

# Which Hospitals Are Complying with HIPAA: An Empirical Investigation of US Hospitals<sup>1,2</sup>

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

\* Center for Digital Strategies, Tuck School of Business at Dartmouth, Hanover NH 03755

† Department of Sociology, Dartmouth College, Hanover NH 03755

## Abstract

Since the passage of HIPAA regulation, US hospitals have gone on a high gear by investing organizational resources on HIPAA policy and procedures, information technologies, and information privacy & security safeguards to achieve compliance status by the enforcement dates. Yet, recent industry report, conducted post HIPAA enforcement deadlines, presents a bleak picture of HIPAA compliance, raising concerns for the privacy and security of patient data, as well transactional efficiency of hospitals. Drawing from organizational sociology and organizational behavior literature we examine propensity of hospitals being fully compliant with privacy, security and transaction rules of HIPAA. In particular, we focus on several hospital characteristics including academic status, profit status, hospital size and industry leadership in IT use to identify which type of hospitals are more likely to be HIPAA compliant. Overall, our findings offer insights on the current state of performance outcome of information security investments in the healthcare sector as measured by hospitals' HIPAA compliance, an area under researched in information security literature. Moreover, we expect our findings may inform policy decisions in particular reference to HIPAA compliance.

**Keywords:** Information Privacy, Information Security, HIPAA Compliance, IT Leaders

---

<sup>1</sup> 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.

<sup>2</sup> We acknowledge the Health Information and Management Systems Society Foundation for sharing the 2003 annual survey data on health information technology and HIPAA implementation among US hospitals.

# Which Hospitals Are Complying with HIPAA: An Empirical Investigation of US Hospitals

## 1 Introduction

The Health Information Interoperability and Accountability Act (HIPAA)<sup>3</sup> of 1996 was enacted with the intent of leveraging information technology (IT) to reduce costs, and enabling the portability and continuity of health insurance coverage (OCR 2006). An obvious implication of this dependence on information technologies to collect, store and process patients' health information, especially in the age of internet, across entities in the health sector is ensuring privacy of patient's identifiable information. Such concerns led to provision of Privacy Rules and Security Rules along with the Transaction Rules (Hoffman and Podgurski 2006). Recent studies, on the one hand, offer empirical evidence that adoption of IT systems such as physician order entry systems, clinical reminder systems, and electronic health records are having significant impact on care quality improvement (e.g. Kaelber and Bates 2007; Garg et al. 2005; Linder, et al. 2007). On the other hand, IT spending in healthcare sector trails that of many other industries, typically 3-5% of revenue, far behind industries like financial services where closer to 10% is the norm (Bartels 2006).

The issues of information security and privacy has been brought to the forefront of healthcare managements' attention with the enactment of the HIPAA which set compliance dates for Privacy Rules as April, 2003 for Transaction Rules as October 2003, and for Security Rules as April 2005. The security standard released under HIPAA, in April 2003, specifies five categories of security measures including administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information; and organizational requirements governing contractual agreements; and policies, procedures and documentation requirements governing overall information security policy management (NIST 2005). Pursuant to regulatory mandates, expectedly hospitals will implement all basic safeguards 'required' by HIPAA and implement 'addressable' specifications in their organizational context. However, recent industry surveys, surprisingly, present a bleak picture of HIPAA compliance status among US hospitals. According to a recent survey of about 1100+ hospitals and health systems in the 2006, only 39% are fully compliant with privacy regulation, 25% are fully compliant with security regulation, and 72% have implemented transaction rules (AHIMA 2006). On a positive note, 30% of providers report that HIPAA compliance initiatives has smoothed the process of becoming a member of regional health information organization (RHIO). Despite the significance of HIPAA regulation in healthcare sector, our review of information security literature shows a lack systematic investigation of HIPAA compliance initiatives among healthcare providers perhaps with exceptions of annual surveys conducted by industry associations such as AHIMA. More importantly, empirical research in information security risk management is lacking (Kotulic and Clark 2004).

US hospitals are adopting state-of-the-art Health Information Technologies (HIT) to improve patient safety, care quality, customer service, business processes, workforce, and public health and safety, though they are far behind the adoption curve compared to other developed nations (Anderson et al. 2006). In a recent theoretical development, Barros et al. (1999) argue that provider organizations may

---

<sup>3</sup> The HIPAA rules are applicable to several 'covered entities' including hospitals, hospice, clinics, insurance, payer organizations, employers, regional health information organizations among others who manage patient information in electronic form. In this study we focus only on hospitals and/or hospital systems.

invest in state-of-the-art technologies to “signal” their intrinsic quality of service offerings. This is transparent from the way hospitals often advertise their ‘most wired hospital’ status<sup>4</sup>, as recognized by a third party benchmark, on their websites and marketing materials, for example Appendix A shows Avera Health System prominently displaying the logo of ‘most wired hospitals’ on its home page). These IT leaders, i.e. ‘most wired hospitals’, are found to have superior performance compared to other hospitals in terms of higher productivity, resource utilization, marginal revenue, and customer satisfaction (Solovy 2001; 2005). The increasing emphasis on HIT, despite their benefits (Borzekowski 2002; Hillestad et al. 2005; Parente and Van Horn 2003), raises concerns for information security. Especially, on the one hand, anecdotal evidences from recent years suggest lack of adequate security measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish, and possible social stigma (Health Privacy Project 2007). On the other hand, a recent survey in the United States suggests that 75% of patients are concerned about health Web sites sharing information without their permission (Raman 2007). Possibly this is because medical data disclosure is the second highest reported breach (Hasan and Yurcik 2006). This negative aspect of IT investments raises an important question on whether the IT Leaders among healthcare providers pursue adequate privacy and security safeguards.

The goal of this research is to provide empirical evidence on the state of HIPAA compliance among US hospitals by examining the association of hospital characteristics to their propensity of being compliant with the triad of HIPAA rules – Privacy, Security and Transaction rules. In particular, we focus on several hospital characteristics including academic status, tax status, and hospital size to identify which type of hospitals are more likely to be compliant with the privacy, security and transaction rules. In addition, given increasing deployment of IT investments, we set out to examine whether hospitals considered as IT Leaders by industry benchmarks are more likely to be compliant with the privacy, security and transaction rules. Further we examine, as well, which types of hospitals are more likely to be compliant with all three rules of HIPAA for comparative study.

We use hospital level data from the Dorenfest Institute database for 1342 hospitals obtained from a national survey of US hospitals conducted by Health Information and Management Systems Society (HIMSS) in 2003, henceforth referred as HIMSS dataset. The HIMSS provided us with data on each hospital’s perceived level of compliance, as reported by hospital executives, on privacy, security, and transaction rules, total number of beds, profit status, academic status, number of EMR technologies installed, if a HIPAA consultant has been hired, and demographic information including website URL. In addition to this dataset, we obtained the list of ‘100 most wired hospitals’ for the year 2003 from [www.hhnmag.com](http://www.hhnmag.com) of AHA, henceforth referred as IT Leaders list. This list contains hospital system name, city, state and website address. We linked these two datasets by using the website URL which we found to be most consistent common denominator between two datasets.

