



The Neo-Institutional View of HIPAA Compliance in Home Health Care

Ajit Appari, M. Eric Johnson
Dartmouth College

Denise L. Anthony

Association of Information
Systems SIGSEC Workshop on
Information Security &
Privacy (WISP 2009). December
14, 2009, Phoenix, AZ, USA

Workshop Chairs
Merrill Warkentin
Mississippi State University,
USA

Rita Walczuch
Maastricht University, The
Netherlands

AIS SIGSEC Chair
Gurpreet Dhillon
Virginia Commonwealth
University, USA

AIS SIGSEC Secretary
Mark Weiser
Oklahoma State University,
USA

www.security-conference.org/sigsec

Abstract

Despite many years since the enactment of the Health Insurance Portability and Accountability Act (HIPAA), healthcare providers have been slow to fully comply with the regulatory requirements, especially the privacy and security rules concerning protection of electronic personal health information. Neo-institutional theory, a dominant analytical perspective of organizational behavior, suggests that variability in local markets—both in terms of competition and institutional environment— influence compliance behavior. Drawing from literature on neo-institutional theory, we empirically examine important factors influencing HIPAA compliance in a specific provider segment, home health care. Our analysis of national-level data on home health agencies provides initial evidence of mimetic influence for compliance arising from other home health agencies that have achieved full compliance. We also find normative influence for privacy compliance arising from affiliation to local acute care hospitals. Finally, we find that the interdependency between the privacy rule and security rule appears to exert coercive influence on compliance effort.

Keywords: HIPAA compliance, Neo-Institutional Theory, Home Health Agencies.

Introduction

As the baby boomers age and the focus of healthcare shifts from acute care to chronic care, home healthcare will become increasingly important in controlling cost and quality (Kemper 2003). Health information technology (HIT) will undoubtedly play an important role toward this goal. In the last decade, the healthcare sector has experienced a significant shift in using HIT—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). Furthermore, among the home health agencies (HHA), a recent survey suggests 58% have adopted at least one clinical system, and 97% have adopted one or more administrative system (Fazzi Associates 2007). Yet, growing adoption of HIT by providers, particularly home health agencies, raises important questions related to the privacy and security of protected health information. For example, studies of media-reported data breaches show medical data disclosure is the second highest breach category (Hasan and Yurcik 2006), and these breaches often expose patients to economic threats, mental anguish, and possible social stigma (Health Privacy Project 2007). Moreover as one recent study shows, such breaches could occur unintentionally when healthcare professionals are using peer-to-peer networking software (Johnson 2009). Foreseeing such issues, the 1996 Health Insurance Portability and Accountability Act (HIPAA) mandated privacy protections (privacy rule) and information security safeguards (security rule), which became effective in April 2003 and April 2005 respectively. Despite the long lead time for compliance,

industry surveys of provider organizations show poor compliance to HIPAA, e.g. by 2006 merely 39% of providers were privacy compliant and only 25% were security rule compliant (AHIMA 2006). This poor state of compliance could reflect lackluster situation for cyber security, necessitating a better understanding of HIPAA compliance efforts in provider organizations, especially home health agencies.

Even though an extensive body of research has drawn attention to the technical, behavioral, process, and policy issues concerning information security and privacy (Appari and Johnson 2009), relatively little has been focused on the unique issues concerning HIPAA compliance, perhaps with the exception of Johnston and Warkentin (2008) and Appari, et al. (2009). Observing this dearth of focus on HIPAA compliance in information security research, especially work grounded in theory, we investigate the variability in firm-level information privacy and security behavior among US home health agencies as measured by their HIPAA compliance level. Björck (2004) and Greenway and Chan (2005) advocated the application of neo-institutional theory (DiMaggio and Powell 1983, Meyer and Rowan 1977)—a dominant paradigm in socio-organizational literature to study the institutional and competitive environment of organizations (Scott 2001) —to frame inquiries on firms' information privacy and security behavior. Furthermore, compliance research largely depends on the neo-institutional framework as a lens to understand the dynamics of compliance both in national and international context (see Edelman and Suchman 1997). In the same vein more recently, researchers have used neo-institutional theory to advance information security research (Appari, et al. 2009; Hu, et al. 2007) and shed light on factors influencing firm behavior.

