2009

# HIPAA Compliance: An Institutional Theory Perspective

Ajit Appari
*Dartmouth College*, ajit.appari@tuck.dartmouth.edu

M. Eric Johnson
*Dartmouth College*, m.eric.johnson@tuck.dartmouth.edu

Denise L. Anthony
*Dartmouth College*, denise.l.anthony@dartmouth.edu

# HIPAA Compliance: An Institutional Theory Perspective

**Ajit Appari**
Dartmouth College
Ajit.Appari@tuck.Dartmouth.Edu

**M. Eric Johnson**
Dartmouth College
M.Eric.Johnson@tuck.Dartmouth.Edu

**Denise L. Anthony**
Dartmouth College
Denise.L.Anthony@Dartmouth.Edu

## ABSTRACT

One would think that the enactment of the HIPAA and associated mandates on data security and privacy has brought a major shift in the information security management practices across the US healthcare sector. Unfortunately, recent industry reports indicate substantially low level of regulatory compliance, thus raising security concerns to US health IT infrastructure. This research develops a regulatory compliance model by drawing insights from institutional theory literature to identify the key drivers influencing compliance, both institutional and market forces - e.g. mix of state and federal privacy regulations, pressure from compliance leaders in the region, and the consumer demand for privacy among others. 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 Security and Privacy, HIPAA Compliance, Institutional Theory.

## INTRODUCTION

The Health Information Interoperability and Accountability Act (HIPAA) of 1996 was enacted with the intent of leveraging information technology (IT) to reduce costs, improve quality, and ensure portability and continuity of health insurance coverage. An implication of the growing dependence on IT to manage health information is the increased information security and privacy risks. In fact, recent studies of publicly reported data breaches show that medical data disclosure is the second highest (e.g. Hasan and Yurcik 2006) and such breaches have exposed patients to economic threats, mental anguish, and even social stigma (Health Privacy Project 2007). It is no surprise that over 75% of consumers who use health websites are wary of these websites sharing their personal information for secondary purposes without 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).

Managing information security risks is a "balancing act between maintaining security and not inhibiting the business," that demands proactive information security investments strategies (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 of health information, yet relatively little has been focused on the unique managerial, regulatory, and policy challenges found in healthcare (Appari and Johnson 2009). Though, HIPAA and associated mandates on data security, and privacy have brought a major shift in the security management practices within the US healthcare. Recent industry reports (e.g. AHIMA 2006), unfortunately, suggest low level of compliance to HIPAA security and privacy rules among US hospitals reflecting a lackluster state of cyber security in healthcare organizations. From a policy perspective, we lack systematic investigation of such aberration, especially a rigorous and well-grounded empirical research (Kotulic and Clark 2004).

The purpose of this research is to investigate the variability of HIPAA compliance among US hospitals. Greenway and Chan (2005), in their exposition of firms' response to information security and privacy issues, contend that information security research could leverage socio-organizational theory, e.g. institutional theory (DiMaggio and Powell 1983, Meyer and Rowan 1977), to frame inquiries. Similarly, D'Arcy and Hovav (2009) advocate application of institutional theory to study the relationship between organizational characteristics and security best practices. In this research we build a regulatory compliance model, drawing insights from institutional theory literature, to identify the key drivers of HIPAA compliance among US hospitals in terms of several institutional and market forces, e.g. coercive pressure arising from state-level

regulations, mimetic pressure arising from compliance leaders in the state, and market pressure arising from consumers' privacy concern among others.

The primary contribution of this research lies in the novel application of institutional theory to explain variability in regulatory compliance prevalent in the US healthcare sector. In particular, our findings could offer insights on the major drivers influencing the current state of cyber security behavior in the healthcare as measured by hospitals' HIPAA compliance. Moreover, we expect our findings may inform policy decisions to promote HIPAA compliance. The rest of the paper is structured as follows. First we briefly review past research on information security and privacy in healthcare. Next we present a regulatory compliance model based on institutional theory, and the methodology. Finally we conclude with our remarks on limitations and future steps for this research.

## LITERATURE REVIEW

The privacy and security rules of HIPAA became effective from April 2003, and April 2005 respectively. While the privacy rules provide overarching norms for ensuring confidentiality of PHI, the security rules specifies series of security safeguards including administrative, physical, and technical safeguards for electronic PHI, and policies, procedures & documentation requirements governing overall information security management (NIST 2005). Clearly, HIPAA compliance 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). In fact, "regulatory compliance and its enforcement produce an ever-changing environment […] and organizations struggle to understand and manage within this maelstrom of rules and regulations (Silverman 2008:p. 33)." Over the past two decades an extensive body of research has developed addressing information security and privacy in healthcare, a comprehensive review of such literature could be found elsewhere (e.g. see Appari and Johnson 2009). In this section we briefly examine some of the more recent research in the information security and privacy in healthcare.

