legal environment for organizations is a prime example of institutional pressure where "law appears as a system of substantive edicts, invoking societal authority over various aspects of organizational life" (Edelman, and Suchman 1997: p. 483). In recent years the legal environment has become more pervasive, demanding significant structural changes, especially from the

information management perspective (e.g., increasing governmental intervention in the form of regulations such as Sarbanes Oxley Act and HIPAA). These regulatory forces from the institutional environment could lead to the standardization of processes, practices and IT assets to show conformity and gain legitimacy (Zucker 1987). Research focused on the healthcare industry has used the institutional framework extensively to study the impact of various regulations in shaping hospital management (e.g. Covaleski, et al. 1993). Similarly, a growing body of IS research has exploited institutional theory, both in conceptual and empirical work, to study issues like organizational consequences of IT (Robey and Boudreau 1999) adoption challenges of enterprise information systems (Gosain 2004; Benders, et al. 2006), diffusion of Software Engineering Institute's Capability Maturity Model (CMM®) for managing software development (Adler 2005), and globalization of IT innovation (King, et al. 1994).

Recent industry surveys show a lack of full compliance to HIPAA among US hospitals (e.g., AHIMA 2006). Björck (2004) argues that, because effective information security depends on social behavior of organizations and their employees, institutional theory may offer a new lens of rigor to examine the dynamics of information security management in the healthcare. Moreover, he expresses surprise in noting that "almost no theories concerned with social behavior - which is exactly what the management of IS/IT security is about - have found their way into managerial IS/IT security research. (p. 3)" In a similar vein, Mishra and Chen (2008) argue in favor of applying institutional theory to examine regulatory effects on information technology management, since over a over a period of time the presence of strong institutional forces homogenizes the overall response of organizations that operate within a similar industry. In concurrence with these scholars and recognizing the need to understand the underlying dynamics of HIPAA compliance among US hospitals we next present our research model building on institutional theory. In particular, we are interested in examining the effect of various institutional and market forces operating in the healthcare industry on compliance behavior of hospitals.

3.1 Effect of Institutional Pressures on Regulatory Compliance

Research examining organizational behavior grounded on institutional theory use three types of institutional pressure, namely coercive, mimetic, and normative operating on firms. In this section, we identify sources of these pressures that may influence HIPAA compliance initiatives within hospitals and present our hypotheses.

State-level Privacy Regulations as Source of Coercive Pressure:

The healthcare sector in the US is considered one of the most regulated industries (Walshe and Shortell 2004). The regulations, especially with provisions for enforcement actions against violators, act as 'implicit general deterrence' (Gunningham, et al. 2005). Prior research has also found that the 'explicit general deterrence' arising from enforcement actions taken on violators to be a key coercive factor in increasing regulatory compliance (Thornton, et al. 2005). At the federal level, the HIPAA regulation lays out a broad set of specifications for Privacy, and

Security rules, stipulating punitive actions for compliance failure[3]. Since the enactment of HIPAA, numerous complaints have been filed by consumers. However, rarely have any punitive actions been taken against hospitals (LA Times 2008) [4]. This is perhaps because the industry is in early stage of implementing the regulation and hospitals still need guidance on appropriate interpretation of regulatory requirements. Nevertheless, the mere threat of legal sanctions against privacy violations may act as deterrence to hospitals and ensure that management undertakes adequate safeguards to protect themselves from possible violations (Braithwaite and Makkai 1991).

As such HIPAA defines the floor of regulatory requirements for personal health information (PHI) and allows state laws to override it with more stringent ones. This creates additional pressures on health providers to institutionalize HIPAA compliant systems. Following HIPAA, several states have enacted their own laws to regulate transfer and management of health information which are substantially different. Indeed the variability in this patchwork of state-level and federal regulations are so significant (Hodge 1999; Langenderfer and Cook 2004) that scholars consider it be a major impediment to healthcare organizations' ability to comply with regulations as well as to the adoption of health IT such as EMR systems. Many have called for the creation of uniform standards (Cunningham 2000; Hodge 1999, 2000; Gostin, et al. 2001). Despite this variability in state laws, we expect to observe positive effect of state-level regulations, especially in states that have more comprehensive set of regulations encompassing different dimensions of PHI privacy. This is particularly because health providers in such states will face less uncertainty in terms of developing HIPAA compliant systems compared to other states where absence of comprehensive laws places the health providers in precarious situations. Therefore we hypothesize that

> H1: *Hospitals located in the states with more comprehensive regulations for PHI will exhibit a higher tendency to become HIPAA compliant.*

Because of variability in state-level information regulations, when providers treat patients from other states, they are expected to meet the norms of multiple states while resolving consent and disclosure requirements across states. In a policy study across eleven states, one recent project shows that for non-emergency treatments, states like Indiana, Utah, Wisconsin, and Oklahoma require the fewest instances of consent, whereas New York and Minnesota require the maximum instances of consents (Prescott and Stone 2009). Therefore hospitals who are treating a relatively high proportion of out-of-state patients may find it difficult to deploy effective privacy and security policies.

> H2: *Hospitals located in states with higher patient inflow (i.e., out-of-state patients) will exhibit a lower tendency to become HIPAA compliant.*

[3] In general, for any willful violation of patient's privacy, health care provider could face penalty of $50,000 and/or one year imprisonment. And if such violations are carried out with intent to harm the patient or making profit, provider could face penalty of $250,000 and/or 10 years imprisonment.

[4] Office for Civil Rights has received about 34,000 complaints for privacy violations, among which 26% of the cases led to formal investigations and the rest were dismissed (Los Angeles Times April 2008).