Our specific aim is to identify the primary drivers influencing HIPAA compliance in home health agencies. The unique context of home health agencies and its organizational environment presents an interesting case to elicit meaningful interpretations of different factors that may have a bearing on compliance efforts. The findings suggest that among other factors considered, mimetic pressure arising from compliance leaders in the local market, normative pressure arising from affiliation to a local acute-care hospital, and coercive pressure arising from interdependency between privacy rule and security rule are important factors influencing HIPAA compliance in home health agencies.

The rest of the paper is structured as follows. First, we briefly explain the neo-institutional theory and its application to different contexts. Next, we elaborate our research model drawing from research on information security and privacy, and neo-institutional theory. Then we present our analysis results and conclude with implications and limitations of this research.

Theoretical Background

Information security and privacy issues rose to the forefront of managements' attention with the enactment of HIPAA. 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 for data security, real time availability, encryption and authentication, network communications, and disaster recovery (Chao, et al. 2005; Dynes 2009; Huston, 2001); implement adequate privacy policies and appropriate controls at all data access points to maintain data integrity, and

maintain audit trails (Mercuri, 2004; Peterson and Burns, 2005). Despite such wider attention to information security issues, almost no theories of social behavior have found their way into managerial information security research. Recognizing this gap, Björck (2004) noted that because effective information security practices depend on social behavior of organizations and their employees, neo-institutional theory (Powell and DiMaggio 1991) may offer a new lens of rigor to examine the information security practices.

Neo-Institutional Theory

The question of what drives or impedes organizations to adopt standards, best practices, and regulations is an important issue in organizational theory. The neo-institutionalism perspective, one of the most dominant lens of organizational analysis (Davis and Marquis, 2005), suggests that organizations obtain legitimacy by conforming to institutional and market pressures within their business environment (Scott 2001; DiMaggio and Powell 1983). When a new regulation, technical or process standard is introduced, or a new best practice emerges, their diffusion or organizational adoption could vary, because competitive and institutional environments affect organizational responses (e.g. Dacin 1997), and more importantly, competitive and institutional environments could vary in intensity at the local level (Hannan et al., 1995; Wade et al., 1998). In addition, resource heterogeneity among firms could lead to variation in organizational response to institutional pressures (Lounsbury, 2001; Suchman, 1995). The neo-institutional theorists have emphasized the importance of both institutional and market forces in explaining the divergence in adopting radical changes (D'Aunno, et al. 2000; Powell and DiMaggio 1991; Scott et al 2000).

Traditionally, institutional forces are 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 arises from the need to respond to uncertainty, often by copying successful competitors; and (c) *normative pressure* which arises from the norms embedded in the profession or industry (DiMaggio and Powell 1983; Scott 2001). The legal environment for organizations is a prime example of coercive 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). Such regulatory forces could lead to the standardization of processes, practices and IT assets to show conformity and gain legitimacy (Zucker 1987). Besides, these three archetypes of institutional pressures, D'Aunno, et al. (2000) emphasize that the framing of radical change, including regulatory compliance, should be viewed from market forces as well, particularly, the relative size of an organization to its competition, and consumer demand among others.

Applications of neo-institutional theory have been seen in a range of situations. For example, prior research in healthcare has used the institutional framework extensively to study the impact of various regulations in shaping hospital management (e.g. Anthony and Banaszak-Holl 2003; Covaleski, et al. 1993; Lorence and Richards 2003), and adoption of innovations like process reengineering, and medical technologies (see Rye and Kimberly 2007 for review of literature). Similarly, a growing body of information

