

PRIVACY AND SECURITY OF ELECTRONIC INFORMATION
FOR HIPAA COMPLIANCE IN U.S. HOSPITALS

Diane C. Davis, Ph. D.
Information Management Systems, College of Applied Sciences and Arts
Southern Illinois University
Carbondale, IL 62901
dcdavis@siu.edu
(618) 453-7296

and

Karen M. Having
Department of Health Care Professions, College of Applied Sciences and Arts
Southern Illinois University
Carbondale, IL 62901
khaving@siu.edu
(618) 453-4950

PRIVACY AND SECURITY OF ELECTRONIC INFORMATION
FOR HIPAA COMPLIANCE IN U.S. HOSPITALS

Abstract

A study of 1,000 randomly selected U.S. hospitals was conducted to identify (1) the perceptions of HIPAA officers regarding the level of compliance attained toward meeting the security standards and (2) the security methods, hardware devices and software systems utilized. Usable surveys were received from 286 hospitals yielding a response rate of 28.6%. The top two security standards in which the respondents indicated the highest level of compliance were in obtaining required business associate agreements and in physical safeguards to limit access to electronic information systems. The two that were the farthest from compliance was policies for addressing security incidents and performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule. The security methods, devices, and tools most commonly used were firewalls (73%), electronic authorization for entry into secure areas (58%), virtual private networks (43%), and secure web servers (37%).

Keywords: HIPAA, security, privacy, healthcare

Introduction and Purpose of the Study

With the widespread use of the Internet and increased use of networks throughout businesses and organizations, the amount of information stored electronically has grown exponentially. This increase in the storage of electronic data has led to more and more concerns regarding privacy and security of electronic information. Identity theft and other fraudulent activities are producing a greater need for trained IT managers and solid IT budgets. The consensus among industry analysts in 2002 was that the global information security marketplace would grow at more than double the rate of the larger IT market in the next few years. This predicted growth in security has already been proven. Research conducted by Datamonitor (2004, p. 1) found “combined revenues of 22 of the largest publicly listed pure-play IT security vendors grew 14 percent last year [2003].” However, it is important to note that an IT manager must be able to look beyond the concept of installing firewalls, intrusion detection systems, and antivirus software toward the policies and procedures for meeting the goals of the organization.

IT managers must be able to understand how technology supports the goals and how the organization uses the information to carry out the day-to-day business operations.

Currently the healthcare industry is being put to the test with federal legislation to protect the privacy and security of information with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. According to Halamka, CIO of CareGroup Health Systems in Boston (as cited in Ferrarini), “Adhering to the HIPAA privacy and security rules are more than just about compliance, they make sound business sense” (2003, p. 34). Most healthcare entities realize that the patients have entrusted them with protecting their confidential records and it is a responsibility that must be taken very seriously. A breach by a hacker could jeopardize the trust of the patients in any healthcare entity. This is the same concern that other industries have in regard to protecting private information regarding their customers, clients, and business partners.

In order to better understand the effect of HIPAA on security policies and practices in the healthcare industry, a study was conducted to identify the policies, procedures, and devices that hospitals in the United States are using to meet HIPAA compliance and to determine the perceived level of compliance to specific security standards of the Security Rule.

Review of Literature

HIPAA was signed into law on August 21, 1996, and modified by the Administrative Simplification Compliance Act on December 27, 2001. The Department of Health and Human Services (DHHS) was charged with implementing the Act and establishing regulations for accessing, transmitting, and storing health information. These regulations mandated by HIPAA include standards related to electronic transmission of data and those designed to ensure the security and privacy of health information. DHHS estimated that \$29.9 billion would be saved over 10 years due to the efficiency that would be gained in administrative processes and

procedures (Maddox, 2003). All healthcare organizations including healthcare providers, physician offices, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, and service organizations are affected by the Security Rule (Phoenix Health Systems, 2003). “It mandates that electronically stored personal health information be kept confidential and protected against unauthorized users and any threats to its security or integrity” (Birnbach and Gametchu, 2003).