Regulatory Interdependency as Source of Coercive Pressure:

The privacy and security rules of HIPAA are closely intertwined and designed to be compatible with each other; however they differ in their interdependence (Fedorowicz and Ray 2004). The security rule governs control of physical access to data, internal audit, security breach mitigation procedures and security risk management process, whereas the privacy rule deals with patients' rights and preferences regarding use and disclosure of their personal health information. Electronically stored information can be secured by deploying necessary technology safeguards (without being private). However, it cannot be made private without security safeguards (Fedorowicz and Ray 2004). Thus, the coercive pressure arising from this interdependency of privacy and security regulation may influence the compliance initiatives of hospitals, even though security compliance was not mandated until two years after privacy compliance. In particular, we expect hospitals that are undertaking security compliance in tandem with privacy compliance will have achieved higher level of privacy compliance. Therefore, we posit that:

> H3: *Hospitals with a higher compliance to privacy (security) rules will exhibit a higher tendency to become security (privacy) rules compliant.*

Regional Compliance Leaders as Source of Mimetic Pressure:

In the situations of poor clarity of organizational technologies, goals, or even the institutional environment, organizations tend to mold themselves on other organizations that have dealt with such uncertainty successfully (DiMaggio and Powel 1983; March and Olsen 1976). For example, Miller and Tucker (2007) find empirical evidence for higher propensity to adopt an EMR system in a state with no privacy law with increased installed base of such systems across hospitals in that state compared to states with privacy laws. Likewise, Oliver (1991) argues that acquiescence by imitating successful peers to gain organizational legitimacy is a common strategic response to regulatory pressure. Greenway and Chan (2005: p 181), building on institutional theory, proposed that "firms with compliance perspective [approach] on information privacy will adopt privacy behaviors that demonstrably conform to industry norms." We contend that in a state with a higher compliant base (i.e. higher proportion of hospitals already compliant), there will be higher pressure for other hospitals to conform. Therefore, we posit that

> H4: *Hospitals located in a state with a higher HIPAA compliant base will exhibit a higher tendency to become HIPAA compliant.*

EMR Adoption Intensity as Source of Mimetic Pressure:

EMR systems enhance the management of patient information through controlled and auditable data access processes and improve data security (Agrawal 2002). These systems could support hospitals in conducting both intra and inter organizational transactions based on standardized data formats, as well as enhance the hospitals' ability to coordinate with accreditation and regulatory agencies by sharing analysis of patient data (Chaiken 2003). Furthermore, data on patients from EMR systems could be aggregated, after applying de-identifying protocols, into larger data repositories for secondary purposes such as research to improve patient safety, public health, and enhance medical knowledge (Aspen, et al. 2003). Hospitals located in states with a higher installed base face higher pressure to adopt EMR systems (Miller and Tucker 2008). This external force, in turn, promotes HIPAA compliance among such hospitals. Overall, we expect

the implementation of EMR systems would have positive influence on a hospital's ability to comply with HIPAA rules. Thus we hypothesize:

> H5: *Hospitals located in a state with a higher EMR installed based will exhibit a higher tendency to become HIPAA compliant.*

External Consultants as Source of Normative Pressure:

Normative pressure stems from the cultural expectation that agents feel compelled to honor, often because they are rooted in professional affiliations, including educational background, professional networks, and consultant arrangements (DiMaggio and Powell 1983). In the healthcare sector, the patient-physician relationship is based on the Hippocratic principle and every physician operates within that norm while ensuring patient's privacy. The evolution of the health care sector and its increasingly complex underlying structure, however, has shifted the onus of patient privacy and confidentiality from physicians to multiple organizations who participate in health care service provision. This may create additional pressure to hire external consultants, especially in the context of HIPAA, when there is a high degree of uncertainty associated with interpretation of regulations and organizations' lack adequate in-house resources. Organizations often use external consultants to implement enterprise-wide change management projects, such as the deployment of enterprise information systems Consultants bring industry norms to practice, based on their experience with multiple organizations (Gosain 2004) and act as facilitators of "organizational learning" (Massey and Walker 1999). Management consultancy has been shown to effect organizational transformation in non-profit organizations (Irvine 2007). Hence, we propose:

> H6: *Hospitals employing external consultants will exhibit a higher tendency to become HIPAA compliant*.

Professional Background of Compliance Officers as Source of Normative Pressure

HIPAA, as part of its administrative safeguards, requires appointment of a security and privacy officer to provide organizational oversight on a firm's information security and privacy effort (Choi, et al. 2006). According to recent industry reports, a significant number hospitals are deputizing executives from other functional areas, including finance, quality, and operations, with responsibilities of chief compliance officers (HCCA 2002; 2008). Such dual roles may have a compromising effect on hospitals' compliance initiatives, because the functional background of decision making agents often defines their cognitive base and affects social behavior (DiMaggio and Powell 1983). Decision making agents in organizations of similar educational and professional background tend to view problems in similar fashion, and see policies, procedures, and structures through the same normatively sanctioned lens. In particular, compliance professionals act as social filters interpreting regulatory norms based on their professional background and experience (i.e. functional conditioning (Chattopadhyay, et al 1999) and transmit them into the organizational routines). For executives with primary responsibilities of other core organizational functions compliance becomes a secondary task, and concerns about law subsume under concerns about productivity, profit, market share. Therefore, we posit that:

> H7: *Hospitals employing dedicated officer with a compliance background will exhibit a higher tendency to become HIPAA compliant*.

3.2 Effect of Market Forces on Regulatory Compliance

D'Aunno, et al. (2000) emphasize that the framing of regulatory compliance should be viewed from both institutional forces and market forces, as strategic response of organizations depends on their contextual interpretations. In particular, the relative size of an organization to its competition and consumer demand plays a significant role.

Consumer Concern for Information Privacy

Despite HIPAA's mandated privacy requirements, consumers continue to be anxious about the privacy of their personal health information. The California Healthcare Foundation, in a recent survey, reported that over two-thirds of consumers are concerned about the privacy of their electronic medical records; just over half of consumers believe they are obligated to share health information to advance healthcare; and public disclosure of data breaches has further heightened privacy concerns among consumers (CHCF 2005). Additionally, the survey reports that, among the consumers who recognize benefits of implementing electronic medical records, about 42% believe their records are more potentially unsafe (unlike the 34% who believe paper records are under threat). Organizations in regulated industries, often strive to maintain the trust of local communities, avoid attention of consumer groups, and preserve the company's reputation as a socially responsible entity (Gunningham, et al. 2005). Furthermore, prior research on compliance to environmental regulations have shown that customer demand, especially of firm's environmental policies and practices to assess potential environmental impact, play an important role in improving compliance behavior in addition to other market pressures such as the intensity of competition (Darnall, et al. 2006; Delams and Toffel 2007).