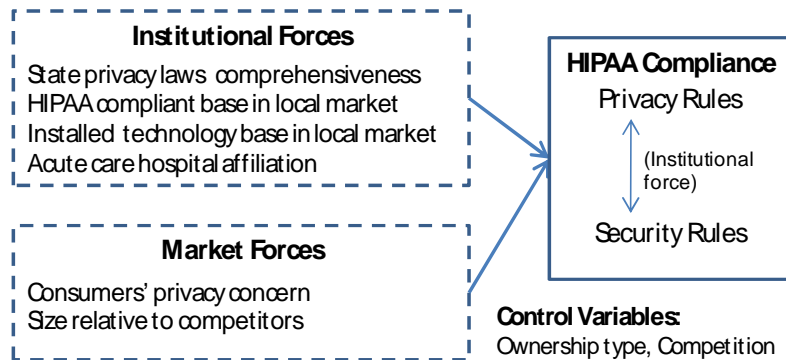
systems research has exploited institutional theory, both in conceptual and empirical work, to study issues like adoption challenges of enterprise information systems (Gosain 2004; Benders, et al. 2006), and adoption of information security practices in multinational organization (Hu et al. 2007), among others. Next we present our arguments for hypotheses associated with institutional and market forces considered in the model.

Research Model

Building on the rich literature in neo-institutionalism and its applications, we develop a regulatory compliance model for home health care in the context of HIPAA. Figure 1 depicts our research model that identifies five major institutional forces and two market forces that are expected to drive HIPAA compliance effort at home health agencies. In addition, to account for confounding factors we include agency’s ownership type and competition level as control variables.

Effects of Institutional Forces

Drawing on the neo-institutional theory, we consider two sources of coercive pressure—state privacy laws and the interdependency between HIPAA privacy and security rules; two sources of mimetic pressure—HIPAA compliant base and installed technology base in the local market; and one source of normative pressure—affiliation with an acute care hospital in the local market.



Note: The interdependency between privacy and security rule as a source of institutional force is shown within the HIPAA compliance box.

Figure 1: Regulatory Compliance Model for Home Health

HIPAA sets forth a ‘floor’ of privacy and security safeguards, including administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI; organizational requirements governing contracts with business associates; and policies, procedures and documentation governing overall information security policy management. Further it allows more stringent state-level laws to take precedence. Following HIPAA, most states have enacted local laws to regulate transfer and management of health information, which could be substantially different. Despite differences between state-level requirements and HIPAA requirements, we contend that if a state has more comprehensive privacy laws, it will present less uncertainty, and hence act as positive force (coercive pressure) for home health agencies to adopt

HIPAA compliant systems compared to other states where an absence of comprehensive laws places the health providers in precarious situations due to uncertainty of future state-level regulations. Thus we hypothesize:

H1: Home health agencies located in states with more comprehensive regulations for PHI will exhibit a higher tendency to become HIPAA compliant.

The privacy and security rules of HIPAA are closely intertwined and designed to be compatible with each other (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 home health agencies, even though security compliance was not mandated until two years after privacy compliance. In particular, we expect home health agencies that are undertaking security compliance in tandem with privacy compliance will have achieved higher level of privacy compliance. Therefore, we posit:

H2: Home health agencies with higher compliance to privacy rules (security rules) will exhibit a higher tendency to become security rules (privacy rules) compliant.

In situations where the institutional environment is unclear, organizations tend to mold themselves after other organizations that have dealt with such uncertainty successfully (DiMaggio and Powel 1983; March and Olsen 1976). In fact, acquiescence by imitating successful peers to gain organizational legitimacy is a common strategic response to regulatory pressure (Oliver 1991). Moreover, firms "with compliance perspective [approach] on information privacy will adopt privacy behaviors that demonstrably conform to industry norms. (Greenway and Chan (2005: p 181)" Thus we contend that markets with a higher HIPAA compliant base (i.e. higher proportion of HHAs already compliant) will exert higher mimetic pressure on home health agencies that are non-compliant to regulations. Hence, we hypothesize:

H3: Home health agencies located in markets with higher HIPAA compliant base will exhibit a higher tendency to be HIPAA compliant.

Health information technologies, in particular clinical systems such as electronic medical record (EMR), enhance the management of patient information through controlled and auditable data access processes and improve data security (Agrawal 2002). They also facilitate both intra and inter organizational transactions based on standardized data formats and enhance the ability to share patient data with accreditation agencies required per regulatory norms (Chaiken 2003). Finally, they contribute to research data repositories for improving public health and enhance medical knowledge (Aspden, et al. 2003). Prior research has shown that hospitals located in states with a higher EMR installed base face higher pressure to adopt EMR systems (Miller and Tucker 2009). This external force, in turn, promotes HIPAA compliance among providers. Thus, we expect that:

H4: Home health agencies located in markets having a higher installed technology base will exhibit a higher tendency to become HIPAA compliant.