This paper’s primary contribution is to information security and privacy literature focusing on regulatory policy aspects in health care sector. In this study we provide first empirical evidence of hospitals’ propensity to be compliant with HIPAA rules, i.e. privacy, security and transactions, as a function of organizational characteristics. We find several unique profiles of hospitals that are more likely to be HIPAA compliant. For example, larger non-profit hospitals that are considered as leaders in IT use and have higher installed base of EMR systems are more likely to be compliant with all three HIPAA rules considered collectively. In case of privacy rule, larger for-profit hospitals and

---

<sup>4</sup> Over the past several years, the Hospital and Health Network (HHN) magazine of American Hospital Association (AHA) has conducted annual benchmarking surveys of US hospitals to identify leaders of IT users and share their best practices to promote wider adoption of health information technology.

larger academic hospitals have higher propensity to be in compliance. Similarly we identify hospital profiles with respect to security rule and transaction rules. Overall, our findings offer insights on the current state of performance outcome of information security investments in the healthcare sector as measured by hospitals' HIPAA compliance, an area under researched in information security literature. Moreover, we expect our findings may inform policy decisions in particular reference to HIPAA compliance.

The rest of the paper is structured as follows. First we briefly review past research on information security in healthcare, and then we discuss our research model and the research methods applied to validate the model. Finally we conclude with our remarks on limitations and future directions for research.

## **2 Information Security in Healthcare**

### ***2.1 Background***

The healthcare sector is experiencing a tectonic shift in the enablement of care services through IT, in particular, internet and mobile technologies such as remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access, and asset tracking among others (Kalorama 2007). Further web technology has even enabled new approaches to patient information management such as "Health Banks" (Ball and Gold 2006) giving further control to patients of their health information, e.g., recent launches of 'HealthVault' by Microsoft and 'Google Health' by Google.

Increasing adoption of information systems, though beneficial in terms of improving productivity and service quality, also raises major concerns for information security threats. In the modern networked world, security risks to health information could arise from various sources including accidental disclosure, data breach by insider, data breach by outsider with physical intrusion and/or intrusion of network system (NRC 1997; Rindfleisch 1997). As personal health information is digitized, transmitted and mined for effective care provision, new forms of threat to patients' privacy are becoming evident (Mercury 2004). Anecdotal evidence suggests information security incidents often lead to patients' privacy violations and cause socio economic implications (Health privacy Project 2007). Furthermore, such incidences when publicized, hospitals may suffer reputation loss and face diminishing market share. As patients may be discouraged to share critical information with their physicians in the fear of potential security threats, or even switch to new provider.

### ***2.2 Health Service Providers' Perspective***

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

Patients' health information plays a major role in conducting medical research for improving healthcare quality. Anecdotal evidence suggests that the new regulatory requirements have had an adverse effect on the conduct of medical research (e.g. Kaiser 2006). In a nationwide web-based survey of epidemiologists Ness (2007) report that nearly 68% of researchers perceived that HIPAA has made medical research highly difficult and only about 25% believed that it has increased patients' confidentiality or privacy. More importantly, about 39% of researchers believed HIPAA had increased research cost by a great deal, especially due to additional compliance related administrative cost and over 50% of researchers believed HIPAA enforcement lead to delays in research. In a critical review of three cases of health research projects, Shen et al. (2006) report that several factors including the complexity of consent forms and privacy protection forms, and time consuming procedures often get in the way of patient recruitment. This adverse view of HIPAA is also reflected in lower adoption rate of health information systems such as EMR bolstering the perception that privacy laws may actually have negative effect on the ulterior goals of providing quality care at low cost. Recently, Miller and Tucker (2007), in a study of US hospitals, found that hospitals in states with privacy laws were 33% less likely to adopt an EMR system that is compatible with other neighboring hospitals. However, in states with no privacy laws, they found that a hospital's adoption of EMR may increase the likelihood of neighboring hospital adopting EMR by about 6 percent.

### **2.3 Healthcare Consumers Perspective**

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

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).

## **3 Research Model**

Edelman and Suchman (1997), in a recent essay on legal environments of organizations, argue that a significant body of organizational sociology research theorizes regulatory compliance behavior of organizations from a *materialist perspective*. In this perspective organizations are perceived as wealth maximizing rational agents and the law as an encompassing system of incentives and

punishment in which organizations conduct their business. In the context of healthcare, as such traditionally the patient-physician relationship is based on the Hippocratic principle and every physician operates within that norm while ensuring patient's privacy. The evolution of health care sector and its increasingly complex underlying structure, however, has shifted the onus of privacy and confidentiality to patient information from physicians to multiple organizations who participate in health care service provision. In effect, we adopt the materialist perspective to motivate our research model to examine hospitals' compliance to HIPAA regulation. It is worth noting that the HIPAA regulation while proscribing a broad set of specifications for Privacy, Security, and Transaction rules stipulates punitive actions for failure to comply with requirements and standards. In general, for each violation a penalty of \$100 could be imposed with a maximum of \$25,000 during a calendar year. Furthermore, for any willful violation of patient's privacy, health care provider could face penalty of \$50,000 and/or 1 year prison sentence. And if such violations are carried out with intent to harm the patient or making profit, provider could face penalty of \$250,000 and/or 10 years prison sentence. These penalties may act as deterrence to hospitals and ensure that management undertakes adequate safeguards to protect themselves from possible violations (Braithwaite and Makkai 1991)<sup>5</sup>.

In the organizational behavior literature scholars have predominantly considered certain individual, organizational and contextual characteristics as predictors of technology adoption (Kimberly and Evanisko 1981). However, there exists a lack of consensus on which specific characteristics influence technology adoption. As such HIPAA compliance, which requires adoption of information privacy and security policies, security risk management, information security technology, interoperable systems and transactional standards among others, is a regulatory mandate. Yet recent industry surveys show lack of 100% compliance among US hospitals (e.g., AHIMA 2006). To examine the variation in adoption of requirements of privacy, security and transaction rules of HIPAA, we identify five organizational characteristics as being salient to HIPAA compliance, drawing from organizational behavior literature (e.g., Kimberly and Evanisko 1981; Damanpour 1987) as well as the HIT literature (e.g., Burke et al. 2002; Hikmet et al. 2008); (1) IT Leaders (hospitals identified as leaders in IT adoption and use) (2) hospital's tax status (profit vs. non-profit), (3) hospital's academic status, (4) size of EMR systems installed base, and (5) hospital size (number of beds) (see Fig. 1). The theoretical rationale for choosing these specific factors is explained below.

