HIPAA Compliance in Home Health: A Neo-Institutional Theoretic Perspective

Ajit Appari  
Center for Digital Strategies at Tuck  
Dartmouth College  
Hanover, NH 03755, USA  
1-603 646 9017  
Ajit.Appari@Dartmouth.Edu

M. Eric Johnson  
Tuck School of Business  
Dartmouth College  
Hanover, NH 03755, USA  
1-603 646 0526  
M.Eric.Johnson@Dartmouth.Edu

Denise L. Anthony  
Department of Sociology  
Dartmouth College  
Hanover, NH 03755, USA  
1-603 646 0017  
Denise.L.Anthony@Dartmouth.Edu

ABSTRACT
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 improving quality. Health IT will undoubtedly play critical role toward these goals. Yet, growing adoption of Health IT raises important questions related to privacy and security of protected health information, necessitating a better understanding of compliance to HIPAA regulation, which mandates privacy and security safeguards by care providers. In this research we investigate the prevalence of HIPAA compliance in home healthcare to identify drivers influencing HIPAA compliance in home health agencies. The research design involves a model of regulatory compliance comprising institutional and market forces that may have a bearing on home healthcare. We develop hypotheses guided by neo-institutional theory, and conduct quantitative analysis with the goal of generating insights on the primary drivers and barriers of HIPAA compliance.

Categories and Subject Descriptors
K.5.2 [Legal Aspects of Computing]: Governmental Issues – regulation.

General Terms
Management, Security, Theory, and Legal Aspects.

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

1. 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 IT (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, a recent survey suggests 58% of the agencies had adopted at least one clinical system, and 97% had 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 publicly reported data breaches show that medical data disclosure is the second highest breach category (e.g. Hasan and Yurcik 2006), and these breaches often expose patients to economic threats, mental anguish, and possible social stigma (Health Privacy Project 2007). Furthermore, personal health records are being unintentionally disclosed via unexpected mediums such as peer-to-peer networks (Johnson 2009). Precisely because of such reasons the 1996 Health Insurance Portability and Accountability Act (HIPAA) mandated privacy protections (privacy rule) and information security safeguards (security rule) that became effective in April 2003 and April 2005 respectively. Despite the long compliance lead time, recent industry surveys of provider organizations show a bleak picture of HIPAA compliance, e.g. by year 2006 merely 39% of providers were privacy compliant and only 25% were security rule compliant (AHIMA 2006). Such a poor state of compliance could reflect lackluster situation for cyber security, necessitating a better understanding of HIPAA compliance efforts in home health.

Even as the recently enacted Health Information Technology for Economic Clinical Health Act (HITECH) 2009 attempts to intensify the adoption of health IT (HIT) and strengthen the enforcement of HIPAA, current research on information security has rarely paid attention to HIPAA compliance issues 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). 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 firm behavior.

Our specific aim is to identify the primary drivers influencing HIPAA compliance in home health agencies. We focus on the unique context of home health agencies and its organizational environment to develop a regulatory compliance model and validate it using secondary data sources. The primary contribution of this research lies in the novel application of neo-institutional theory to explain variability in regulatory compliance prevalent in US home healthcare sector. 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 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 analysis results and its implications to research and practice. Finally we conclude with remarks on limitations and future steps for this research.

2. THEORETICAL FRAMEWORK AND RESEARCH MODEL

Information security and privacy issues have been brought 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 maestrom 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 and Burns, 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 and Burns, 2005), implement adequate privacy policies and appropriate controls at all data access points to maintain data integrity (Mercuri, 2004).

In a recent critique, Björck (2004) noted 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)”. Further he argued 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 dynamics of information security management in the healthcare.

2.1 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; Heugens and Landier 2009), 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 (Dacin 1997; Haveman and Rao 1997), and more importantly, competitive and institutional environments could vary in intensity at the local level (Hannan et al., 1995; Wade et al., 1988). In addition, resource heterogeneity among firms could lead to variation in organizational response to institutional pressures (Lounsbury, 2001, 2008; 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), diffusion of Software Engineering...
Institute’s Capability Maturity Model (CMM®) (Adler 2005), and globalization of IT innovation (King, et al. 1994) among others. 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.

Next we present our arguments for hypotheses associated with institutional and market forces considered in the model.

2.2 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, installed technology base in the local market; and one source of normative pressure -affiliation with acute care hospital in the local market.

Figure 1: Regulatory Compliance Model for Home Health

HIPAA sets forth a broader set 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 (NIST 2005). 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 due to uncertainty of future state-level regulations. Thus, we hypothesize that:

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). Because of this, the coercive pressure arising from interdependency of privacy and security rules may influence the compliance initiatives of home health agencies. Thus we hypothesize that:

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 Powell 1983; March and Olsen 1976). Oliver (1991) argues that acquiescence by imitating successful peers to gain organizational legitimacy is a common strategic response to regulatory pressure. 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 that:

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

Health information technologies, in particular clinical systems such as 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.