The business environment of home health agencies is diverse in the sense that some agencies often serve patients discharged from acute care hospitals and they may attract different patients (Mor 2005). Indeed, prior literature documents that hospital-based home health agencies differ significantly in their service mix compared to home health agencies without any affiliation to a hospital (e.g. Fortinsky et al. 2003). Likewise, we contend that if a home health agency is affiliated to an acute care hospital located in its market, the agency may experience certain normative pressure to be compliant with privacy and security rules. Hence we hypothesize that:

H5: Home health agencies with affiliation to acute-care hospitals will exhibit a higher tendency to be HIPAA compliant.

Effects of Market Forces

Besides institutional forces, we consider two sources of market pressure—consumers' privacy concern and relative size of home health agencies in the local market. Here we explain our rationale.

The California Healthcare Foundation, in a recent survey, reported that over two-thirds of consumers were concerned about the privacy of their electronic medical records, and public disclosure of data breaches had further heightened privacy concerns among consumers (CHCF 2005). 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, several studies found significant differences in privacy preferences across gender, geographical regions, and culture (Bellman, et al. 2002; Pedersen and Frances 1990; Varian, et al. 2005). In particular, Varian, et al (2005) observed significant differences in privacy preferences among American consumers residing in various geographical regions. Consequently, it could be argued that 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:

H6: Home health agencies located in states with higher consumer concern for privacy will be more likely to become HIPAA compliant.

Regulatory requirements often have a discriminatory impact on small firms (Baron and Baron 1980). Though limited, prior empirical research show 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 the potential benefits from regulation (Eldridge and Kealey, 2005). The larger firms, unlike smaller, 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:

H7: Home health agencies of larger size relative to competitors will exhibit a higher tendency to be HIPAA compliant.

Data and Research Methods

We use research data from multiple sources. HIPAA compliance status and information technology adoption data for home health agencies and their parent organizations were obtained from Health Information Management and Systems Society (HIMSS). This data is based on the annual survey conducted by HIMSS in year 2003. The data on state-level privacy regulations is derived based on a contemporaneous report by Joy Pritts and her colleagues (Pritts, et al. 2002). In addition, consumer concern for privacy, measured at state level, was obtained from Varian, et al. (2005). Lastly, market information, such as health referral region (HRR) and associated zip codes that defines the local market was obtained from the '2003 Zip code cross walk' available at the Dartmouth Atlas website, and the total population of home health agencies was obtained the 2003 Home Health Compare database published by Center of Medicare and Medicaid Services.

Operationalization

Dependent Variables: HIPAA compliance levels for privacy and security rules were coded as ordered variables on a scale of 1-4 corresponding to the compliance level (<50%, 50-75%, 76-99%, and 100% compliant).

Independent Variables: The *state privacy laws comprehensiveness* was measured at the state-level by codifying the information available in Pritts, et al. (2003). We examined the presence of state statutes along the ten dimensions, including access to health record, denial of access, right to amend, disclosure restriction, and condition specific privacy protections including birth defects, cancer, genetic test, sexually transmitted diseases, HIV status, and substance abuse. Each dimension was coded as a dichotomous variable with 1 representing enactment of statutes by the year 2002, and 0 otherwise. The linear sum of these 10 dimensions, after dividing by 10 for normalization purposes, was used to indicate the comprehensiveness of state-level privacy rules. The *acute care hospital system affiliation* was coded as dichotomous variable with 1 denoting if the HHA was affiliated with an acute care hospital in the region, 0 otherwise. The HIPAA compliant base, i.e. *privacy compliant base* and *security compliant base in the local market*, was computed as the proportion of HHA in a health referral region reporting 100% compliance with privacy and security rules respectively. Similarly, the *installed technology base in local market* is operationalized for two types of HIT systems—administrative and clinical systems separately as the proportion of HHAs in each referral region that had operational/administrative and clinical systems respectively. These measures of compliant bases and technology bases are notionally similar to the installed base of EMR systems used in Miller and Tucker (2009).