**IT Leaders:** investments in HIT have been shown to improve healthcare quality and patient satisfaction (Bhattacharjee, et al. 2007 ; Whitten, et al. 2008). From HIPAA compliance perspective, meeting the requirements of privacy, security and transaction rules would require IT savvy culture and strong IT infrastructure. Superior health information technology infrastructure may help hospitals in being compliant to regulatory requirements as HIT systems enable timely and accurate capture of patient information, record keeping and reporting, error free clinical decision making and patient safety among others (Agrawal 2002). We therefore hypothesize:

*H1. Hospitals considered as IT Leaders are more likely to be compliant with privacy, security, and transaction rules of HIPAA.*

**Profit Status:** for profit hospitals, in addition to HIPAA, are subjected to other regulations such as Sarbanes Oxley Act which mandates information security requirements based on Control Objectives

---

<sup>5</sup> It is fair to note that the HHS Office for Civil Rights (OCR), responsible for enforcing HIPAA, has received about 34000 complaints for privacy violations and it is yet to levy a penalty against anyone. Only about 26% of these cases led to formal investigations and the rest were dismissed (Los Angeles Times April 2008).

for Information and related Technology (COBIT) framework. Higher investments in information technology by for-profit hospitals, on the one hand, could be due to their objectives of optimizing operational costs and efficiencies to maximize profitability, and eventually maximize shareholder returns (e.g., Robinson 2002; Corder 2001; Hikmet et al. 2008). The non-profit hospitals as such do not have the incentives of profit maximization. On the other hand, for-profit hospitals may have greater propensity to investment in necessary infrastructure to ensure privacy and security of patient information. This is perhaps due to potential reputational loss and firm value in the event of data breach. Therefore we expect:

*H2. For-profit (non-profit) hospitals are more (less) likely to be compliant with privacy, security, and transaction rules of HIPAA.*

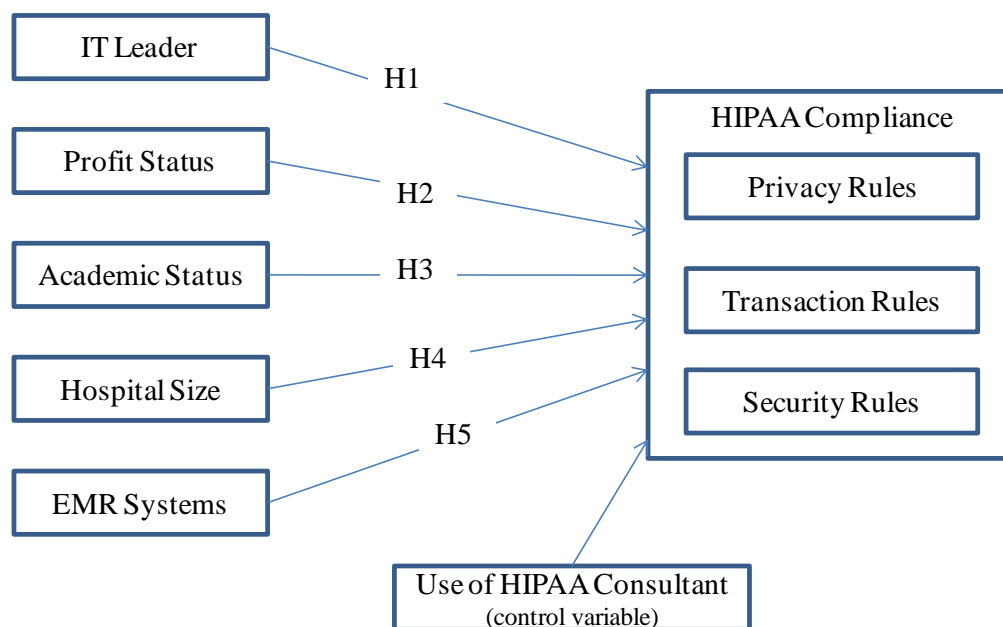


Figure 1: Research Model

**Academic Status:** academic hospitals are generally engaged in medical research that demands use of patient's information and participation. Disclosure of health information to researchers raises concerns of privacy violations. To overcome such issues, it is customary among medical researchers to obtain consents from research participants or in exceptional cases obtain approval from an Institutional Review Board (IRB). Though there exists some empirical evidence of increased administrative cost with introduction of HIPAA regulation in conducting medical research (e.g. Kaiser 2006; Turner 2002), academic hospitals, who are generally well endowed in terms of financial and human resources, will have higher propensity to invest in HIPAA compliance. Therefore we hypothesize:

*H3. Academic hospitals are more likely to be compliant with privacy, security, and transaction rules of HIPAA.*

**Hospital Size:** 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. As a result, an undue burden is placed on the small firm in meeting the same standards of a large firm. Though limited, there are empirical studies that infer compliance costs are generally

regressive in nature and do not scale with firm size. In particular, for smaller firms the compliance cost could pose excessive burden and may exceed potential benefits from regulation (Eldridge and Kealey, 2005) and often forces firms to go private (Engel et al. 2007). The larger firms, unlike smaller firms, tend to have more financial resources and manpower, and enjoy economies of scale (Weidenbaum 1979). As a result, they have the discretionary power to allocate larger resources to implement necessary policies and safeguards to comply with regulatory requirements. Hence, we hypothesize:

*H4. Larger Hospitals are more likely to be compliant with privacy, security, and transaction rules of HIPAA.*

**EMR Systems:** the use of EMR systems facilitates enhancing management of patient information through controlled and auditable data access processes and improves data security (Agrawal 2002). These systems could support hospitals in conducting both intra and inter organizational transactions based on standardized data formats, as well enhance hospitals' ability to coordinate with accreditation and regulatory agencies by sharing analysis of patient data (Chaiken 2003). Furthermore, data on patients from EMR systems could be aggregated, after applying de-identifying protocols, into larger data repositories for secondary purposes such as research to improve patient safety, public health, and enhance medical knowledge base (Aspen, et al. 2003). Overall, we expect implementation of EMR systems would have positive influence on hospital ability to comply with HIPAA rules. Thus we hypothesize:

*H5. Hospitals with larger EMR systems installed base are more likely to be compliant with privacy, security, and transaction rules of HIPAA.*

**Control Variable:** in response to meeting the deadlines of HIPAA regulation, many hospitals have hired external consultants to guide them through the implementation process. We expect that such hiring of HIPAA consultants would be most likely done by the hospitals that lack in-house resources, especially knowledge, to address regulatory requirements.

In summary, we hypothesize that propensity to be HIPAA compliant, both at individual rules and overall, of hospitals is associated to five organizational characteristics industry status as IT leaders, tax status, academic status, size of EMR installed base, and hospital size. The associations were empirically tested using secondary data, as described next.