2.3 Effects of Market Forces
Besides institutional forces, we consider two sources of market pressure – consumers’ privacy concern, and relative size of home health agency 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 that:

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). Larger firms tend to have more financial resources and manpower, and enjoy economies of scale (Weidenbaum 1979). Hence we hypothesize that:

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

3. 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 HIMSS. This data is based on the annual survey conducted by HIMSS in year 2003. The data on state-level privacy regulations was compiled based on recent 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.

3.1 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 HHAs 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.

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 the health referral region.

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.

3.2 Statistical Model

For analyzing ordered categorical dependent variables, an ordered probit model is a commonly used statistical framework (Agresti 2003). We use this methodology to estimate the influence of institutional forces and market forces on the probability of a HHA to be in one of the four levels of compliance, in the increasing order, while controlling for ownership type and competition in local market. In an ordered probit model, the error associated with the focal HHA to average home visit volume of all HHAs located in the health referral region.

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.

Yi*j = β*IFi + γ*MFi + δ*Cj + εi

In this equation, i is index for ith home health agency, IFi is a vector of institutional forces, MFi is a vector of market forces, Cj denotes vector of control variables, and εi ~ N(0,1). The Yi*j represents latent and continuous measure of HIPAA compliance and is modeled by:

Yi = j ⇔ μj-1 < Yi*j ≤ μj

Where index j=0, 1, 2, 3 corresponds to <50%, 50-75%, 76-99% and 100% compliance; μj’s denote thresholds for the latent variable. Alternatively, this probit model is represented as:

P[Yi≤j | IFi, MFi, Cj] = Φ(β*IFi + γ*MFi + δ*Cj)
Where $\Phi$ is the cumulative standard normal function and the coefficients are estimated using the maximum likelihood method. The statistical significance test of coefficients $\beta$ and $\gamma$ allow us to validate the research model shown in figure 1.

3.3 Descriptive Statistics

The HIMSS 2003 database has information on about 1900+ home health agencies. However, upon closer examination of survey data in reference to our research model we found that many of the records did not have relevant information, including HIPAA compliance status, and home visit volume. After excluding such agencies, our sample size was reduced to 809 home health agencies.

Table 1. Distribution of HHAs by HIPAA compliance level

<table>
<thead>
<tr>
<th>Compliance Level</th>
<th>Privacy Compliance</th>
<th>Security Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;50%</td>
<td>2%</td>
<td>26%</td>
</tr>
<tr>
<td>50 - 75%</td>
<td>9%</td>
<td>24%</td>
</tr>
<tr>
<td>76 - 99%</td>
<td>33%</td>
<td>29%</td>
</tr>
<tr>
<td>100%</td>
<td>56%</td>
<td>21%</td>
</tr>
</tbody>
</table>

The table 1 shows distribution of HHAs reporting compliance to privacy and security rule. As the enforcement date of HIPAA privacy rule was earlier than security rule, we observe higher proportion of HHAs reporting a higher level of compliance to privacy rule than security rule (e.g. 56% of HHAs are fully compliant to privacy as compared to 21% fully compliant to security rule).

Table 2. Summary statistics of institutional and market forces

<table>
<thead>
<tr>
<th>Model Variables</th>
<th>Mean</th>
<th>Std. Dev.</th>
<th>Min.</th>
<th>Max.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed technology base (Clinical)†</td>
<td>79%</td>
<td>24%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Installed technology base (Administrative) †</td>
<td>96%</td>
<td>12%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Security compliant base†</td>
<td>13%</td>
<td>23%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Privacy compliant base†</td>
<td>43%</td>
<td>32%</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Consumers’ privacy concern††</td>
<td>37%</td>
<td>9%</td>
<td>14%</td>
<td>54%</td>
</tr>
<tr>
<td>Size relative to competitors††</td>
<td>0.985</td>
<td>0.781</td>
<td>0</td>
<td>8.376</td>
</tr>
<tr>
<td>State privacy laws comprehensiveness††</td>
<td>0.74</td>
<td>0.15</td>
<td>0.3</td>
<td>1</td>
</tr>
</tbody>
</table>

††Measured at health referral region level; †Measured at State level

The Table 2 shows summary statistics for independent variables that are measured either at health referral region level or state level. For example, the average security compliant base is 13% (standard deviation 23%) as compared to 37% (standard deviation 32%) for privacy compliant base across all the referral regions. The consumers’ privacy concern varies significantly across states with average of 37% (standard deviation 9%) and ranges from a minimum of 14% to maximum of 54%. The state 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 a comprehensive set of privacy statutes.

3.4 Analysis Results

Table 3 shows the summarized results of two separate ordered probit regressions conducted for privacy compliance and security compliance. The analysis shows partial support to our regulatory compliance model. In particular, we find that the state privacy laws comprehensiveness is statistically insignificant in both privacy compliance and security compliance regressions, suggesting no evidence of coercive pressure from state privacy laws on HIPAA compliance effort of home health agencies (H1). We investigated another form of coercive pressure arising from the interdependency of privacy rules and security rules of HIPAA. The coefficient of security rules compliance in the case of privacy compliance is positive and statistically significant (0.267, p<0.01). Likewise, the coefficient of privacy rules compliance in the case of privacy compliance is positive and statistically significant (0.26, p<0.01). The similar values of these coefficients suggest the magnitude of coercive pressure is alike toward compliance for both privacy and security rules, despite the two-year gap between enforcement dates for privacy and security rules.