Since the HIPAA legislation had to be followed by everyone from the small single-doctor practice to the largest hospital, one of the biggest challenges that the authors of the security rule faced was how to codify information security standards and implementation specifications that could be understood and imposed fairly on a group of organizations that differed greatly in scale (Smith, 2003). The solution was to incorporate a set of security standards inside the final Security Rule that would apply to everyone along with a set of implementation specifications that applied selectively. Some of the implementation specifications were required and others were considered addressable. “Covered entities were not required to implement those that, in view of the organization’s size and the availability of resources, were either ‘inappropriate’ or ‘unreasonable’” (Smith, 2003, p. 17). According to Smith (2003), the required implementation specifications include risk analysis, risk management, sanctions policy, information system activity review, isolation of clearinghouse functions, incident response, backup, disaster recovery, emergency mode of operation, business associate contracts, disposal, media re-use, unique user identification, emergency access procedure, and documentation. These were categorized into three groups of safeguards to establish a minimum level of protection—administrative safeguards, physical safeguards, and technical safeguards. The regulations became effective on April 21, 2003, and the deadline for compliance with these requirements is

April 21, 2005. “Small health plans have until April 21, 2006, to comply with the rule”
(Fitzgerald, 2004).

Methodology

A survey instrument was developed based on a review of the literature. It was designed to gather answers to the research questions listed below. The survey instrument was reviewed by a panel of experts which included medical personnel and information systems personnel in local hospitals. Revisions were made to the survey instrument based on the comments of the reviewers. The survey was then approved by the Human Subjects Committee at the university employing the researchers prior to pilot testing. Next, the survey was sent to ten randomly selected hospitals from a national list of hospitals for pilot testing. It was also reviewed by three attendees at the HIPAA E-Security conference held in St. Louis, Missouri, in October 2003. Comments from these experts were reviewed and used as feedback for final revision of the instrument.

A database of 1000 randomly selected member hospitals of the American Medical Association was purchased from Third Wave Research. A mailing including a cover letter, survey instrument, and self-addressed return envelope was sent the last week of 2003 and surveys were received by HIPAA officers the first week of January 2004. A follow-up mailing was sent the second week of February. There were 286 usable surveys returned for a response rate of 28.6%. Responses were coded onto Scantron sheets and tabulated using the Statistical Analysis Systems (SAS), Version 6.11.

Research Questions

The research questions for this study were as follows:

1. What are the characteristics, duties, and responsibilities of the individuals serving as HIPAA compliance officers in U.S. hospitals?
2. What are the perceptions of the HIPAA officers regarding their facility's current administrative, physical, and technical HIPAA compliance status in regard to privacy and security?
3. Is there a significant difference in the HIPAA officers' perceptions of the level of compliance toward the security standards based on the size of the hospital?
4. What methods, hardware devices, software tools, and information systems' management practices are employed by U.S. hospitals in meeting HIPAA compliance?

Findings

Demographics

The largest number of respondents indicated that the total number of beds in their healthcare system was less than 250. Specifically, 108 of the 286 hospitals (41%) were part of an integrated healthcare system. Table 1 shows the responses regarding the size of the hospital system.

Table 1
Size of Healthcare System

Number of Beds	Number	Percent
Less than 250 beds	168	61.99
250 to 499 beds	29	10.70
500 to 999 beds	20	7.38
1000 to 1999 beds	26	9.59
2000 or more beds	28	10.33

When the respondents were asked which of the listed titles best matched their job description, the largest number of respondents indicated the title of "Privacy Officer." This question was designed for the respondent to mark only one answer. However, some respondents

marked more than one, so all answers were tabulated. Forty-six percent indicated that Privacy Officer matched their job title and 32% indicated HIPAA Officer. Job titles indicated by the respondents can be seen in Table 2.

Table 2
Job Titles

Title	Number	Percent
HIPAA Officer	91	31.82
Privacy Officer	132	46.15
Security Officer	19	6.64
Compliance Officer	52	18.18
Health Information Manager	29	10.14
Other	41	14.34

The respondents were also asked what new job titles had been created at their facility to meet HIPAA compliance. This time they were asked to mark all that applied. The largest number of respondents (78%) indicated a new job title was created for Privacy Officer, 56% indicated a new title for Security Officer, and 35% for HIPAA Officer.

A large majority of the respondents (89%) indicated that no new person outside the system was hired for any of the above listed job titles. Of the 11% that did hire an outside person, the largest number indicated the new position was for a Privacy Officer. The largest number of the individuals performing HIPAA related-duties (50%) came from the medical records department, 29% from information systems, and 29% from hospital administration.

Characteristics, Duties, and Responsibilities of the HIPAA Officers

When asked what areas of responsibility the HIPAA officer engaged in on a recurrent basis, the majority of the respondents said privacy issues, training, compliance administration, and security issues.

Although the majority of the respondents (63%) indicated that they spent 25% or less of their time on HIPAA related duties, it is interesting to note that 26% spent 26% to 50% of their time on these duties, 4% spent 51% to 75% to their time, and another 4% spent 76% to 100% of their time working with HIPAA requirements.