Several studies find significant differences in privacy preferences across gender, geographical regions, and culture (Bellman, et al. 2002; Pedersen and Frances 1990; Varian, et al. 2003; 2005). In particular, Pedersen and Frances (1990) and Varian, et al (2005) observed significant differences in privacy preferences among American consumers residing in various geographical regions. Consequently, it could be argued that hospitals' strategic choices of implementing HIPAA compliant processes and safeguards could vary across states as a result of the variability in consumer demand for privacy. This leads us to hypothesize that:

> H8: *Hospitals located in states with higher consumer concerns for privacy will exhibit a higher tendency to become HIPAA compliant.*

Relative Size to competitors:

Regulatory requirements often have a discriminatory impact on small firms (Baron and Baron 1980). Government regulation forces firms of varying sizes to take the same compliance measures. As a result, an undue burden is placed on the small firm in meeting the same standards of a large firm. Though limited, there are empirical studies that infer compliance costs are generally regressive in nature and do not scale with firm size. In particular, for smaller firms the compliance cost could pose excessive burden and may exceed the potential benefits from regulation (Eldridge and Kealey, 2005) and often forces firms to go private (Engel et al. 2007). The larger firms, unlike smaller firms, tend to have more financial resources and manpower, and enjoy economies of scale (Weidenbaum 1979). As a result, they have the discretionary power to

allocate more resources to implement the necessary policies and safeguards to comply with regulatory requirements. Hence, we hypothesize:

> H9: *Within a state, relatively large hospitals will exhibit a higher tendency to become HIPAA compliant.*

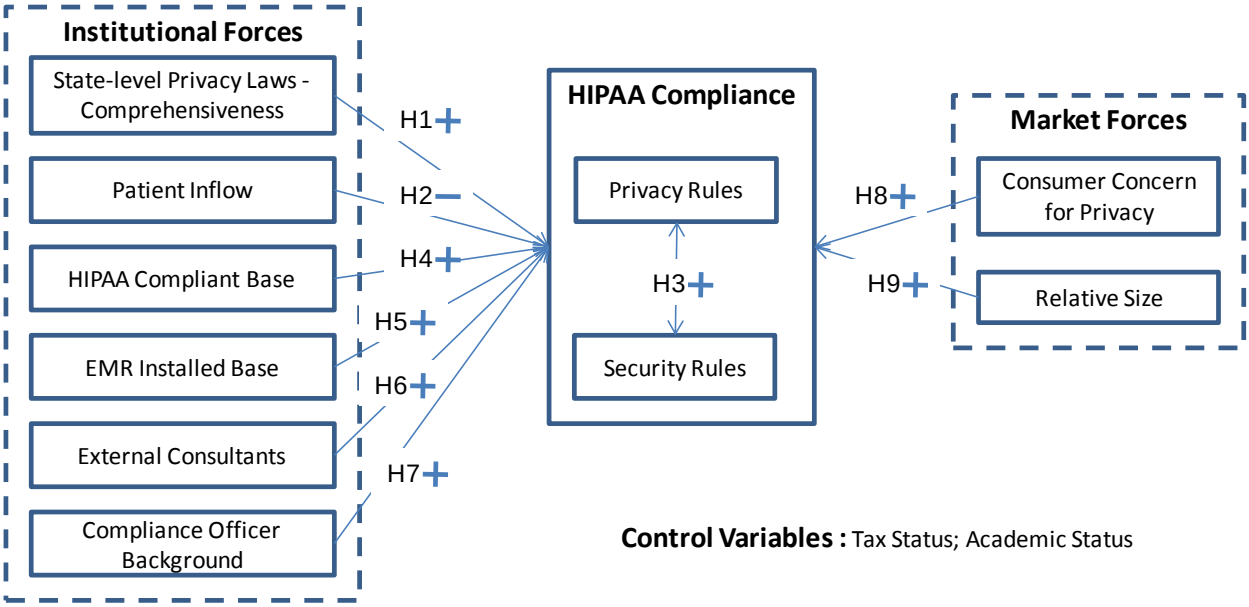

Figure 1: Regulatory Compliance Model for Acute Care Hospitals

Figure 1 summarizes our research model. Prior research in health IT (e.g., Burke et al. 2002; Hikmet et al. 2008), and organizational behavior literature (e.g., Kimberly and Evanisko 1981; Damanpour 1987) have considered tax status, and academic as being salient. Following this literature, we use the tax status and the academic status of hospitals as control variables. In addition, the costs for implementing HIPAA compliant policies, processes, and technology safeguards could be significant and vary across hospitals (Kilbridge 2003). To account for the potential effect of the financial resources, we also control for the HIPAA compliance budget allocated by hospital management. Next we introduce the research method adopted for this empirical investigation.

4 Data and Research Methods

The data on hospitals for this study was obtained from the Dorenfest® Institute, which is a research division of the Health Information and Management Systems Society (HIMSS) Analytics. Our data is a subset of survey conducted in 2003, and contains information for over 4000 hospitals on several dimensions including self-reported level of compliance to HIPAA privacy, and security rules, hiring of HIPAA consultant, hospital bed size[5], tax status, academic

[5] Though prior studies generally use bed size of hospitals from American Hospital Association (AHA) database, we rely on the self reported accuracy of hospitals surveyed by HIMSS. We believe that any discrepancy between these two databases on hospital bed size may wash out as we focus on relative size of the hospital as a measure for one of the market force.

status, and geographical location. The HIMSS dataset was available in an MS Access database format. We wrote several SQL queries to extract necessary raw data for the research purpose. Following other studies in HIT literature, we include hospitals with at least 100 beds (Miller and Tucker 2007). This led to a reduce sample of about 2700+ hospitals. Subsequently, we removed all of the hospitals that had missing observations on any of the hospital related research variables considered in this study. This led to our final sample of 1564 hospitals from 797 integrated health delivery systems for statistical analysis. However, to compute state-level metrics such as EMR installed base, HIPAA compliant base, We use hospital as the unit of analysis.

4.1 Operationalization

Dependent Variables: The HIPAA compliance is measured along two dimensions Privacy rules, and Security rules as ordered variables on a scale of 0-3, with 0 being <50%, 1 being 50-75%, 2 being 75-99%, and 3 being 100% compliant.