## 4 Research Methods

### 4.1 Data

Empirical data for study was obtained from two different sources. First, data on hospital characteristics including size, tax status, academic status, number of beds, number of EMR systems installed, and perceived level of compliance to privacy, security and transaction rules of HIPAA were obtained from Dorenfest® Institute, which is a research division of the Health Information and Management Systems Society (HIMSS) Analytics. HIMSS conducts annual survey of US hospitals on their inventory of IS investments, strategy and plans. Our data is a subset of survey conducted in the year 2003, when HIMSS surveyed the US hospitals for their status of HIPAA compliance and their investments in information security and privacy. The HIMSS dataset was available in the MS Access databases format. We write several SQL queries to extract necessary raw data for the research purpose. The raw dataset contained information on hospital name, location (city and state), website URL, tax status, academic status, number of beds, perceived level of compliance, and each instance

of installed EMR system. Following other studies in HIT literature we include hospitals with at least 100 beds (Miller and Tucker 2007) The perceived level of compliance was on ordinal scale of <50%, 50-75%, 76-99% and 100% compliant. We created a dichotomous variable with value 1 indicating 100% compliant and 0 otherwise. The EMR systems installed base is count of EMR systems installed in the hospital. The tax status is coded as 1 for non-profit and 0 otherwise. Similarly, academic status of hospital is coded as 1 for academic and 0 otherwise. Second, list of IT leaders ('most wired hospitals') was obtained from the website of the Hospitals & Health Networks (HHN) magazine, a practitioner journal of the American Hospital Association which publishes every year the '100 Most Wired' hospitals and health systems in the US using a benchmarking survey. This list provides information on name of hospital system, location (city and state), and website URL. This annual benchmarking survey asks hospitals to self report on their use of information technology in five key areas including business processes, quality and patient safety, customer service, work force management, and public health and safety (see appendix B for dimensions of benchmarking evaluation criteria). HHN evaluates the survey data using proprietary analysis method and identifies which hospitals have highest performance. The list of top 100 hospitals is published in a special issue of HHN magazine which is also made available on their website. As such, HHN does not publish actual scores obtained by these 100 top ranked hospitals.

The IT leaders list and the dataset from HIMMS is first matched by using name of hospital systems. On closer scrutiny of hospital system names in HIMSS dataset and IT Leaders list, we observed that for several hospital systems the name string did not match correctly due to missing articles (e.g 'The') or reorganized sequence of words or presence of city name in the hospital system name in IT leaders list compared to HIMSS dataset. Therefore, we matched the two dataset by using the website address. This matching led to about 2000+ hospitals. Subsequently, we removed all the records that had missing observations on any of the research variables considered in this study. This further reduced our sample size to 1342 hospitals. Among these matched hospitals the number of hospitals coded as IT leader could be more than 100 because every member hospital of a hospital system coded as IT leader, if the particular hospital system appeared in the IT leader list.

#### ***4.2 Descriptive Statistics and Initial Analysis***

Table 1 gives summary statistics of model variables. Among the 1342 hospitals, 81% are non-profit, 13% academic, and 10% IT leaders. Surprisingly only 24% of the hospitals have hired external consultants. Further, we group hospitals as small, medium, large, and very large hospitals in correspondence with quartiles of bed size (Q1=157, Q2=239; Q3=367). The mean and standard deviations of bed size for small hospitals 125.3 and 17.4, medium hospitals 196.1 and 24.7, large hospitals 297.3 and 37.5, and very large hospitals 542.4 and 181.7 respectively. The mean and standard deviation of number of EMR systems is 3.8 and 1.4 respectively. By year 2003, in our sample, 645% of hospitals self reported as 100% compliant to privacy rule, 18% of hospitals self reported as 100% compliant to security rule, 40% of hospitals self reported as 100% compliant to transaction rule and only 16% of hospitals self reported as 100% compliant to all three HIPAA rules. The substantially large proportion (i.e. 64%) of hospitals reporting full compliance to privacy rule is expected since privacy rule has the earliest deadline among all three rules. Conversely, very small proportion (i.e. 18%) of hospitals reported full compliance to security rule as it has the latest deadline among three rules. The breakdown of hospitals for each variable by hospital size is provided in table 1, as well. The table 2 reports correlation of all model variables using Kendall's Tau-b at 5% significance level. Most of the variables have statistically significant correlation.

As seen in the table 3a, one way ANOVA of IT leaders on remaining model variables suggest on average IT leaders are profit oriented, large hospitals, have higher number of EMR systems installed

and tend to hire external consultants for HIPAA compliance. In terms of achieving full compliance IT leaders are less likely to be compliant with privacy and transaction rules, and more likely to be compliant with security rule when compared with hospitals not considered as IT leaders. The Table 3b and 3c provides similar one way ANOVA for tax status and academic status against level of compliance achieved. For-profit hospitals are more likely to be compliant with privacy rule and transaction rule but less likely to be compliant with security rules. Academic hospitals are more likely to be compliant with privacy and security rules compared to other hospitals. In summary, this preliminary analysis offer partial support to hypotheses H1, H2, and H3. The table 4 provides frequency analysis for compliance status of hospitals against IT leaders, tax status, academic status and if HIPAA consultants were hired. The results are consistent with one way ANOVA analysis.

### 4.3 *Logistic Regression Analysis*

The next step was to examine which of our five hypothesized organizational characteristics better explain the likelihood of hospitals being compliant to HIPAA rules. Four logistic regressions were employed for this purpose: first using the ‘Is 100% compliant to privacy rule’ followed by ‘Is 100% compliant to security rule’, ‘Is 100% compliant to transaction rule’, and ‘Is 100% compliant to all HIPAA rules’ as the dependent variable. In each case, ‘Is IT Leader?’, ‘Is Nonprofit?’, ‘Is Academic?’ were included as dummy variables. The ‘Hospital Size’ as measured by number of beds was a continuous variable. In addition ‘Is HIPAA Consultant Hired?’ was included as dummy variable for control. To examine differential impact of EMR systems installed base, we run two models for each case – one without (Model -1) and another with ‘#EMR Systems’ (Model -2) as independent variable. Table 5 reports Logit regression coefficients and robust standard errors of estimated coefficients. As most of the model variables are correlated (see Table 2), we adjust for error and ran robust Logit models (Agresti 2002; Hosmer and Lemeshow 2000). As seen from the table, all four regression models are statistically significant with Wald’s chi-square statistic significant at 1%.

**IT Leaders:** the beta coefficients for IT Leaders are positive and statistically significant for both models, i.e. with and without #EMR systems in the regression of security compliance (Model -1: 0.48 and Model -2: 0.39) and regression for compliance with all three rules (Model -1: 0.73 and Model -2: 0.64). As compared to one way ANOVA analysis, in the Logit regression analysis, we find that there is no significant difference between hospitals considered as IT leaders and other hospitals in propensity to comply with privacy rules and transaction rules. Whereas the higher tendency to comply with security rules, as reflected by positive coefficient, among IT leaders is consistent with ANOVA analysis. Furthermore, magnitude of beta coefficients reduces by about 9 basis points for both security compliance and for compliance to all three rules together when ‘#EMR Systems’ is included in the analysis. In summary, we find support for H1 when all three rules are considered collectively, whereas among the three rules only security rule is supported.

**Tax Status:** the beta coefficients for non-profit hospitals are statistically significant for both models in all cases, though with negative sign for privacy and transaction rules and positive for others. In particular we observe marginal change in the magnitude of coefficients with inclusion of ‘#EMR Systems’ for all cases - privacy rule (Model -1: -1.40 and Model -2: -1.39), security rule (Model -1: 1.69 and Model -2: 1.72), transaction rule (Model -1: -1.36 and Model -2: -1.35), and compliance to all three HIPAA rules (Model -1: 1.53 and Model -2: 1.56). In terms of marginal impact of including ‘#EMR System s’ into regression varies across all four cases. For compliance to privacy and transaction rules, on the one hand, the magnitude of coefficients reduces by about 1 basis point. On the other hand, magnitude of coefficients for compliance to security rules and all three HIPAA

rules together increases by 3 basis points. In summary, we find support for H2 when all three rules are considered collectively, whereas among the three rules when considered individually we find mixed support for the hypothesis H2.