The *consumers' privacy concern*, because of lack any good data source within the same timeframe as the HIMSS survey of HIPAA compliance, was measured at state level by a proxy as the average proportion of citizens registered for Do-Not-Call list by year 2003 as reported in Varian, et al. (2005). This measure of privacy concern (or preference) has been used as acceptable measure by researchers, e.g. in the context of EMR adoption among hospitals (Miller and Tucker 2009). The *size relative to competitor* was measured by the ratio of home visit volume of focal HHA to average home visit volume of all HHAs located in a HRR.

Control Variables: The *competition* in a health referral region was measured as the proportion of total home health agencies in the nation that were operating in the region. The *ownership type* was coded as dichotomous variable with 1 being for-profit and 0 being non-profit.

Analysis Results

Our initial sample size from the HIMSS 2003 database was about 1900+ home health agencies. After excluding HHAs that did not report compliance status and home visit volume, our sample size was reduced to 809 home health agencies. Among these 809 agencies only 10 are for-profit agencies. Tables 1 and 2 show summary statistics of the model variables.

Table 1. Distribution of home health agencies reporting compliance in 2003

Compliance Level	Privacy Rule	Security Rule
< 50%	2%	26%
50 - 75%	9%	24%
76 - 99%	33%	29%
100%	56%	21%

Table 2. Summary of independent variables

Model Variables	Mean	Std. Dev.
State privacy laws comprehensiveness	0.74	0.15
Security compliant base	13%	23%
Privacy compliant base	43%	32%
Installed technology base (Clinical)	79%	24%
Installed technology base (Admin.)	96%	12%
Consumers' privacy concern	37%	9%
Size relative to competitors	0.98	0.78

Table 3 shows the summarized results of two separate ordered probit regressions conducted for privacy compliance and security compliance as dependent variables. For both regressions the model statistics were significant—Wald's chi-square of 266 for privacy compliance and 195 for security compliance. The analysis shows partial support to our regulatory compliance model. In particular, we find that the variation in state privacy laws comprehensiveness does not seem to make any difference on compliance status suggesting no evidence of coercive pressure from state privacy laws on HIPAA compliance effort of home health agencies (H1). The other form of coercive pressure arising from the interdependency of privacy rules and security rules of HIPAA appear to positively influence HIPAA compliance as the coefficient of security (privacy) compliance level in the case of privacy (security) compliance regression is positive and statistically significant (H2).

Further, positive and statistically significant coefficient estimates for privacy (security) compliant base in the privacy (security) compliance regressions suggest strong support for hypothesis H3. Moreover, the magnitudes of these coefficients are largest among all factors considered in compliance model indicating this particular type of mimetic pressure has a dominant effect among all. Next, though the level of mimetic pressure

arising from installed technology base in local market (measured separately for administrative systems and clinical systems) does not seem to influence compliance to privacy rule, it does influence compliance to security rule. Surprisingly the sign of effects flip from positive for clinical systems to negative for administrative systems. Thus we find mixed support for hypothesis H4. The last factor among institutional forces, normative pressure arising from affiliation to acute care hospital in local market, appears to positively influence compliance to privacy rule alone suggesting partial support for hypothesis H5.

Finally, among the two sources of competitive forces none appear to influence HIPAA compliance suggesting lack of support for hypotheses H6 and H7.

Table 3. Results of ordered probit regressions for HIPAA compliance

Variables [hypothesis]	Privacy Compliance	Security Compliance
State privacy laws comprehensiveness [H1]	0.27 (0.308)	-0.165 (0.262)
Security compliance level [H2]	0.267 (0.041) ***	
Privacy compliance level [H2]		0.26 (0.052) ***
Privacy compliant base [H3]	2.596 (0.178) ***	
Security compliant base [H3]		2.451 (0.237) ***
Installed technology base (Clinical) [H4]	-0.092 (0.221)	0.713 (0.227) ***
Installed technology base (Admin.) [H4]	0.585 (0.587)	-1.503 (0.373) ***
Acute care hospital affiliation [H5]	0.404 (0.086) ***	0.093 (0.084)
Consumers' privacy concern [H6]	-0.48 (0.454)	0.259 (0.445)
Size relative to competitors [H7]	0.012 (0.053)	0.068 (0.05)
Ownership type	-0.021 (0.404)	0.124 (0.221)
Competition	-0.031 (0.043)	0.061 (0.039)