Independent Variables: To operationalize the 's*tate-level privacy laws comprehensiveness*' we first code existence of state statutes on ten privacy related dimensions – patients' access privilege, denial to access, right to amend, disclosure restriction for hospitals, doctor-patient privilege, and confidentiality of special conditions including birth defects, cancer, genetic tests, mental health and HIV/STD status. Each dimension is coded as 1 if a regulation exists and 0 otherwise based on the compilation of state privacy laws in Pritts, et al. (2003). The linear sum of these ten dimensions represents state-level privacy laws comprehensiveness. To avoid scale effect we normalize this linear sum by dividing it with 10 (i.e. maximum number of dimensions). The '*patient inflow*' is measured based on the Net Flow Ratios of Medicare spending in the focal state by all hospitals vis-à-vis Medicare expenditure for all patients of the focal state. The net flow ratios are published at CMS website. According to Martin, et al. (2007) net flow ratio higher than 1 indicates patients from the focal state have consumed health care services out of state as well (i.e. patient outflow), and lower than 1 indicates out-of-state patients have consumed services in the focal state (i.e. patient inflow). Since our focus is to measure the patient inflow, first we take the inverse of these ratios so that values higher than 1 would indicate patient inflow and then we allocate '0' to all states that has ratio value <=1 and retain the ratio value as it if greater than 1. This gave us 26 states experiencing patient inflow. Then we obtain the 1st, 2nd, and 3rd quartile of patient inflow ratio for these 26 states and coded them into four groups based on these quartile values. Thus the variable '*patient inflow*' is an ordered variable with 0 being no inflow, 1 being low, 2 being medium, 3 being high and 4 being very high inflow rate. The '*HIPAA compliant base*' is measured for both privacy rules and security rules separately as the proportion of hospitals reporting 100% compliance in a state to privacy, and security rules respectively. The '*EMR installed base*' is computed as the proportion of hospitals that have computerized patient record system installed in the focal state.

The '*external consultants*' is coded as 1 if a consultant has been hired by the focal hospital/ hospital system and 0 otherwise. The '*compliance officer* background' is coded as 1 if the compliance officer has no other functional role in the organization such as CEO, CFO, COO, director of quality management, director of risk management, etc., otherwise 0. In cases where individual hospital do not have compliance officer but only at the hospital system level, we apply same rule at hospital system level and transfer the value to member hospitals. However it should be noted that the acceptable title of compliance officer could be different such as chief compliance officer, SVP corporate compliance, chief compliance/legal officer, HIPAA program

manager, HIPAA officer, compliance/privacy officer among others. The '*relative size*' of a hospital is measured as the hospital's bed size to average bed size of hospitals in the state of focal hospital. Lastly, the variable '*consumer concern for privacy*' is measured at state-level by a proxy, for the lack relevant data in HIMSS database, the average proportion of consumers registered for Do-Not-Call list as reported in Varian, et al. (2005).

Control Variables: The '*tax status*' of a hospital is coded as 1 if it is for-profit and 0 otherwise. Similarly, '*academic status*' of a hospital is coded as 1 if it is academic and 0 otherwise.

4.2 Descriptive Statistics

Table 1A shows distribution of hospitals reporting various levels of compliance for HIPAA privacy and security rules. Among all hospitals 64% and 19% report full compliance to privacy and security rules respectively; 26% and 43% report compliance of 76-99% for privacy and security rules respectively suggesting they are in compliance with most of the requirements. Among the academic hospitals, 77% and 28% report full compliance with privacy and security rules respectively. Whereas among for-profit hospitals 86% and 6% report full compliance to privacy and security rules respectively. On a comparative basis it is surprise to see that in our sample hospitals for-profit hospitals report consistently better than academic hospitals on privacy rule compliance levels. Whereas, in case of security rule higher proportion of academic hospitals are fully compliant than for-profit hospitals, and for-profit hospitals perform better than academic hospitals on lower level of compliance. Table 1B shows summary statistics for variables that are measured at state level across. .

The privacy laws comprehensiveness score varies from 0.3 to 1.0 suggesting some states having fewer privacy related statutes, however mean value of 0.74 indicates encouraging signs that on average states have enacted comprehensive set of privacy statutes. The average patient inflow is 1.056 indicating states that serve out-of-state patients, tend to incur about 5.6% of healthcare spending on out-of-state patients. The 'privacy concerns among consumers' varies significantly across states with average of 37% (standard deviation 9%) and ranges from a minimum of 14% to maximum of 54%. The privacy compliance base, security compliance base, and EMR installed base is computed based on the initial sample to ensure that we capture as much information as available in the sample. On average 45% of hospitals in each state are fully compliant to privacy rules. However the dispersion of privacy compliance base is very large and ranges from 7% to as high as 93% suggesting privacy compliance is not uniform across states. Similarly, on average 12% of hospitals are in full compliance with security rules. While security compliance base ranges from 0% to 67% indicating there are some states where none of the hospitals are security compliant. However, observing that the enforcement date for security rules was still two years away (i.e. April 2005 compared to survey year 2003) this poor state of security compliance is not surprising. For our sample, the EMR installed is fairly high suggesting on average 54% of hospitals in a focal state have EMR system installed. However the dispersion of EMR installed base quite high and ranges from 27% to 83%. Table 1C shows spearman rank correlation matrix for all variables. Though, many of the predictor variables are correlated, the strength of correlation ($\rho < 0.4$) is weak enough to safely ignore.

4.3 Results and Discussion

To test the research model, we used probit regression approach and two separate regressions with privacy rule compliance level and security rule compliance level as dependent variables. As most of the model variables are correlated (see Table 1C), we adjust for error and ran robust Logit models (Agresti 2002). Table 2 reports Probit regression coefficients and robust standard errors of estimated coefficients.

State-level Privacy Laws Comprehensiveness: the beta coefficient is positive and statistically significant for the case of compliance to privacy rule (0.466; $p<0.05$) and for the case of security compliance the coefficient is negative and insignificant (-0.265), indicating partial support for hypothesis H1. This suggests that hospitals are more likely to be privacy compliant in states that have more comprehensive privacy laws, whereas compliance to security rules is unaffected by the level of regulatory comprehensiveness.