Table 2. Summary results of ordered probit regressions for HIPAA compliance in home health agencies

<table>
<thead>
<tr>
<th>Model Variables</th>
<th>Privacy Compliance</th>
<th>Security Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coercive</td>
<td>State privacy laws comprehensiveness</td>
<td>0.27 (0.308)</td>
</tr>
<tr>
<td></td>
<td>Privacy compliance level</td>
<td>0.267*** (0.041)</td>
</tr>
<tr>
<td></td>
<td>Security compliance level</td>
<td>0.259*** (0.178)</td>
</tr>
<tr>
<td>Minimic</td>
<td>Privacy compliant base</td>
<td>0.585 (0.587)</td>
</tr>
<tr>
<td></td>
<td>Security compliant base</td>
<td>-0.092 (0.221)</td>
</tr>
<tr>
<td></td>
<td>Installed technology base in market (Administrative)</td>
<td>0.585 (0.587)</td>
</tr>
<tr>
<td></td>
<td>Installed technology base in market (Clinical)</td>
<td>-0.092 (0.221)</td>
</tr>
<tr>
<td>Norm</td>
<td>Acute care hospital affiliation</td>
<td>0.404*** (0.086)</td>
</tr>
<tr>
<td></td>
<td>Consumers’ privacy concern</td>
<td>-0.48 (0.454)</td>
</tr>
<tr>
<td></td>
<td>Size relative to competitors</td>
<td>0.012 (0.053)</td>
</tr>
<tr>
<td></td>
<td>Ownership type [profit=yes]</td>
<td>-0.021 (0.404)</td>
</tr>
<tr>
<td></td>
<td>Competition</td>
<td>-0.031 (0.043)</td>
</tr>
<tr>
<td></td>
<td>Number of observations</td>
<td>809</td>
</tr>
<tr>
<td></td>
<td>Wald chi2(11)</td>
<td>266.02</td>
</tr>
<tr>
<td></td>
<td>Pseudo R2</td>
<td>0.1708</td>
</tr>
<tr>
<td></td>
<td>Log Pseudo-Likelihood</td>
<td>-656.6455</td>
</tr>
</tbody>
</table>

*** p<0.01                      ** p<0.05                  * p<0.10
The coefficients for privacy compliant base in the case of privacy compliance is positive and statistically significant (2.596, p<0.01), and as well for security compliant base in the case of security compliance (2.451, p<0.01). This finding supports hypothesis H3. Moreover, the magnitudes of these coefficients are largest among all forces indicating their dominant effect. Next, we considered installed technology base as a source of mimetic pressure. The coefficients of administrative and clinical technology base are statistically significant only in the case of security compliance showing partial support for hypothesis H4 (Administrative: -1.503 and Clinical: 0.713, p<0.01). Though, the estimates are in the opposite directions perhaps capturing characteristic of the underlying technology.

The coefficient for affiliation with acute care hospital is positive and statistically significant only in the case of privacy compliance (0.404, p<0.01) providing partial support to hypothesis H5. Lastly, the coefficients for two market forces—consumers’ privacy concern and size of HHA relative to competitors are statistically insignificant for both regressions indicating a lack of support for hypotheses H6 and H7. Likewise, the coefficients for the control variables are statistically insignificant.

4. DISCUSSION and CONCLUSIONS

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 competitive and institutional environment, organizations could be at different levels of compliance. Although industry surveys conducted post enforcement dates of HIPAA rules suggest low level of full compliance among healthcare providers (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 home health agencies’ compliance behavior, we developed a research model grounded in neo-institutional theory and tested the model using an ordered probit regression approach. Our analysis finds partial support for the regulatory compliance model. In particular, we show that for both privacy and security rule compliance, the coercive pressure arising from interdependency of HIPAA privacy and security rules; and mimetic pressure arising from HIPAA compliant base play significant role in explaining the variation in HIPAA compliance among home health agencies. 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.

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 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, being the first of its kind, 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. 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, however the real issue appears to be the divergence in disclosure consent requirements for different parts of electronic health records. Future studies may include the 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 healthcare. For example, HIPAA compliance requires significant investments on technology implementation, training and awareness, compliance personnel, policy formulation and revision, and period audits. Future research may examine the strategic posture adopted by hospitals in achieving and sustaining HIPAA compliance.

5. ACKNOWLEDGMENTS

We acknowledge partial support by 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 #2006-CS-001-000001. The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the NIST or DHS. In addition, we are grateful to the Health Information and Management Systems Society (HIMSS) Foundation for sharing the 2003 annual survey data on health information technology and HIPAA compliance.

6. REFERENCES

Implications for Institutional Change,” Research in the Sociology of Health Care 21, pp 21-38


[56] Rye, C.B., Kimberly, J.R. 2007 “The Adoption of Innovations by Provider Organizations in Health Care,” Medical Care Research and Review 64:3; pp 235