*** significant at $p < 0.01$

Implications and Limitations

Information technology adoption in home health will certainly facilitate productivity and quality improvements. However, the rising adoption of these technologies also poses threats to privacy and security of protected health information, demanding the implementation of effective safeguards. To investigate whether healthcare providers are adopting the necessary safeguards, we explored compliance to privacy, and security rules mandated by HIPAA. In particular, drawing from neo-institutional theory, we focused on the influence of key forces operating in the institutional and competitive environment of home health agencies. As presented earlier, our analysis of 809 home health agencies shows only 56% reported full compliance to privacy rule and merely 21% reported full compliance to security rule. When we examine this low rate of HIPAA compliance through the lens of neo-institutional theory our analysis suggest partial support for the regulatory compliance model. Specifically, we showed that for both

privacy and security rule compliance, the coercive pressure arising from the interdependency of HIPAA privacy and security rule and mimetic pressure arising from HIPAA compliant base play significant role in explaining the variation in HIPAA compliance. In addition, we find partial evidence of installed technology base and affiliation to acute care hospital in explaining the variation in compliance to the security rule and privacy rule respectively. It is interesting to note the lack of empirical evidence for influence of variation in state-level privacy laws on either privacy rule or security rule compliance. Among the healthcare community and various forums, the variation in state-level privacy laws are often considered a major roadblock to adoption of HIPAA compliant health information technology and processes. In this light, our finding seems to be counter intuitive and perhaps require further examination. Particularly, since we operationalize the state-laws comprehensiveness measure based on presence or absence of law in reference to various dimensions of health information, a better understanding could be gained by considering actually complexity of state laws.

Since our empirical study is based on cross-sectional data, we seek prudence in making causal relationship claims and believe it is more appropriate to take our findings as evidence of association. In light of this key limitation, the implications of our findings to practice are threefold. First, home health agencies are better off by pursuing privacy compliance in conjunction with security compliance efforts, particularly because of their interdependent nature. This strategy could be of critical significance even in the context of new revisions being brought in privacy and security rules under the umbrella of the HITECH act. Second, as the mimetic effect of the HIPAA compliant base is dominant, it would be beneficial to home health sector to undertake appropriate policy and industry level initiatives that could effectively facilitate the transfer of knowledge and skills from successful home health agencies to trailing agencies. Finally, home health agencies need to be cautious about deploying administrative and clinical systems as the practices being embedded in these technologies may not always be favorable towards compliance. Specifically, in the context of security compliance, our analysis shows that a larger installed base of administrative systems in a local market tends to have a negative effect on compliance, while a larger installed base of clinical systems tends to have positive effect.

This research has several limitations that future research may address. First, the data comes from an 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 further light on HIPAA compliance. For example, workforce competency with respect to privacy and security may play an integral role in HIPAA compliance. Moreover, longitudinal data could be more valuable in offering insight into the dynamics of HIPAA compliance among home health agencies. Second, in this study we considered the comprehensiveness of state-level privacy laws, whereas the real issue appears to be the divergence in consent requirements for disclosure of different parts of electronic health records. Future studies may include the complexity of EMR 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 healthcare. For example, HIPAA compliance requires significant investments on technology implementation, training and awareness, compliance personnel, policy formulation and revision, and periodic audits. Future research may examine the strategic posture adopted by hospitals in achieving and sustaining HIPAA compliance.

Conclusion

When a new regulation is introduced, organizations respond by changing their business practices and adopting new processes and infrastructure to comply with requirements set forth by regulation. However, because of variation in the local environment, particularly the competitive and institutional environment, organizations may exhibit different levels of compliance. Although 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), industry surveys suggest low level of full compliance among healthcare providers (AHIMA 2006). Recent research on HIPAA compliance, though, suggests that perception of organizational support and self-efficacy among healthcare professionals influence their intent to comply with regulatory requirements (Johnston and Warkentin 2008). Regulatory compliance is a much broader phenomenon and could be influenced by both internal and external forces. To enhance our understanding of HIPAA compliance among home health agencies, we developed a research model grounded in neo-institutional theory and tested the model using a national sample. This research addresses an important gap and we further hope it will generate interest among information security researchers to examine deeper issues related to HIPAA compliance.