Patient Inflow: the beta coefficient is negative and statistically significant for privacy rule compliance (-0.059; $p<0.05$), but positive and statistically insignificant for security rule compliance (0.021) indicating partial support to hypothesis H2. This result does support our argument that when patients from other states are getting healthcare, the focal hospital has to struggle through the complex web of privacy rules from multiple states to ensure regulatory norms, and in doing so may become prone to noncompliance.

Regulatory Interdependency: the beta coefficients are positive and statistically significant for security rule compliance (0.41; $p<0.01$), and privacy rule compliance (0.489; $p<0.01$) when viewed as a source of pressure on compliance to privacy rules and security rules respectively. This offers a strong support to hypothesis H3 suggesting compliance to both privacy and security rules go hand-in-hand.

HIPAA Compliant Base: the beta coefficients are positive and statistically significant for privacy compliance base (1.696; $p<0.01$), and security compliance base (2.477; $p<0.01$) when viewed as a source of coercive pressure on compliance to privacy rules and security rules respectively. Indeed the magnitude of these coefficients are largest compared to coefficients of any other institutional forces and market forces. Thus peer pressure is acting as dominant force on hospitals to achieve HIPAA compliance.

EMR System Installed Base: the beta coefficients for EMR installed base are statistically not significant for both privacy rule compliance (-0.255) and security rule compliance (0.493) indicating lack of support for hypothesis H5. Further we observe that while the sign of coefficient changes between privacy and security rule compliance, the standard error of estimate is same 0.322 in both cases. As such, we do not infer any special meaning behind the opposite signs of coefficients as they are statistically not significant.

External Consultant: while the beta coefficient is negative and statistically significant for privacy rule compliance (-0.575; $p<0.01$), it is negative and statistically insignificant for security rule compliance (-0.104). The negative of the coefficients are opposite to the hypothesized direction of effect in H6. Conventionally, external experts on regulation are beneficial especially

if the regulations are new and organization does not have adequate knowledge resources. In this light, perhaps most of the hospitals that have hired external consultants are yet to be compliant.

Compliance Officer Background: the beta coefficients are statistically significant, though is positive for privacy rule compliance (0.345; $p<0.01$), and negative for security rule compliance (-0.211; $p<0.01$). This shows that compliance to privacy rules is more likely to be aggressive if compliance officers do not have other functional roles as their responsibility. However the divergence of functional role appears to be a facilitator in security compliance.

Consumer Concern for Privacy: the coefficients are not statistically significant indicating lack of support for hypothesis H8.

Relative Size: the coefficient is positive and statistically significant only for security rule compliance (0.153, $p <0.01$), suggesting that larger hospitals are more likely to be security compliant. Whereas, insignificant coefficient for privacy rule compliance suggest hospitals of all sizes are equally likely to be privacy compliant.

Besides these core model variables, among the control variables, we find statistically significant coefficients for academic hospitals in privacy compliance model (0.457. $p<0.01$), suggesting they are more likely to be privacy compliant, and the coefficient for for-profit hospitals are statistically significant in both privacy compliance (0.73. $p<0.01$) and security compliance models (0.175. $p<0.01$). In summary we find partial support for our hypotheses.

5 Conclusion

Although industry surveys conducted post enforcement dates of HIPAA rules suggest low level of full compliance among US hospitals (AHIMA 2006), industry experts agree that "adhering to the HIPAA Privacy and Security rules are more than just about compliance, they make sound business sense" (Computer World 2001). To enhance our understanding on hospitals' compliance behavior, we developed a research model grounded in institutional theory. The study find partial support for the compliance model offering important insight on which type of pressure factors have statistically significant effect on HIPAA compliance in the acute care hospitals. In particular, privacy compliance level is positively influenced by the comprehensiveness of state-level privacy regulations, current security compliance level (i.e. interdependency factor), functional background of compliance officer, and HIPAA privacy compliant base in the state. Further, patient inflow from neighboring state affects negatively thus acting as a barrier to achieve higher privacy compliance. The security compliance is positively influenced by current level of privacy compliance, HIPAA security compliance base in the state. However, contrary to expectation the functional background of compliance is negatively associated with security compliance level. In addition, academic hospitals and for-profit hospitals tend to have higher level of compliance with HIPAA privacy and security rules.

This research, being first of its kind, has several limitations that future research may address. First, the data is somewhat older and comes from early period of HIPAA enforcement. Though using such data may help in characterizing the early adoption of HIPAA compliant practices,

future research must replicate this investigation with more recent compliance data and by incorporating confounding factors that may shed light on HIPAA compliance. Moreover, longitudinal data could be more valuable in offering better insight to dynamics of HIPAA compliance among US hospitals. Second, in this study we considered comprehensiveness of privacy laws at state-level, however the real issue appears to be the divergence in disclosure consent requirements for different parts of electronic health records. Future study may include complexity of EHR disclosure consent and examine its effect on HIPAA compliance. Despite these limitations, this research opens up new venues for research in the broader area of information security in health care. For example, HIPAA compliance requires significant investments on technology implementation, training and awareness, compliance personnel, policy formulation and revision, and period audits among others. Future research may examine strategic posture adopted by hospitals in achieving and sustaining HIPAA compliance. Moreover, impact of HIPAA compliance on hospital performance such as financial performance, efficiency, customer satisfaction and care quality could be other fruitful research areas.

Table 1A: Percentage distribution of hospitals with reference to reported HIPAA compliance level

Compliance Level	Overall (1564 hospitals)		Academic (192 hospitals)		For Profit (285 hospitals)	
	Privacy	Security	Privacy	Security	Privacy	Security
<50%	1	15	1	18	0	1
50 - 75%	9	23	4	23	1	14
76 - 99%	26	43	18	31	13	79
100%	64	19	77	28	86	6

Table 1B: Summary statistics of variables measured at State-level (50 states + DC)

Variables	Mean	Std. Dev.	Minimum	Maximum
Privacy Laws Comprehensiveness	0.74	0.15	0.3	1.0
Patient Inflow[1]	1.056	0.115	1.001	1.592
Privacy Compliance Base[2]	45%	18%	7%	93%
Security Compliance Base[2]	12%	13%	0%	67%
EMR Installed Base[2]	54%	13%	27%	83%
Privacy Concern	37%	9%	14%	54%

1 This statistic is bade on Medicare spending for hospitals [source Martin, et al. 2007)
2 These statistics are based on the initial sample of 2707 hospitals with bed size of 100 or more. We use the initial sample to capture all the information possible to compute the base metric. However the ordered probit regression is conducted using final sample of 1564 hospitals.