### Information security in healthcare

Healthcare organizations, pursuing to become HIPAA compliant, face significant security and privacy challenges in meeting the regulatory norms (Choi, et al. 2006). 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). As personal health information is being 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 significant 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).

HIPAA compliance entails 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 controls at all data access points to maintain data integrity (Mercuri, 2004).

### Information Privacy Behavior in Health Service Providers

Regulatory mandate has made HIPAA compliance a business necessity in healthcare industry. Recent study of compliance behavior show that the 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 (Warkentin et al. 2006). Further, on average, administrative staff exhibit higher self-efficacy than medical staff across both public and private hospitals. Moreover, the behavioral intent of healthcare professionals was positively correlated to self efficacy and perceived organizational support. However, healthcare professionals 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). Furthermore, Anoton, et al (2007) reports that privacy policy documents published after HIPAA enactment by organizations on their websites, though, are more descriptive, they have become less reliable, difficult to comprehend and pose greater burden on consumers.

The maelstrom of privacy regulations directed toward health information tends to have 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 leads 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) found that state-level privacy regulations are actually inhibiting adoption of interoperable EMR systems in the US.

### Information Privacy Concerns of 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) presents and examines 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 reports that user's trust in the health website and their degree of privacy concerns are influenced by several factors including their current health status, personality traits, culture, and prior experience with websites and online privacy invasions. 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. Whereas, only about 10-12% of the patients expected to be asked for permission to use their information for different 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.

Patients' perception of privacy and security could 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).

## RESEARCH MODEL OF REGLUATORY COMPLIANCE

The institutional theory posits that organizations respond to pressures arising from both their external and internal business environments and adopt structures and practices that are 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 guide organizations toward isomorphism, namely (a) *coercive pressure* stemming from political power exerted by state; (b) *mimetic pressure* arising from the need to copy successful competitors in the uncertain environment; 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 isomorphic behavior, it by no means suggests that organizations would not differ in their strategic responses to institutional forces. 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). Organizations are facing ever increasing regulatory interventions (e.g., Sarbanes Oxley Act, and HIPAA) that may lead to significant structural changes such as 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), and globalization of IT innovation (King, et al. 1994).

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 Chin (2008) argue in favor of applying institutional theory to examine regulatory effects on information technology management. 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 to examine the effects of various institutional forces and market forces operating in the healthcare.

### Effect of Institutional Pressures on Regulatory Compliance

*Variability in 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). These regulations, especially with enforcement provisions against violators, act as 'implicit general deterrence' (Gunningham, et al. 2005). As such HIPAA lays out a broad set of specifications for Privacy, and Security rules, stipulating punitive actions for compliance failure (e.g. any willful violation of patient's privacy could result in a penalty of $50,000 and/or one year imprisonment). In addition to HIPAA, several states have enacted local laws to regulate protected health information (PHI) which are substantially different. Indeed legal scholars argue that the variability in this patchwork of state-level and federal regulations are so significant (Hodge 1999; Langenderfer and Cook 2004) that it impedes healthcare organizations' ability to comply with multitude of regulations, and is detrimental to diffusion of health IT (Cunningham 2000; Hodge 1999, 2000; Gostin, et al. 2001). As such HIPAA defines a floor of regulatory requirements for PHI and allows state laws to override it with more stringent laws. This creates uncertainty for hospitals, especially in states that do not have comprehensive regulations for PHI, in terms of their decisions to develop HIPAA compliant systems as future enactment of stringent laws by state could jeopardize their investments rendering it noncompliant. In light of the complex patchwork of state-level and federal regulations, we expect hospitals located in the states with lesser or no privacy laws will tend to adopt wait-and-see approach to comply with HIPAA. Therefore we hypothesize that:

> H1: *Hospitals located in the states with higher state-level regulatory pressure* (*i.e., more comprehensive privacy laws*) *will exhibit higher tendency to become HIPAA compliant.*

*Regional Compliance Leaders as Source of Mimetic Pressure:*

Organizations tend to mold themselves on successful competitors when faced with uncertain business environment, and ambiguity of organizational technologies, or even goals (DiMaggio and Powel 1983; March and Olsen 1976). For example, Miller and Tucker (2007) find empirical evidence for higher propensity to adopt an emerging technology such as EMR system in a health service area increases with the installed base of such systems. Elsewhere, 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:p181), building on the institutional theory propose that "firms with compliance perspective on information privacy will adopt privacy behaviors that demonstrably conform to industry norms." We contend that, hospitals that compete for business in a state with higher HIPAA compliant base, i.e. higher proportion of hospitals fully compliant to HIPAA, would face more pressure to conform to the norms. Therefore, we posit that:

> H2: *Hospitals located within a state with a higher HIPAA compliant base will exhibit 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 governed by Hippocratic principle and every physician operates within that norm to ensure patient's privacy. The recent evolution of health care sector and its increasingly complex underlying structure, however, has broadened the onus of patient privacy and confidentiality from physicians to multiple stakeholders participating in the healthcare. This may create additional pressure for organizations to hire external consultants, especially in the context of HIPAA, when a high degree of uncertainty is associated with interpretation of regulations and they lack adequate in-house resources to establish regulation compliant systems. Organizations often use external consultants to implement enterprise-wide change-management projects (e.g. deployment of enterprise information systems) who bring forth 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 (Irvine 2007). Hence, we posit that:

> H3: *Hospitals employing external consultants will exhibit higher tendency to become HIPAA compliant.*

### 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 organization depends on their contextual interpretations. In particular, relative size of organization to its competition, and consumer demand play a significant role.

*Consumer Concern for Information Privacy*

Recent studies observed that patients exhibit higher concerns to electronic health information and their anxiety is influenced by several factors including their current health status, personality traits, culture, and prior experience with online privacy invasions (Angst, et al. 2006; Bansal, et al. 2007). Organizations in regulated industries, often, strive to maintain the trust of local communities, avoid attention of consumer groups, and preserve company's reputation as a socially responsible entity (Gunningham, et al. 2005). 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 important role in improving compliance behavior in addition to other market pressures such as intensity of competition (Darnall, et al. 2006; Delmas and Toffel 2007). Despite HIPAA's mandated privacy requirements consumers continue to be anxious about privacy of their personal health information. California Healthcare Foundation in a recent survey report that over two-thirds of consumers are concerned about the privacy of their electronic medical records, yet over half of consumers believe they are obligated to share health information to advance healthcare (CHCF 2005). Additionally, the survey shows that among the consumers who recognize benefits of EMR about two-fifth believe their records are potentially unsafe, unlike three-tenth who believe paper records are riskier. Another stream of research find significant differences in privacy preferences across geographical regions and culture (Bellman, et al. 2002; Pedersen and Frances 1990; Varian, et al. 2005). Consequently, it could be argued that strategic choices of implementing HIPAA compliant processes and safeguards could vary in response to differing level of consumer concern to health information privacy. This leads us to hypothesize that:

> H4: *Hospitals located in states with higher consumer privacy concerns will exhibit higher tendency to become HIPAA compliant.*

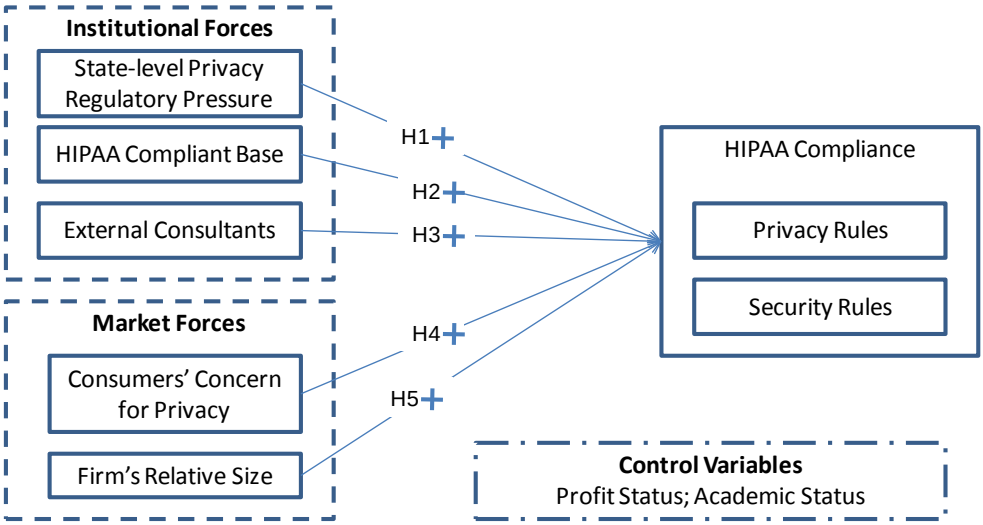


**Figure 1: Regulatory Compliance Model**

*Relative Size to competitors:*

Regulatory requirements often have discriminatory impact on small firms (Baron and Baron 1980). Government regulation forces firms of varying sizes to take the same compliance measures resulting in undue burden on the smaller firms. The larger firms have greater access to financial resources and manpower, and enjoy economies of scale (Weidenbaum 1979). As a result, they have the discretionary power to allocate larger resources to implement necessary policies and safeguards to comply with regulatory requirements. Indeed, empirical studies have shown that 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 potential benefits from regulation (Eldridge and Kealey, 2005; Engel et al. 2007). Hence, we hypothesize:

H5: *Larger Hospitals are more likely to be compliant with privacy, security, and transaction rules of HIPAA.*

The figure 1 summarizes our regulatory compliance 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, in addition to the institutional forces and market forces, tax status, and academic status of hospitals as control variables.

## DATA AND METHODS

The data on 2700+ hospitals for this study was obtained from Health Information and Management Systems Society (HIMSS). Following prior studies in the Health IT literature we include hospitals with at least 100 beds (e.g., Miller and Tucker 2007). Subsequently, we removed all the records that had missing observations on any of the hospital related research variables considered in this study leading to a reduced sample of 1564 hospitals. The model will be tested using logistic regressions. Next we discuss our plan for operationalization of research variables.

**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:** The '*state-level privacy regulatory pressure*' is measured by the number of state-level regulatory provisions that spans eight dimensions - patients' access privilege, denial to access, right to amend, disclosure restriction for hospitals, 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 '*HIPAA compliant base*' is measured as the proportion of hospitals reporting 100% compliance in a state to privacy, and security rules. The '*external consultants*' is coded as 1 if a consultant has been hired by a hospital and 0 otherwise. The '*relative size*' of a hospital is measured as the percentage of total beds across all hospitals in the state. We proxy the '*consumer concern for information privacy*', for the lack relevant data in HIMSS database, by state-level average proportion of consumers registered for Do-Not-Call list reported in Varian, et al. (2005).

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

We are in the preliminary stage of data analysis and expect to report our findings at the conference.

## CONCLUSION

Although industry surveys conducted post enforcement dates of HIPAA rules suggest low level of full compliance among US hospitals (e.g., 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. We shall report our analysis and findings at the conference. 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. Furthermore, the data is related to only acute-care hospitals. As a result, we may not be able to generalize our findings for the entire healthcare sector.

## ACKNOWLEDGEMENTS

We acknowledge Health Information and Management Systems Society for sharing the survey data. This research was supported through the Institute for Security Technology Studies 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.

## REFERENCES

1. AHIMA–The American Health Information Management Association. (2006) "The State of HIPAA Privacy and Security Compliance," http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf
2. 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
3. Anton, A.I., Earp, J.B., Vail, M.W., Jain, N., Gheen, C.M. and Frink, J.M. (2007) "HIPAA's Effect on Web Site Privacy Policies," *IEEE Security & Privacy*, 5,1, 45–52

4. Appari, A. and Johnson, M.E. (2009) "Information Security and Privacy in Healthcare: Current State of Research," forthcoming: *International Journal of Internet and Enterprise Management*
5. 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.
6. Baron, B.R. and Baron, P. (1980) "A Regulatory Compliance Model," *Journal of Contemporary Business*, 9, 2.
7. 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, 40–47.
8. 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
9. Benders, J., Batenberg, R. and Blonk, H. (2006) "Sticking to Standards; Technical and other Isomorphic Pressures in Deploying ERP-Systems," *Information & Management*, 43, 2, 194–203
10. 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
11. Braithwaite, J. and Makkai, T. (1991) "Testing and Expected Utility Model of Corporate Deterrence," *Law & Society Review*, 25, 1, 7–40
12. 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, 404–408
13. Chao, H., Twu, S., and Hsu, C. (2005) "A Patient-Identity Security Mechanism for Electronic Medical Records during Transit and at Rest," *Medical Informatics and the Internet in Medicine*, 30, 3, 227–240
14. CHCF–California HealthCare Foundation (2005), "National Consumer Health Privacy Survey 2005: Executive Summary," available at http://www.chcf.org/topics/view.cfm?itemID=115694
15. 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, 57–64.
16. 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 & Society*, 18, 1.
17. D'Arcy, J. and Hovav, A. (2009) "An Integrative Framework for the Study of Information Security Management Research," in Jatinder Gupta and Sushil Sharma (Eds.), *Handbook of Research on Information Security and Assurance*, Idea Group Publishing, 55–67.
18. 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, 679–703
19. Delmas, M. and Toffel, M.W. (2007) "Organizational Responses to Environmental Demands: Opening the Black Box," Forthcoming: *Strategic Management Journal*
20. DiMaggio, P.J. and Powell, W.W. (1983) "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", *American Sociological Review*, 48, 147–160.
21. Dynes, S. (2009) "Emergent Risks in Critical Infrastructure," in Papa, M. and Shenoi, S. (Eds.) *Critical Infrastructure Protection II*, Springer, 3–16
22. 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, 105–122.
23. Edelman, L.B. and Suchman, M.C. (1997) "The Legal Environments of Organizations," *Annual Review of Sociology*, 23.
24. 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, 116–145
25. Gosain, S. (2004) "Enterprise Information Systems as Objects and Carriers of Institutional Forces: The Iron Cage Revisited," *Journal of AIS*, 5, 4, 151–182
26. 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, 1388–1392
27. Greenway, K.E., and Chan, Y.E. (2005) "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of AIS*, 6, 6, 171–198