**Academic Status:** the beta coefficients for Academic hospitals are positive and statistically significant for both models only in the case of compliance to privacy rules (Model -1: 0.62 and Model 2: 0.61). Furthermore, the magnitude of beta coefficient reduces only by 1 basis point on inclusion of ‘#EMR Systems’. The non significant coefficients for the cases of compliance to security rule, transaction rule and all three rules considered collectively indicate that academic hospitals are as likely to be compliant with HIPAA rules as non academic hospitals. In summary we find mixed support for the hypothesis H3.

**Hospital Size:** the beta coefficients for hospital size are consistently positive and statistically significant for all cases. This indicates that larger hospitals are more likely to be compliant with HIPAA regulation when privacy, security and transaction rules considered individually or collectively. The very small magnitude of these coefficients compared to other predictors, is perhaps due to the fact that we include number of beds as measure of hospital size which ranges from 100 to 1868 as opposed to other variables being dichotomous. Furthermore, magnitude of beta coefficients changes nominally for all cases when ‘#EMR Systems’ is included in the Logit regressions. In summary, we find positive support for the hypothesis H4.

**EMR System Installed Base:** the beta coefficients for IT Leaders are positive and statistically significant for the case of compliance to security rule (0.14) and for the case of compliance to all three HIPAA rules considered together (0.13). This indicates that as hospitals increase their investments in EMR systems their propensity to become security compliant becomes higher. However, when all three rules are considered together, we find hospitals are more likely to be HIPAA compliant. The beta coefficients for compliance to privacy rule and transaction rule were not significant. This we find partial support for hypotheses H5 when privacy, security and transaction rules are considered individually, yet in case of compliance to all three rules are considered collectively we find support for the hypothesis H5.

**Control Variable (Is HIPAA Consultant hired?):** the beta coefficients for ‘Is HIPAA Consultant Hired?’ are consistently negative and statistically significant across all cases for both models, i.e. for privacy rule (model -1 and -2: -1.04), for security rule (model -1: -1.49 and Model -2: -1.47), transaction rule (model -1: -1.49 and -2: -1.48) and all three rules collectively (model -1: -1.91 and -2: -1.88). This indicates that majority of the hospitals that have hired external consultants are still far away from being compliant. The magnitude of coefficients while remains unchanged for compliance to privacy rule when ‘#EMR Systems’ are included in regression, for security rule, transaction rule and all three rules considered collectively increases by 2, 1 and 3 basis points respectively. This could be important in the sense that hospitals that hire consultants may improve their compliance status with increase investments in EMR systems.

#### **4.4 Discussion**

In the spirit of materialist perspective of theory on legal environment (Edelman and Suchman 1997), we set out to examine propensity of hospital systems to comply with HIPAA regulation that was enacted in 1996 with enforcement deadlines for information privacy in April 2003, transaction rules in October 2003, and security rule in April 2005. Though, industry survey conducted post compliant suggest lower level of full compliance among US hospitals (AHIMA 2006), industry experts agree that “adhering to the HIPAA Privacy and Security rules are more than just about compliance, they

make sound business sense” (Dr. John Halamka – CIO of CareGroup Health Systems in Boston in Computer World 2001). To enhance our understanding on which type of hospitals are actually complying with HIPAA regulation, we develop a research model by incorporating five hospital characteristics as predictor variables. In addition, since several hospitals have made strategic decisions of hiring consultants to facilitate their HIPAA compliance initiative, we control for such strategy.

As reported in the previous section we find support for several hypotheses. In particular, compliance to all three HIPAA rules – privacy, security and transaction, are considered collectively, we find that larger non-profit hospitals which are considered as IT leaders and have higher installed base of EMR systems are more likely to be HIPAA compliant irrespective of whether they are academic or not. However, compliance to privacy, security and transaction rules when considered individually a different profile set emerges from our analysis. In case of privacy rule on average larger for-profit hospitals, and larger academic hospitals have higher propensity to comply irrespective of whether they are considered as IT Leader or not. However, the former type (i.e. larger for-profit) have higher propensity to comply with privacy compared to latter (i.e. larger academic hospitals). In case of security rules on average larger non-profit hospitals considered as IT Leader and have higher EMR system installed base are more likely to be compliant irrespective of their academic status. For transaction rule, larger for-profit hospitals have higher propensity to comply regardless of whether they are considered as IT Leader or not.

Besides the typical profiles discussed above, it is important to observe that, though with caution, the hospitals in our sample that did not hire consultants were better off. Conventionally, external experts on regulation are beneficial especially if the regulations are new and organization does not have adequate knowledge resources. As such our sample data comes from year 2003, and search of trade literature suggest many CIOs of hospital systems were skeptical of HIPAA consultants. For example, Greg Walton, VP & CIO at Carilion Health System forewarned that "It's really the obligation of the [hospitals] to figure out what they want from a consultant, [or] the consultant is going to run all over them" (Computer World 200).

## 5 Conclusion

Though HIPAA regulation has been enacted with a spirit of reducing healthcare cost, it is expensive endeavor for hospitals to be incompliant with HIPAA rules on information privacy, information security and transaction standards. In this research we set out to explore which type of hospitals are aggressive in becoming HIPAA compliant. We tested five hypotheses and found substantive support for most of them using secondary data on US hospitals. Our findings have important implication to practice and research. On the one hand, while practitioners need to be cautious when hiring consultants, they certainly need to push aggressively for EMR systems adoption to provide better information privacy and security. On the other hand, policy makers need to develop better incentive mechanisms to ensure hospital systems of all types make adequate investments to comply with HIPAA standards. As such the task of regulation enforcement is very complex, policy makers need to take appropriate steps to encourage adoption of HIPAA compliant policy and procedures.

This research, being first of its kind, has several limitations that future research may address. First, the data is somewhat older and comes from early period of HIPAA enforcement. Though using such data may highlight in identifying the early adopters of HIPAA regulation, future research could replicate this study by using post enforcement period. Moreover, longitudinal data could be more valuable in offering better insight to dynamics of HIPAA compliance among US hospitals. Second,

since enactment of HIPAA most of the states have implemented their own regulations on information privacy and information security. As such certain state level regulatory requirements may supersede HIPAA requirements raising further complexity for hospitals. In addition, many hospital systems operate in multiple states and thus are subjected to a complex concoction of privacy and security regulations. Perhaps this could be a reason why level of HIPAA compliance is still low. Future research should examine the effects of state level variations in information privacy and information security. Finally, the construct of IT Leaders was operationalized based on a third party benchmark study of proprietary in nature. Taking this list of IT Leaders at face value may have influenced our results. Future research should validate this list by using appropriate research methodology, e.g. Data Envelopment Analysis and determine if ‘most wired hospitals’ are indeed efficient user of information technology.

Despite the above noted limitations, this research opens up new venues for research in the broader area of information security in health care. For example, HIPAA compliance requires significant investments on technology implementation, training and awareness, compliance personnel, policy formulation and revision, and period audits among others. Future research may examine strategic posture adopted by hospitals in achieving and sustaining HIPAA compliance. Moreover, impact of HIPAA compliance on hospital performance such as financial performance, efficiency, customer satisfaction and care quality could be other fruitful research areas.