References

- 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).
- AHIMA – The American Health Information Management Association (2006) “The State of HIPAA Privacy and Security Compliance,” last accessed on Nov. 2008,
- Anthony, D.L., and Banaszak-Holl, J. (2003) “Organizational Variation in the Managed Care Industry in the 1990s: Implications for Institutional Change,” *Research in the Sociology of Health Care*, 21, 21-38
- 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*.
- Appari, A., Anthony, D.L., Johnson, E.M. (2009) “HIPAA Compliance: An Examination of Institutional and Market Forces,” *The 8th Workshop on Economics of Information Security*, London, August 24-25
- 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
- Baron, B.R., and Baron, P. 1980. “A Regulatory Compliance Model,” *Journal of Contemporary Business*, 92, 139-150
- 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
- Benders, J., Batenberg, R. and Blonk, H. (2006) “Sticking to Standards; Technical and other Isomorphic Pressures in Deploying ERP-Systems,” *Information & Management*, 43(2)
- 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, January 5-6

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

CHCF – California HealthCare Foundation (2005) "National Consumer Health Privacy Survey 2005: Executive Summary," available at www.chcf.org

Computer World, (2001) "Beware of Predatory HIPAA Consultants," last accessed 11/2008
<http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,60250,00.html>

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), 65 – 80.

D'Aunno, T., Succi, M., Alexander, J. A. (2000) "The Role of Institutional and Market Forces in Divergent Organizational Change," *Administrative Science Quarterly*, 45(4), 679.

Dacin, M. T. (1997) Isomorphism in context: The power and prescription of institutional norms. *Academy of Management Journal*, 40(1), 46–81.

Davis, G.F., and Marquis, C. (2005) "Prospects for Organizations Theory in the Early Twenty-First Century: Institutional Fields and Mechanisms," *Organization Science*, 1-12

DiMaggio, P., W. Powell. (1983) "The Iron Cage Revisited: Institutional isomorphism and collective rationality in organizational fields," *American Sociological Review*, 48,147-160

Dynes, S. (2009) "Emergent Risks in Critical Infrastructure," in Papa, M. and Sheno, S. Eds. *Critical Infrastructure Protection II*, Springer, 3 -16

Edelman, L.B. and Suchman, M.C. (1997) "The Legal Environments of Organizations," *Annual Review of Sociology*, 23, 479-515.

Eldridge, S.W. and Kealey, B.T. (2005) "SOX Costs: Auditor Attestation under Section 404," Available at SSRN: <http://ssrn.com/abstract=743285>

Fazzi Associates. (2007) *Phillips National Study on the Future of Technology and Telehealth in Home Care -- Presentation at National Association for Home Care and Hospice: October 2007. Northampton, MA.*

Fedorowicz, J., and Ray, A.W. (2004) "Impact of HIPAA on the Integrity of Healthcare Information," *International Journal of Healthcare Technology and Management*, 6(2), 142-157.

Fortinsky, R.H., Garcia, R.I., Sheehan, T.J., Madigan, E.A. and Tullai-McGuinness, S. (2003) Measuring Disability in Medicare HomeCare Patients: Application of Rasch Modeling to the Outcome and Assessment Information Set. *Medical Care*, 41(5), 601–15.

Gosain, S. (2004) "Enterprise Information Systems as Objects and Carriers of Institutional Forces: The Iron Cage Revisited," *Journal of AIS*, 5(4), 151 – 182.

Greenway, K.E., and Chan, Y.E. (2005) "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of AIS*, 6(6), 171 – 198

Gunningham, N.A., Thornton, D., and Kagan, R.A. (2005) "Motivating Management: Corporate Compliance in Environmental Protection," *Law & Policy*, 27, 289 – 316

Hannan, M., Carroll, G., Dundon, E. A., & Torres, J. C. (1995) "Organizational evolution in a multinational context: Entries of automobile manufacturers in Belgium, Britain, France, Germany and Italy," *American Sociological Review*, 60, 509–528.