28. Hasan, R., and Yurcik, W. (2006) "A Statistical Analysis of Disclosed Storage Security Breaches," *ACM workshop on Storage security and survivability*.
29. Health Privacy Project (2007) "Health Privacy Stories," http://www.cdt.org/healthprivacy/ accessed 4/10/2009.
30. Hoffman, S., and Podgurski, A. 2006. "In Sickness, Health and Cyberspace: Protecting the Security of Electronic Private Health Information," http://ssrn.com/abstract=931069
31. Huston, T. (2001) "Security Issues for Implementation of E-Medical Records." *Communications of the ACM*, 44, 9.
32. Irvine, H. J. (2007) "Corporate Creep: An institutional View of Consultancies in a Non-Profit Organization," *Australian Accounting Review*, 17, 1, 13–25
33. Johnson, M.E. (2009) "Data Hemorrhages in the Healthcare Sector," *Financial Cryptography and Data Security*, Thirteenth International Conference, February 23–26, 2009
34. Johnson, M.E., and Goetz, E. (2007) "Embedding Information Security into the Organization," *IEEE Security & Privacy Magazine*, 5,3, 16–24
35. Kalorama Information (2007) "Wireless Opportunities in Healthcare" www.MarketResearch.com.
36. 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 Journal*, 24, 4, 689–713
37. 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.
38. Kotulic, A.G., Clark, J.G. (2004) "Why There Aren't More Information Security Research Studies," *Information & Management* 41, 597–607.
39. 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, 734–747
40. Massey, C. and Walker, R. (1999) "Aiming for Organizational Learning: Consultants as Agents of Change", *The Learning Organization*, 6, 1, 38–44
41. Mercuri, R.T. (2004) "The HIPAA-potamus in Health Care Data Security," *Communications of the ACM*, 47, 7.
42. Meyer, J.W. and Rowan, B. (1977) "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony", *American Journal of Sociology*, 83, 2, 340–363.
43. Miller, A.R., and Tucker, C.E. (2007) "Privacy, Network Effects and Electronic Medical Record Technology Adoption," *Proceedings of WEIS*, Carnegie Mellon University.
44. Mishra, S. and Chin, A.G. (2008) "Assessing the Impact of Governmental Regulations on the IT Industry: A Neo Institutional Theory Perspective," in Ramesh Subramanian (ed.) *Computer Security, Privacy, and Politics*, 36–53.
45. Ness, R.B. (2007) "Influence of the HIPAA Privacy Rule on the Health Research," *Journal of American Medical Association*, 298, 18, 2164–2170.
46. NRC–The National Research Council (1997) *For the Record: Protecting Electronic Health Information*
47. Oliver, C. (1991) "Strategic Responses to Institutional Processes", *Academy of Management Review*, (16), 145–179.
48. Pedersen, D.M., and Frances, S. (1990) "Regional Differences in Privacy Preferences" *Psychological Reports*, 66
49. Pritts, J., Choy, A., Emmart, L. and Hustead, J. (2003) "The state of health privacy: A survey of state health privacy statutes," vol. I and II, http://ihcrp.georgetown.edu/privacy/publications.html accessed 4/10/2009
50. 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, 167–185
51. 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, 65–69.
52. Silverman, M.G. (2008) *Compliance management for public, private or nonprofit organizations*, McGraw-Hill.
53. Varian, H.R., Woroch, G. and Wallenburg, F. (2005) "The Demographics of the Do-Not-Call List," *IEEE Security and Privacy*, 3, 1, 34–39
54. 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, 79–99

55. 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.
56. Weidenbaum, M.L. (1979) *The Future of Business Regulation*, Amacom, NY.