## References

1. Agrawal, A. (2002). Return on investment analysis for a computer-based patient record in the
2. Agresti, A. 2002. *Categorical Data Analysis*, Wiley, NJ.
3. AHIMA – The American Health Information Management Association. 2006. “The State of HIPAA Privacy and Security Compliance,” last accessed on Nov. 2008, [http://www.ahima.org/emerging\\_issues/2006StateofHIPAACompliance.pdf](http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf)
4. Anderson J.G. 2007. “Social, ethical and legal barriers to E-health,” *International Journal of Medical Informatics* (76), pp. 480-483.
5. Anderson, G.F., Frogner, B.K., Johns, R.A., and Reinhardt, U.E. 2006. “Health Care Spending and Use of Information Technology in OECD Countries,” *health Affairs* 25(3), pp 819-831.
6. 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
7. 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
8. Ball, M.J. and Gold, J. 2006. “Banking on Health: personal Records and Information Exchange,” *Journal of Healthcare Information Management* 20(2), pp. 71-83.
9. 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.
10. Baron, B.R., and Baron, P. 1980. “A Regulatory Compliance Model,” *Journal of Contemporary Business* 9(2), pp 139-150.
11. Barros, P.P., Pinto, C.G., and Machado, A. 1999. “A Signaling Theory of Excessive Technological Adoption,” *Health Care Management Science* 2, pp 117-123.
12. Bartels, A. 2006. “US IT Spending Benchmarks for 2006,” Forrester Research Report.
13. Baumer, D. L., Earp, J. B., and Payton, F. C. 2000. “Privacy of medical records: IT implications of HIPAA”, *ACM Computers and Society* (30:4), pp 40–47.

14. Bhattacharjee, A., Hikmet, N., Menachemi, N., Kayhan, V.O., and Brooks, R. 2007. "Differential Performance Effects from HIT Investments," *Information Systems Management* 24(1), pp.5-14
15. Borzekowski, R. 2002. "Measuring the Cost Impact of Hospital Information Systems: 1987-1994, Board of Governors of the Federal Reserve System.
16. Braithwaite, J. and Makkai, T. 1991. "Testing and Expected Utility Model of Corporate Deterrence," *Law & Society Review* 25(1), pp 7-40.
17. Burke DE, Wang BBL, Wan TTH, Diana ML (2002) Exploring hospitals' adoption of information technology. *J Med Syst* 26 (4):349-355
18. Campbell, B., Thomson, H., Slater, J., Coward, C., Wyatt, K., and Sweeney, K. 2007. "Extracting Information from Hospital Records: What Patients Think About Consent," *Quality and Safety in Healthcare* (16:6), pp 404-408
19. Chaiken, B. P. (2003a). Clinical ROI: not just costs versus benefits. *J Healthcare Information Management* 17(4), 36-41.
20. Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. 2006. "Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules," *Journal of Medical Systems*, (30:1), pp57-64.
21. Computer World, May 2001. "Beware of Predatory HIPAA Consultants," last accessed on 11/27/2008 at <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,60250,00.html>
22. Corder K (2001) Acquiring new technology: comparing nonprofit and public sector agencies. *Adm Soc* 33(2):194-219
23. Damanpour F (1987) The adoption of technological, administrative, and ancillary innovations: impact of organizational factors. *J Manage* 13(4):675-688
24. Dewar RD, Dutton JE (1986) The adoption of radical and incremental innovations: an empirical analysis. *Manage Sci* 32 (11):1422-1433
25. Earp, J.B., and Payton, F.C. 2006. "Information Privacy in Service Sector: An Exploratory Study of Health Care and Banking Professionals," *Journal of Organizational Computing and Electronic Commerce* (16:2), pp 105-122.
26. Edelman, L.B. and Suchman, M.C. 1997. "The Legal Environments of Organizations," *Annual Review of Sociology* 23, pp 479-515.
27. Eldridge, S., and B. Kealey. 2005. SOX Costs: Auditor attestation under Section 404,
28. Engel, E., R.M. Hayes, and X. Wang. 2007. The Sarbanes-Oxley Act and firms' going private decisions. *Journal of Accounting and Economics* (forthcoming
29. Garg, AX, Adhikari NK, McDonald H, Rosas-Arellano MP, Devereaux PJ, Beyene J, Sam J, Haynes RB. 2005. "Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review," *JAMA* (293:10), pp. 1261-1263.
30. Gottlieb, LK, Stone EM, Stone D, Dunbrack LA, Calladine J. 2005. "Regulatory and policy barriers to effective clinical data exchange: Lessons learned from MedsInfo-ED," *Health Affairs* (24:5), pp. 1197-1204.
31. Hasan, R., and Yurcik, W. 2006. "A Statistical Analysis of Disclosed Storage Security Breaches," *ACM workshop on Storage security and survivability*.
32. Health Privacy Project 2007. "Health Privacy Stories," <http://www.healthprivacy.org>
33. Hikmet, N., Bhattacharjee, A., Menachemi, N., Kayhan, V.O., Brooks, R. 2008. The role of organizational factors in the adoption of healthcare information technology in Florida hospitals," *Health Care Management Science* (11), pp. 1-9
34. Hillestad , R., Bigelow , J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. 2005. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs," *Health Affairs* (24:5), pp.1103-1117