Level of Compliance Toward Security Standards

The respondents were asked to mark the level of compliance they felt their facility had attained in the following areas on a scale of 1 to 5 (with 5 being the highest level of compliance). The top two security standards in which the respondents indicated the highest level of compliance were (1) policies/procedures in obtaining required business associate agreements and (2) policies/procedures in physical safeguards to limit access to electronic information systems. The two that were the farthest from compliance were (1) policies for addressing security incidents and (2) policies for performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule. The results are shown in Table 3 in order of mean; however, the data in the table shows the frequency for each number on the Likert scale.

Table 3
 Level of Compliance of Security Standards (5 Being Most Compliant)

Security Standard	1	2	3	4	5	NA
Policies/procedures for obtaining required business associate agreements.	10	11	39	82	137	0
Policies/procedures for physical safeguards to limit access to electronic information systems with facility access controls, workstation use and security, and device and media controls.	11	20	60	112	74	1
A security manager responsible for implementing and maintaining the requirements of the Security Rule.	25	31	51	74	94	3
Policies/procedures for information access management (authorizing access to electronic protected health information (EPHI) consistent with requirements).	17	36	75	87	57	7
Policies/procedures for workforce security (ensuring all members have appropriate access to EPHI and preventing access to EPHI to those who should not have it).	17	39	71	91	59	1
Policies/procedures for technical safeguards to provide access control, audit controls, integrity, person or entity authentication, and transmission security.	16	39	78	91	51	1
A contingency plan for responding to an emergency or other occurrence of damage (such as a data backup plan, a disaster recovery plan, and an emergency mode operation plan).	17	53	75	84	49	1
Program for security awareness and training for hospital personnel (including protection from malicious software and monitoring log-in attempts and password management).	29	51	75	72	52	1
A security management process including risk analysis, risk management, sanction policies, and review of IS activities.	26	51	73	85	42	1
Policies/procedures for addressing security incidents (a response and reporting plan).	37	52	77	71	41	1
Policies/procedures for performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule.	47	68	72	67	23	1

Differences Based on Size of Healthcare System

An analysis of variance (ANOVA) was performed to determine if the level of perceived compliance at the respondent’s facility was based on the size of the healthcare system of the respondent. The overall F test using an alpha level of 0.05 did reveal a significant difference among groups with different size healthcare systems (see Table 1) in 6 of the 11 areas. Table 4 shows each listed with the F value and probability; those marked with an asterisk were significant.

Table 4
Differences of Compliance Level Based on Size of Healthcare System

Security Standard	F Value	Prob.
Policies/procedures for obtaining required business associate agreements.	2.31	0.0585
Policies/procedures for physical safeguards to limit access to electronic information systems with facility access controls, workstation use and security, and device and media controls.	4.42	0.0018*
A security manager responsible for implementing and maintaining the requirements of the Security Rule.	1.00	0.4064
Policies/procedures for information access management.	1.00	0.4071
Policies/procedures for workforce security.	1.61	0.1732
Policies/procedures for technical safeguards to provide access control, audit controls, integrity, person or entity authentication, and transmission security.	4.30	0.0022*
A contingency plan for responding to an emergency or other occurrence of damage.	6.08	0.0001*
Program for security awareness and training for hospital personnel.	5.35	0.0004*
A security management process including risk analysis, risk management, sanction policies, and review of IS activities.	2.58	0.0381*
Policies/procedures for addressing security incidents (a response and reporting plan).	4.36	0.0020*
Policies/procedures for performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule.	3.89	0.0043*

^a df = 4

*p < 0.05

Methods, Devices, and Tools Used to Provide Security

The majority of respondents (58%) indicated they used electronic authorization for entry into secure areas (such as swipe cards or access codes) and 41% employed a security guard or other security personnel when asked about the physical on-site methods used to provide security. Only 5% indicated they used a service provider for physical on-site security.

Almost half of the respondents (46%) indicated that they did not have an Incident Response Team. Of those that did have an Incident Response Team, the Privacy Officer and/or HIPAA Officer were the ones held responsible for these issues.

Over one-third of the respondents (35%) indicated they were using outside consultants for one of the three main aspects of HIPAA (privacy, transactions, and security). Of those, 21% said they had consultants for security, 19% for privacy, and 19% for transactions. Many of these were using consultants for two or more of these three areas.