Table 1C: Spearman rank correlation matrix

	Variables	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]
[1]	Privacy Rules Compliance	1.00												
[2]	Security Rules Compliance	**0.31**	1.00											
[3]	Privacy Compliance Base	**0.19**	**0.05**	1.00										
[4]	Security Compliance Base	**0.10**	**0.18**	**0.33**	1.00									
[5]	EMR Installed Base	-0.03	**0.05**	**-0.15**	**0.13**	1.00								
[6]	State-level Privacy Laws Comprehensiveness	**-0.04**	0.02	**-0.16**	-0.03	-0.03	1.00							
[7]	Patient Inflow	0.02	0.01	**0.11**	**0.24**	0.01	**-0.14**	1.00						
[8]	Privacy Concern	**0.07**	0.03	**0.21**	**0.24**	**-0.11**	**0.09**	**0.23**	1.00					
[9]	Compliance Official Background	**0.13**	**-0.05**	**0.04**	-0.02	**-0.04**	**-0.05**	**-0.05**	0.00	1.00				
[10]	Relative Size	**0.08**	**0.05**	**0.03**	-0.01	0.00	0.01	0.02	0.00	**0.11**	1.00			
[11]	External Consultant	**-0.28**	**-0.13**	**-0.05**	-0.03	0.04	0.03	-0.04	**-0.06**	**-0.07**	-0.01	1.00		
[12]	Academic Status	**0.10**	0.02	0.01	**0.13**	**0.05**	0.01	0.02	**0.05**	**0.06**	**0.25**	-0.02	1.00	
[13]	Profit Status	**0.22**	**0.11**	**0.12**	**-0.23**	**-0.06**	**-0.11**	**-0.12**	**-0.09**	-0.02	**-0.14**	**-0.16**	**-0.14**	1.00

Note: Bold values are statistically significant correlation coefficients with p <0.05

Table 2: Ordered probit regression (robust error) results for privacy rules and security rules compliance

Note: The shaded cell show support for hypothesized relationships

Model Variables	Privacy Rules Compliance Level	Security Rules Compliance Level
State-level Privacy Laws Comprehensiveness	0.466** (0.239)	-0.265 (0.201)
Patient Inflow (Medicare)	-0.059** (0.024)	0.021 (0.023)
Privacy Compliance Level	NA	0.489*** (0.040)
Security Compliance Level	0.410*** (0.035)	NA
Privacy Compliance Base	1.696*** (0.290)	NA
Security Compliance Base	NA	2.477*** (0.383)
EMR Installed Base	-0.255 (0.322)	0.493 (0.322)
External Consultant	-0.575*** (0.072)	-0.104 (0.067)
Compliance Officer Background	0.345*** (0.066)	-0.211*** (0.057)
Consumer Concern for Privacy	0.352 (0.363)	-0.278 (0.351)
Relative Size of Hospital	0.062 (0.059)	0.153*** (0.048)
Is Academic Hospital	0.457*** (0.120)	-0.150 (0.102)
Tax Status [Profit = Yes]	0.730*** (0.099)	0.175*** (0.061)
/cut1	-0.348 (0.351)	0.891 (0.314)
/cut2	0.853 (0.330)	1.684 (0.316)
/cut3	1.957 (0.333)	2.99 (0.320)
Number of Observations	1564	1564
Wald Chi2(11)	370.65	349.58
Log Pseudo Likelihood Ratio	-1208.83	-1907.19
Pseudo R2	0.1472	0.0643

*** p <0.01, ** p<0.05, * p<0.10 NA: Not Applicable

References

1. Adler, P.S. (2005) "The Evolving Object of Software Development," *Organization* 12(3)
2. Agrawal, A. (2002). "Return on Investment Analysis for a Computer-based Patient Record in the Outpatient Clinic Setting," *Journal of the Association for Academic Minority Physicians* 13, p 61
3. AHIMA – The American Health Information Management Association. (2006). "The State of HIPAA Privacy and Security Compliance," last accessed on Nov. 2008, http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf
4. Angst, C.M., Agrawal, R., and Downing, J. 2006. "An Empirical Examination of the Importance of Defining the PHR for Research and for Practice," working paper
5. Appari, A., and Johnson, M.E. (2009) "Information Security and Privacy in Healthcare: Current State of Research," forthcoming in *International Journal of Internet and Enterprise Management*
6. Aspden, P., Corrigan, J.M., Wolcott, J., and Erickson, S. M. (2003). *Patient Safety: Achieving a New Standard for Care*. Washington, DC: National Academies Press
7. Bansal, G., Zaheid, F.,M., and Gefen, D. 2007. "The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online," *AMCIS*, Keystone, CO.
8. Baron, B.R., and Baron, P. 1980. "A Regulatory Compliance Model," *Journal of Contemporary Business* 9(2), pp 139-150.
9. Bartels, A. 2006. "US IT Spending Benchmarks for 2006," Forrester Research Report.
10. Baumer, D. L., Earp, J. B., and Payton, F. C. 2000. "Privacy of medical records: IT implications of HIPAA", *ACM Computers and Society* (30:4), pp 40–47.
11. Bellman, S., Johnson, E.J., Kobrin, S.J., and Lohse, G.L. (2002) "Regional Differences in Privacy Preferences: Implications for the Globalization of Electronic Commerce," working paper, Columbia University
12. Benders, J., Batenberg, R. and Blonk, H. (2006) "Sticking to Standards; Technical and other Isomorphic Pressures in Deploying ERP-Systems," *Information & Management* (43:2), pp 124
13. Björck, F. (2004) "Institutional Theory: A New Perspective for Research into IS/IT Security in Organizations," *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Hawaii
14. Braithwaite, J. and Makkai, T. 1991. "Testing and Expected Utility Model of Corporate Deterrence," *Law & Society Review* 25(1), pp 7-40.
15. Burke DE, Wang BBL, Wan TTH, Diana ML (2002) Exploring hospitals' adoption of information technology. J Med Syst 26 (4):349–355
16. Campbell, B., Thomson, H., Slater, J., Coward, C., Wyatt, K., and Sweeney, K. 2007. "Extracting Information from Hospital Records: What Patients Think About Consent," *Quality and Safety in Healthcare* (16:6), pp 404–408
17. Chaiken, B. P. (2003) "Clinical ROI: Not Just Costs Versus Benefits," *Journal of Healthcare Information Management* (17:4), pp 36-41
18. Chao, H., Twu, S., and Hsu, C. (200*5) "A Patient-Identity Security* Mechanism for Electronic Medical Records during Transit and at Rest," *Medical Informatics and the Internet in Medicine (30: 3), pp 227* – 240
19. CHCF – California HealthCare Foundation (2005), "National Consumer Health Privacy Survey 2005: Executive Summary," available at http://www.chcf.org/topics/view.cfm?itemID=115694

20. Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. 2006. "Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules," *Journal of Medical Systems*, (30:1), pp57–64.
21. Computer World, May 2001. "Beware of Predatory HIPAA Consultants," last accessed on 11/27/2008 at http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,60250,00.html
22. Covaleski, M.A., Dirsmith, M.W., and Michelman, J.E. (1993) "An Institutional Theory Perspective on the DRG Framework, Case-Mix Accounting Systems and Healthcare Organizations," *Accounting, Organization and Society* (18:1), pp 65 – 80
23. Cunnigham, E. (2000) "Old Before Its Time : HIPAA and eHealth," *Health Affairs* (19:6), pp 231 - 238
24. D'Aunno, T., Succi, M. and Alexander, J.A. (2000) "The Role of Institutional and Market Forces in Divergent Organizational Change," *Administrative Science Quarterly* (45), pp. 679-703
25. Damanpour F (1987) The adoption of technological, administrative, and ancillary innovations: impact of organizational factors. J Manage 13(4):675–688
26. Darnall N., Jolley G.J., and Ytterhus B. (2006) "Understanding the Relationship between a Facility's Environmental and Financial Performance," Johnstone N. (ed.) *Environmental Policy and Corporate Behaviour*, Northampton, MA: Edward Elgar Publishing, in association with Organisation for Economic Co-Operation and Development (OECD), Paris
27. Delmas, M. and Toffel, M.W. (2007) "Organizational Responses to Environmental Demands: Opening the Black Box. Strategic Management Journal, Forthcoming; HBS Technology & Operations Mgt. Unit Research Paper No. 07-022. Available at SSRN: http://ssrn.com/abstract=994893
28. DiMaggio, P.J. and Powell, W.W. (1983) "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", *American Sociological Review*, (48), pp. 147-160.
29. Dynes, S. (2009) "Emergent Risks in Critical Infrastructure," in Papa, M. and Shenoi, S. (Eds.) *Critical Infrastructure Protection II*, Springer, pp 3 -16
30. Earp, J.B., and Payton, F.C. 2006. "Information Privacy in Service Sector: An Exploratory Study of Health Care and Banking Professionals," *Journal of Organizational Computing and Electronic Commerce* (16:2), pp 105-122.
31. Edelman, L.B. and Suchman, M.C. 1997. "The Legal Environments of Organizations," *Annual Review of Sociology* 23, pp 479-515.
32. Eldridge, S., and B. Kealey. 2005. SOX Costs: Auditor attestation under Section 404,
33. Eldridge, S.W. and Kealey, B.T. (2005) "SOX Costs: Auditor Attestation under Section 404," Available at SSRN: http://ssrn.com/abstract=743285
34. Engel, E., Hayes, R.M., and Wang, X. (2007) The Sarbanes–Oxley Act and Firms' Going-Private Decisions," *Journal of Accounting and Economics* (44:1-2), pp. 116 – 145
35. Engel, E., R.M. Hayes, and X. Wang. 2007. The Sarbanes-Oxley Act and firms' going private decisions. *Journal of Accounting and Economics* (forthcoming)
36. Fedorowicz,
37. Garg, AX, Adhikari NK, McDonald H, Rosas-Arellano MP, Devereaux PJ, Beyene J, Sam J, Haynes RB. 2005. "Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review," *JAMA* (293:10), pp. 1261-1263.
38. Gosain, S. (2004) "Enterprise Information Systems as Objects and Carriers of Institutional Forces: The Iron Cage Revisited," *Journal of AIS* (5:4), pp 151 - 182