35. Hoffman, S., Podgurski, A. 2006. "In Sickness, Health and Cyberspace: Protecting the Security of Electronic Private Health Information," <http://ssrn.com/abstract=931069>
36. Hosmer, D.W., and Lemeshow, S. 2000. *Applied Logistic Regression*, 2<sup>nd</sup> edn. Wiley, NJ
37. Institute of Medicine (IOM): Committee on Quality of Health Care in America, 2001. *Crossing the Quality Chasm*. Washington DC: National Academy Press.
38. Kaelber, DC, Bates DW. 2007. "Health information exchange and patient safety," *Journal of Biomedical Informatics* (40), pp. S40-S45.
39. Kaiser, J. (2006) "Patient Privacy: Rule to Protect Records may Doom Long-Term Heart Study," *Science*, vol.311, no.5767, pp 1547-1548.
40. Kalorama Information (a division of MarketResearch.com) 2007. "Wireless Opportunities in Healthcare".
41. Kimberly, J.K., Evanisko M.J. 1981. "Organizational innovation: the influence of individual, organizational, and contextual factors on hospital adoption of technological and administrative innovation," *Academy of Management J* 24(4):689–713
42. Kotulic, A.G., Clark, J.G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* 41, pp 597-607.
43. Linder, JA, Ma J, Bates DW, Middleton B, Stafford RS. 2007. "Electronic health record use and the quality of ambulatory care in the United States," *Archives of Internal Medicine* (167:13), pp. 1400-5.
44. Los Angeles Times. April 2008. "Effectiveness of medical privacy law is questioned," last accessed on 11/27/08 <http://articles.latimes.com/2008/apr/09/nation/na-privacy9>
45. Menachemi N, Burkhardt J, Shewchuk R, Burke D, Brooks R (2006) Hospital information technology and positive financial performance: a different approach to ROI. *J Healthc Manag* 51 (1):263–268
46. Menachemi, N., Burkhardt, J., Shewchuk, R., Burke, D., Brooks, R. 2006. "Hospital Information Technology & Positive Financial Performance: A different approach to ROI," *Journal of Healthcare Management* 51(1), pp. 40-59
47. Mercuri, R.T. 2004. "The HIPAA-potamus in Health Care Data Security," *Communications of the ACM* (47:7).
48. Miller RH, and Sim I. 2004. "Physicians' use of electronic medical records: Barriers and solutions," *Health Affairs* (23:2), pp. 116-126.
49. Miller, A.R., and Tucker, C.E. 2007. "Privacy, Network Effects and Electronic Medical Record Technology Adoption," *Proceedings of WEIS*, Carnegie Mellon University.
50. Ness, R.B. 2007. "Influence of the HIPAA Privacy Rule on Health Research," *Journal of American Medical Association* (298:18), pp 2164-2170
51. NIST – National Institute of Standards and Technology. 2005. "An Introductory Resource Guide for Implementing the Health Information Portability and Accountability ACT (HIPAA) Security Rule," NIST Special publication 800-66.
52. NRC – The National Research Council 1997. *For the Record: Protecting Electronic Health Information*
53. OCR – The Office of Civil Rights 2006. HIPAA Administrative Simplification Regulation Text, last accessed on Nov. 2008 <http://www.hhs.gov/ocr/AdminSimpRegText.pdf>
54. Parente, S.T., Van Horn, R.L. 2007. "Valuing Hospital Investment in Information Technology: Does Governance Makes a Difference?" *Health Care Financing Review* 28(2), pp 31-43.
55. Raman, A. 2007. "Enforcing Privacy through Security in Remote Patient Monitoring Ecosystems," *6th International Special Topic Conference on Information Technology Applications in Biomedicine*.

56. Rindfleisch, T.C. 1997. "Privacy, Information Technology, and Health Care," *Communications of the ACM*, (40:8), pp 93 – 100.
57. Robinson JC (2002) Bond-market skepticism and stockmarket exuberance in the hospital industry. *Health Affairs* 21 (1):104–117
58. Shen, J.J., Samson, L.F., Washington, E.L., Johnson, P., Edwards, C., Malone, A. 2006. "Barriers of HIPAA Regulation to Implementation of Health Services Research," *Journal of Medical Systems* (30:1), pp 65
59. Solovy A. 2001. "The big payback: 2001 Survey shows a healthy return on investment for into tech," *Hospitals & Health Networks*, pp. 40-50
60. Turner, G.M. 2002. "HIPAA and the Criminalization of American Medicine," *Cato Journal* 22(1), pp 121-150.
61. 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
62. Weidenbaum, M.L. 1979. *The Future of Business Regulation* Amacom, NY.
63. Whitten, P., Mylod, D., Gavran, G. and Sypher, H. 2008. "Most Wired Hospitals' Rates Patient Satisfaction," *Communications of the ACM* 51(4), pp 96-102.

**Table 1 : Summary Statistics of Hospitals' Characteristics**

Variables	Hospital Size Group [#Beds]				Total N = 1342	
	Small [100-156]	Medium [157-238]	Large [239-367]	Very Large [> 367]		
Is IT Leader?	NO	315(26%)	304(25%)	304(25%)	279(23%)	1202(90%)
	YES	21(15%)	33(24%)	33(24%)	53(38%)	140(10%)
Is Non Profit?	NO	92(36%)	78(31%)	52(20%)	33(13%)	255(19%)
	YES	244(22%)	259(24%)	285(26%)	299(28%)	1087(81%)
Is Academic?	NO	322(27%)	318(27%)	292(25%)	242(21%)	1174(87%)
	YES	14(8%)	19(11%)	45(27%)	90(54%)	168(13%)
Is HIPAA Consultant Hired?	NO	247(24%)	264(26%)	258(25%)	255(25%)	1024(76%)
	YES	89(28%)	73(23%)	79(25%)	77(24%)	318(24%)
Is 100% Compliant to Privacy Rules	NO	141(29%)	109(23%)	126(26%)	108(22%)	484(36%)
	YES	195(23%)	228(27%)	211(25%)	224(26%)	858(64%)
Is 100% Compliant to Security Rules	NO	285(26%)	283(26%)	283(26%)	245(22%)	1096(82%)
	YES	51(21%)	54(22%)	54(22%)	87(35%)	246(18%)
Is 100% Compliant to Transaction Rules	NO	212(26%)	197(25%)	209(26%)	184(23%)	802(60%)
	YES	124(23%)	140(26%)	128(24%)	148(27%)	540(40%)
Is 100% Compliant to All HIPAA Rules	NO	293(26%)	290(26%)	289(26%)	254(23%)	1126(84%)
	YES	44(20%)	47(22%)	47(22%)	78(36%)	216(16%)
# EMR Systems*		3.7(1.4) [0-6]	3.8(1.5) [0-6]	3.7(1.3) [0-6]	4.1(1.3) [0-6]	3.8(1.4) [0-6]
Hospital Size (#Beds)*		125.3(17.4) [100-156]	196.1(24.7) [157-238]	297.3(37.5) [239-367]	542.4(181.7) [368-1868]	289.5(183.1) [100-1868]

\* Summary statistics for these variables indicate average count (std. dev. Of count) and [range of count]

Note: For all the variables, except marked \*, summary statistics indicate frequency distribution.

**Table 2 : Correlation of Hospital Variables (Kendall's Tau at 5% significance level )**

Variables	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[1] Is 100% Compliant to Privacy Rules	1								
[2] Is 100% Compliant to Security Rules	0.32*	1							
[3] Is 100% Compliant to Transaction Rules	0.48*	0.49*	1						
[4] Is IT Leader?	-0.053	0.046	-0.07*	1					
[5] Is Non Profit?	-0.22*	0.17*	-0.28*	0.16*	1				
[6] Is Academic?	0.09*	0.08*	-0.073	-0.019	0.14*	1			
[7] Hospital Size (#Beds)	0.06*	0.08*	0.042	0.09*	0.14*	0.22*	1		
[8] Is HIPAA Consultant Hired?	-0.25*	-0.16*	-0.28*	0.21*	0.17*	-0.047	-0.013	1	
[9] # EMR Systems	0.040	0.09*	0.041	0.10*	0.001	0.08*	0.06*	-0.039	1

**Table 3a: One way ANOVA for IT Leaders on Hospital Characteristics**

Variables	Is IT Leader?		F Statistic
	NO	YES	
Is Non Profit?	0.789(0.408)	0.993(0.085)	34.79 ***
Is Academic?	0.127(0.333)	0.107(0.31)	0.46
Is HIPAA Consultant Hired?	0.206(0.405)	0.5(0.502)	62.51***
Hospital Size (#Beds)	284.15(182.91)	335.08(178.92)	9.77 ***
# EMR Systems	3.782(1.387)	4.221(1.536)	12.29 ***
Is 100% Compliant to Privacy Rules	0.648(0.478)	0.564(0.498)	3.82 **
Is 100% Compliant to Security Rules	0.177(0.382)	0.236(0.426)	2.87 *
Is 100% Compliant to Transaction Rules	0.413(0.493)	0.307(0.463)	5.91 **
Is 100% Compliant to All HIPAA Rules	0.153(0.360)	0.229(0.421)	5.23 **