- Hasan, R., and Yurcik, W. (2006) "A Statistical Analysis of Disclosed Storage Security Breaches," ACM workshop on Storage security and survivability.
- Health Privacy Project (2007) "Health Privacy Stories," <http://www.healthprivacy.org>
- Hu, Q., Hart, P., and Cooke, D. (2007) The role of external and internal influences on information security – a neo-institutional perspective. *Journal of Strategic Information Systems*, 16, 153-172.
- Huston, T. (2001) "Security Issues for Implementation of E-Medical Records." *Communications of the ACM*, 44(9).
- Johnson, M.E. (2009) "Data Hemorrhages in the Healthcare Sector," *Financial Cryptography and Data Security, Thirteenth International Conference, February 23-26, 2009*
- Johnston, A.C. and Warkentin, M. (2008) "Information Privacy Compliance in the Healthcare Industry" *Information Management and Computer Security*, 16(1), 5-19
- Kalorama Information (MarketResearch.com) (2007) "Wireless Opportunities in Healthcare".
- Kemper, P. 2003 "Long-Term Care Research and Policy," *The Gerontologist* 43(4), 436-446.
- Lorence, D.H., and Richards, M.C. (2003) "Adoption of Regulatory Compliance Programs Across United States Health Care Organizations: A view of Institutional Disobedience," *Health Services Management Research*, 16(3), 167-178
- Lounsbury, M. (2001) Institutional sources of practice variation: Staffing college and university recycling programs. *Administrative Science Quarterly*, 46, 29–56.
- March, J.G. and Olsen, J.P. (1976) *Ambiguity and Choice in Organizations*, Norway
- Mercuri, R.T. (2004) "The HIPAA-potamus in Health Care Data Security," *Communications of the ACM*, 47(7).
- Meyer, J.W. and Rowan, B. (1977) "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony", *American Journal of Sociology*, 83(2), 340-363.
- Miller, A.R., and Tucker, C.E. (2009) "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science*, 55(7), 1077-1093.
- Mor, V. (2005) "Improving the Quality of Long-Term Care with Better Information," *The Milbank Quarterly*, 83(3), 333-364.
- Oliver, C. (1991) "Strategic Responses to Institutional Processes", *Academy of Management Review*, 16, 145
- Pedersen, D.M., and Frances, S. (1990) "Regional Differences in Privacy Preferences" *Psychological Reports*, 66, 731
- Peterson, Z. and Burns, R. (2005) "Ext3cow: A Time-Shifting File System for Regulatory Compliance," *ACM Transactions on Storage*, 1(2), 190-212
- Powell, W.W., DiMaggio, P.J. eds. (1991) *The New Institutionalism in Organizational Analysis*, Chicago: University of Chicago Press.
- Pritts, J., Choy, A., Emmart, L., Husted, J. (2002) "The State of Health Privacy Second Edition: A Survey of State Health Privacy Statute," Vol. I & II, <http://ihcrp.georgetown.edu/papers.html>
- Rye, C.B., Kimberly, J.R. 2007 "The Adoption of Innovations by Provider Organizations in Health Care," *Medical Care Research and Review* 64(3), 235
- Scott, R.W. (2001) *Institutions and Organizations*, Second Edition. Thousand Oaks, CA: Sage Publications

Scott, R.W., Ruef, M., Mendel, P.J., and Caronna, C.A. (2000) *Institutional Change and Healthcare Organizations: From Professional Dominance to Managed Care*. Chicago: University of Chicago Press.

Silverman, M.G. (2008) *Compliance Management for Public, Private, or Non-Profit Organizations*, McGraw-Hill, NY

Suchman, M. C. (1995) Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20(3), 571–610.

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.

Wade, J. B., Swaminathan, A., and Saxon, M. S. (1998) Normative and resource flow consequences of local regulations in the American brewing industry, 1845–1918. *Administrative Science Quarterly* 43, 905–935.

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

Zucker, L.G. (1987) “Institutional Theories of Organizations,” *Annual Review of Sociology*, 13.