39. Gostin, L.O., Hodge, J.G., Valdiserri, R.O. (2001) "Informational Privacy and the Public's Health: The Model State Public Privacy Act," *American Journal of Public Health* (91:9), pp 1388-1392
40. Greenway, K.E., and Chan, Y.E. (2005) "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of AIS* (6:6), pp 171 – 198
41. Gunningham, N.A., Thornton, D., and Kagan, R.A. (2005) "Motivating Management: Corporate Compliance in Environmental Protection," *Law & Policy* (27), pp. 289 – 316
42. Hasan, R., and Yurcik, W. 2006. "A Statistical Analysis of Disclosed Storage Security Breaches," *ACM workshop on Storage security and survivability*.
43. HCCA – Health Care Compliance Association (2002) "5th Annual Survey: 2002 Profile of Healthcare Compliance Officers," http://www.hcca-info.org
44. HCCA – Health Care Compliance Association (2008) "10th Annual Survey: 2002 Profile of Healthcare Compliance Officers," http://www.hcca-info.org
45. Health Privacy Project 2007. "Health Privacy Stories," http://www.healthprivacy.org
46. Hikmet, N., Bhattacharjee, A., Menachemi, N., Kayhan, V.O., Brooks, R. 2008. The role of organizational factors in the adoption of healthcare information technology in Florida hospitals," Health Care Management Science (11), pp. 1-9
47. Hodge, J.G. Jr. (1999) "The Intersection of Federal Health Information Privacy and State Administrative Law: The Protection of Individual Health Data and Workers' Compensation," Administrative Law Review (51), pp 118 – 144
48. Hodge, J.G. Jr. (2000) "National Health Information Privacy and New Federalism," *Notre Dame Journal of Law, Ethics & Public Policy* (14:791)
49. Hoffman, S., and Podgurski, A. 2006. "In Sickness, Health and Cyberspace: Protecting the Security of Electronic Private Health Information," http://ssrn.com/abstract=931069
50. Hosmer, D.W., and Lemeshow, S. 2000. *Applied Logistic Regression, 2nd edn.* Wiley, NJ
51. Hsu, Chiung-Wen (2004). "Possibility and Impossibility for Global Online Privacy: A Cross-Country Examination" Paper presented at the annual meeting of the International Communication Association, New Orleans Sheraton, New Orleans, LA, May 27,
52. Huston, T. (2001) "Security Issues for Implementation of E-Medical Records." *Communications of the ACM* (44: 9)
53. Irvine, H. J. (2007) "Corporate Creep: An institutional View of Consultancies in a Non-Profit Organization," *Australian Accounting Review* (17:1), pp 13 – 25
54. Johnson, M.E. (2009) "Data Hemorrhages in the Healthcare Sector," *Financial Cryptography and Data Security*, Thirteenth International Conference, February 23-26, 2009
55. Johnson, M.E., and Goetz, E. "Embedding Information Security into the Organization," *IEEE Security & Privacy Magazine* (5:3), pp 16 – 24
56. Kaiser, J. (2006) "Patient Privacy: Rule to Protect Records may Doom Long-Term Heart Study," *Science*, vol.311, no.5767, pp 1547-1548.
57. Kalorama Information (a division of MarketResearch.com) 2007. "Wireless Opportunities in Healthcare".
58. Kimberly, J.K., Evanisko M.J. 1981. "Organizational innovation: the influence of individual, organizational, and contextual factors on hospital adoption of technological and administrative innovation," *Academy of Management* J 24(4):689–713
59. King, J. L., Gurbaxani, V., Kraemer, K. L., McFarlan, F. W., Raman, K. S., and Yap, C. S. (1994). "Institutional factors in information technology innovation." *Information Systems Research* 5(2), 139-169.

60. Kotulic, A.G., Clark, J.G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* 41, pp 597-607.
61. LA Times. April 2008. "Effectiveness of medical privacy law is questioned," last accessed on 11/27/08 http://articles.latimes.com/2008/apr/09/nation/na-privacy9
62. Langenderfer, J., and Cook, D.L. (2004) "Oh, What a Tangled Web We Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance," *Journal of Business Research* (57), pp 734 – 747
63. March, J.G. and Olsen, J.P. (1976) *Ambiguity and Choice in Organizations*, Bergen, Norway
64. Massey, C. and Walker, R. (1999) "Aiming for Organizational Learning: Consultants as Agents of Change", *The Learning Organization* (6:1), pp 38 – 44
65. Mercuri, R.T. 2004. "The HIPAA-potamus in Health Care Data Security," *Communications of the ACM* (47:7).
66. Meyer, J.W. and Rowan, B. (1977) "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony", *American Journal of Sociology* (83:2), pp. 340-363.
67. Miller, A.R., and Tucker, C.E. 2007. "Privacy, Network Effects and Electronic Medical Record Technology Adoption," *Proceedings of WEIS*, Carnegie Mellon University.
68. Ness, R.B. 2007. "Influence of the HIPAA Privacy Rule on Health Research," *Journal of American Medical Association* (298:18), pp 2164-2170
69. NIST – National Institute of Standards and Technology. 2005. "An Introductory Resource Guide for Implementing the Health Information Portability and Accountability ACT (HIPAA) Security Rule," NIST Special publication 800-66.
70. NRC – The National Research Council 1997. *For the Record: Protecting Electronic Health Information*
71. OCR – The Office of Civil Rights 2006. HIPAA Administrative Simplification Regulation Text, last accessed on Nov. 2008 http://www.hhs.gov/ocr/AdminSimpRegText.pdf
72. Oliver, C. (1991) "Strategic Responses to Institutional Processes", *Academy of Management Review*, (16), pp. 145-179.
73. Pedersen, D.M., and Frances, S. (1990) "Regional Differences in Privacy Preferences" *Psychological Reports* (66), pp 731 – 736
74. Peterson, Z. and Burns, R. (2005) "Ext3cow: A Time-Shifting File System for Regulatory Compliance," *ACM Transactions on Storage* (1:2), pp. 190-212
75. Raman, A. 2007. "Enforcing Privacy through Security in Remote Patient Monitoring Ecosystems," *6th International Special Topic Conference on Information Technology Applications in Biomedicine.*
76. Rindfleisch, T.C. 1997. "Privacy, Information Technology, and Health Care," *Communications of the ACM*, (40:8), pp 93 – 100.
77. Robey, D., Boudreau, M.C. (1999) "Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications," *Information Systems Research* (10:2), pp 167 – 185
78. Shen, J.J., Samson, L.F., Washington, E.L., Johnson, P., Edwards, C., Malone, A. 2006. "Barriers of HIPAA Regulation to Implementation of Health Services Research," *Journal of Medical Systems* (30:1), pp 65
79. Thornton, D., Gunningham, N.A., and Kagan, R.A. (2005) "General Deterrence and Corporate Environmental Behavior," *Law & Policy* (27), pp. 262 – 88
80. Varian, H.R., Woroch, G. and Wallenburg, F. (2005) "The Demographics of the Do-Not-Call List," *IEEE Security and Privacy* (3:1), pp 34 – 39

81. Walshe, K., and Shortell, S.M. (2004) "Social Regulation of Healthcare Organizations in the United States: Developing a Framework for Evaluation," *Health Services Management Research* (17:2), pp 79 – 99
82. Warkentin, M., Johnston, A.C. and Adams, A.M. 2006. "User Interaction with Healthcare Information Systems: Do Healthcare Professionals Want to Comply with HIPAA?" AMCIS 2005
83. Weidenbaum, M.L. 1979. *The Future of Business Regulation* Amacom, NY.
84. Wu, F., and Lee, Y. (2005) "Determinants of eCommunication Adoption: The Internal Push versus External Pull Factors," *Marketing Theory* (5:1), pp 7 – 31
85. Zucker, L.G. (1987) "Institutional Theories of Organizations," Annual Review of Sociology (13), pp 443 – 464