**Table 3b: One way ANOVA for Non Profit Hospital Vs. Compliance Status**

Variables	Is Non Profit		F Statistic
	NO	YES	
Is 100% Compliant to Privacy Rules	0.855(0.353)	0.589(0.492)	66.49***
Is 100% Compliant to Security Rules	0.051(0.220)	0.214(0.410)	37.81***
Is 100% Compliant to Transaction Rules	0.682(0.466)	0.337(0.473)	110.95***
Is 100% Compliant to All HIPAA Rules	0.051(0.220)	0.187(0.390)	28.76 ***

**Table 3c: One way ANOVA for Academic Hospitals Vs. Compliance Status**

Variables	Is Academic		F Statistic
	NO	YES	
Is 100% Compliant to Privacy Rules	0.623(0.485)	0.750(0.434)	10.26***
Is 100% Compliant to Security Rules	0.172(0.377)	0.262(0.441)	7.96***
Is 100% Compliant to Transaction Rules	0.404(0.491)	0.393(0.490)	0.07
Is 100% Compliant to All HIPAA Rules	0.152(0.359)	0.226(0.419)	6.07**

Note: \*\*\* p<0.01, \*\* p<0.05, \* p<0.1

**Table 4: Frequency Analysis on Hospital Characteristics Vs HIPAA Compliance**

Characteristics	# Hospitals	Is 100% Compliant to Privacy Rules		Is 100% Compliant to Security Rules		Is 100% Compliant to Transaction Rules		Is 100% Compliant to All HIPAA Rules	
		YES	Chi -Sqr	YES	Chi -Sqr	YES	Chi -Sqr	YES	Chi -Sqr
Is Non Profit? YES	1,087	640 (58.88)	63.44***	233 (21.44)	36.82***	366 (33.67)	102.62***	203 (18.68)	28.19***
Is IT Leader? YES	140	79 (56.43)	3.82 *	33 (23.57)	2.87*	43 (30.71)	5.89**	32 (22.86)	5.29**
Is Academic? YES	168	126 (75)	10.19***	44 (26.19)	7.92***	66 (39.29)	0.072	38 (22.62)	6.05**
Is HIPAA Consultant Hired? YES	318	135 (42.45)	83.4***	24 (7.55)	32.37***	49 (15.41)	106.86***	15 (4.72)	39.95***

Note 1: he proportion of hospitals are shown in parentheses

**Table 5: Logit Regression Coefficients for Hospitals' Compliance to Privacy, Security and Transaction Rules**

VARIABLES	Is 100% Compliant to Privacy Rules		Is 100% Compliant to Security Rules		Is 100% Compliant to Transaction Rules		Is 100% Compliant to All HIPAA Rules	
	Model - 1	Model - 2	Model - 1	Model - 2	Model - 1	Model - 2	Model - 1	Model - 2
Is IT Leader	0.16 (0.1785)	0.14 (0.1795)	0.48** (0.2338)	0.39* (0.2312)	0.17 (0.1994)	0.13 (0.1982)	0.73*** (0.2436)	0.64*** (0.2409)
Is Non-Profit	-1.40*** (0.1975)	-1.39*** (0.1974)	1.69*** (0.3019)	1.72*** (0.3051)	-1.36*** (0.1556)	-1.35*** (0.1561)	1.53*** (0.3028)	1.56*** (0.3061)
Is Academic	0.62*** (0.2023)	0.61*** (0.2021)	0.13 (0.2152)	0.10 (0.2158)	-0.04 (0.1938)	-0.05 (0.1952)	0.12 (0.2259)	0.10 (0.2265)
Hospital Size (#Beds)	0.0008** (0.0004)	0.0008** (0.0004)	0.0010** (0.0004)	0.0009** (0.0004)	0.0009*** (0.0003)	0.0009** (0.0003)	0.0008** (0.0004)	0.0007* (0.0004)
Is HIPAA Consultant Hired	-1.04*** (0.1359)	-1.04*** (0.1359)	-1.49*** (0.2487)	-1.47*** (0.2458)	-1.49*** (0.1825)	-1.48*** (0.1819)	-1.91*** (0.3093)	-1.88*** (0.3055)
# EMR Systems		0.035 (0.0427)		0.14** (0.0537)		0.05 (0.0445)		0.13** (0.0571)
Constant	1.71*** (0.2042)	1.58*** (0.2464)	-3.10*** (0.3117)	-3.62*** (0.4043)	0.71*** (0.1578)	0.53** (0.2311)	-3.04*** (0.3114)	-3.54*** (0.4142)
# Observations	1342	1342	1342	1342	1342	1342	1342	1342
Wald's Chi-Sqr	120.77***	120.15***	73.67***	74.97***	157.36***	157.77***	66.9***	68.12***

Note 1: Robust standard errors in parentheses

Note 2: \*\*\* p<0.01, \*\* p<0.05, \* p<0.1

## Appendix A: An Example of how a ‘Most Wired’ Hospital Signals the Market for being Technology Leader

The screenshot shows the Avera website homepage. The URL is <http://www.avera.org/avera/index.aspx>. The page layout includes a search bar at the top right, a navigation menu on the left, and a main content area. A prominent banner reads "THE MOST POPULAR BABY NAME AROUND? IT'S AVERA." Below this, there are sections for "Avera, quality health care nearby home – Look no further.", "Wellness Tools", and "Today's Scripture & Reflection". A red box highlights a "Quality Indicators" section featuring a "MOST WIRED" award logo from 2008, labeled "Technology Leader".

## Appendix B: Evaluation Criteria used by American Health Association for identifying ‘most wired hospitals’

<b>Business Processes</b>	Automate the supply chain Automate patient eligibility and financial transactions with insurance and payers Automate the business office and financial operations
<b>Quality and Safety</b>	Reduce errors in prescribing and ordering medications Reduce errors in the administration of medications Improve clinical decision making by providing physicians and clinicians with access to electronic health record for their patients Improve clinical decision making by providing real-time clinical alerts to assist physicians and other clinicians at the point of care Reduce adverse events by electronically monitoring patients and using surveillance systems to alert physicians and other clinicians about changes in a patient's condition
<b>Customer Service</b>	Improve the efficiency of administrative services to patients, e.g., pre-registration Assist patients in researching and tracking their own conditions Provide the general public with health information and resources to improve their health
<b>Work Force</b>	Assist in the recruitment, selection, and training of qualified personnel Provide extensive training and support to hospital staff on information systems Use work force management tools to ensure adequate staffing and measure staff performance
<b>Public Health and Safety</b>	Deployment of security technologies to safeguard confidential patient information Deployment of web-based personal health record Participate in local, regional, and national cooperatives to share health information Use evidence-based standards to monitor and improve the hospital's performance

Source: Adopted from Whitten, et al (2008)