The respondents were asked to mark all security devices or software systems currently being utilized by their facility. The only device used by over a majority of the respondents was some type of firewall. Other devices used are shown in Table 5.

Table 5
Devices Used for Security

Hardware/Software	Number	Percent
Firewalls	209	73.08
VPN to connect remote facilities or users	125	43.71
Secure web servers	104	36.36
Dial-up user access	88	30.77
Wireless access points	70	24.48
Wireless encryption	56	19.58
Handheld wireless devices	52	18.18
Groupware servers	51	17.83
Intrusion detection systems (IDS)	48	16.78
Biometric systems	13	4.55

Summary and Discussion of the Findings

The majority of the healthcare systems surveyed (62%) were those with less than 250 beds. The largest number of respondents (46%) indicated that the title that best matched their job title was Privacy Officer. The responsibilities that a majority of the respondents engaged in on a recurrent basis related to privacy, training, security, and compliance administration. The majority of the respondents (63%) indicated that they spent 25% or less of their time on HIPAA related duties; however, 26% of the respondents spent 26% to 50% of their time on these duties.

The top two security standards in which the respondents indicated the highest level of compliance were in obtaining required business associate agreements and in physical safeguards to limit access to electronic information systems. The two that were the farthest from compliance were policies for addressing security incidents and performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule. An overall F test did indicate a significant difference in perceived level of compliance obtained for several of the security standards based on size of the healthcare system. This might be expected since it is likely more difficult for smaller systems to incorporate technology needed and implement change as quickly as larger healthcare systems that may have greater resources.

The majority of respondents (58%) used electronic authorization for entry into secure areas (such as swipe cards or access codes) and 41% employed a security guard. A large majority (73%) used firewalls to provide some security on their computer systems, and many used virtual private networks and secure web servers. Only slightly over half of the hospitals (54%) had an incident response team which indicates that this is an area they still need to focus on in order to make sure the security policies are followed, evaluated, and maintained. Many of the hospitals (35%) were using outside consultants for one of the three main aspects of HIPAA (privacy,

transactions, and security) which demonstrates the need for students in the field of information systems who may desire to be consultants to be aware of federal legislation and how it affects various industries.

The findings illustrate that significant time and energy has been committed by the healthcare industry on reaching compliance of HIPAA and maintaining privacy and security of electronic health information. They confirm the impact that federal legislation has in general on business and industry. By having a working knowledge of HIPAA as well as other legislation, such as the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act, students in the field of information systems will be better able to understand what businesses go through to reach compliance and how employees must adjust to cultural change within organizations.

The findings also indicate that in healthcare systems, it is often easier to implement physical safeguards to protect information and establish a security manager who will be responsible than to develop and implement procedures to address security incidents and establish a response and reporting plan. Other challenging areas for healthcare systems and other businesses are to perform those most needed periodic technical and non-technical evaluations of security practices. Reporting and evaluation have often been areas that have been overlooked by businesses in many areas of systems development (not just related to privacy and security).

This study reinforces the importance of including the development of solid security policies and the ability to conduct security reporting, evaluation, and maintenance of the policies in curricula for information systems. The curricula must not only include the methods, devices, and systems that industries are using to provide security of information (as discovered in studies like this), but it is also essential for students to understand why devices are used, how employees must accept change, and how they must be involved in the process of lifelong learning.

References

- Birnback, D. S. & Gametchu, M. (2003, April 30). How HIPAA's security rule could affect IT. Computerworld. Retrieved May 14, 2003, from www.computerworld.com/printthis/2003/0,4814,80816,00.html
- Datamonitor (2004, April 6). Security budgets soared in 2003. *The Register*. Retrieved September 28, 2004 from http://www.theregister.co.uk/2004/04/06/datamonitor_security2003
- Ferrarini, E. M. (2003, Spring). Best practices for security and privacy make good business sense. *Disaster Recovery Journal*, 16(2), 34-47.
- Fitzgerald, T. (2004). The final HIPAA security rule is here! Now what? In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (pp. 1919-1935). Boca Raton, FL: CRC Press LLC.
- Maddox, P. J. (2003, February). HIPAA: Update on rule revisions and compliance requirements. *MEDSURG Nursing*, 12(1), 59-63.
- Phoenix Health Systems. (2003). HIPAA Advisory—HIPAA primer. Retrieved March 12, 2003, from <http://www.hipaadvisory.com/regs/HIPAAprimer1.htm>
- Smith, H.E. (2003, October). The HIPAA final security rule – more than a new security standard. *The ISSA Journal*, 16-19.