

HIPAA Compliance in U.S. Hospitals: A Self-Report of Progress Toward the Security Rule

by Karen Having, MS Ed, RT(R), RDMS, and Diane C. Davis, PhD

Abstract

In January 2004, a random sampling of 1,000 U.S. hospitals was surveyed by researchers at a midwestern university to determine perceived level of compliance with the security requirements of the federal Health Insurance Portability and Accountability Act (HIPAA). Exactly one year later, a follow-up survey was sent to the 286 respondents of the 2004 survey, yielding a 50 percent return rate (n = 144). There was an overall trend in increased HIPAA security compliance from 2004 to 2005. There was no significant difference in perceived level of compliance based on the size of the hospital for the majority of security standards.

Key Words: HIPAA, security, compliance, healthcare, hospitals

Introduction and Purpose of the Study

Implementation of the federally mandated Health Insurance Portability and Accountability Act (HIPAA) has impacted all aspects of healthcare delivery. The primary intent of HIPAA was to safeguard the privacy of patient records. As stated by Fitzgerald, "True privacy of information cannot be achieved without adequate security controls."¹ This legislation has, therefore, directly impacted the accountability of the information systems and technologies provided at all medical facilities. Minimal information has been reported regarding progress toward compliance with HIPAA security standards and the associated challenges encountered.

The purpose of the study was to identify the progress toward perceived level of compliance with the security standards. The need existed to identify organizational strategies for implementation of the standards as well as general threats, problems, and solutions related to providing a private and secure environment for electronic protected health information (EPHI). The findings are being reported as a benchmark for comparison among healthcare institutions regarding progress toward achieving compliance with the security standards. This information may indicate areas of concern to be addressed by those responsible for information security and health information management.

Background and Literature Review

HIPAA was signed into law on August 21, 1996, and was modified by the Administrative Simplification Compliance Act on December 27, 2001. The regulations became effective on April 21, 2003, and the deadline for compliance with these requirements was April 21, 2005. However, as stated by Fitzgerald, “small health plans have until April 21, 2006, to comply.”²

The Department of Health and Human Services (DHHS) was charged with implementing HIPAA and establishing regulations for accessing, transmitting, and storing health information. The regulations mandated “that electronically stored personal health information be kept confidential and protected against unauthorized users and any threats to its security or integrity.”³ 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.⁴

One of the biggest challenges presented by the security rule of HIPAA 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. The solution was to incorporate a set of “required,” mandatory security standards and a set of specifications that were “addressable.” Addressable standards were not required to be implemented by organizations for which, in view of the organization’s size and available resources, the standards were either “inappropriate” or “unreasonable.” According to Smith, the required implementation specifications include safeguards related to risk analysis, risk management, sanctions policies, information system activity review, isolation of clearinghouse functions, incident response, backup, disaster recovery, emergency modes of operation, business associate contracts, disposal, media reuse, unique user identification, emergency access procedures, and documentation. These were categorized into three groups of safeguards to establish a minimum level of protection—administrative safeguards, physical safeguards, and technical safeguards.⁵

HIPAA aligns with other legislation such as the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOXA), which require organizations to develop policies and procedures to assist them in mitigating their liabilities under federal regulation. The literature contains many guidelines for developing and implementing security policies to assist in reaching compliance. “An organization’s first step toward the secure information path is a comprehensive and structured information classification process.”⁶ Once a security process, plan, or policy is in place, it must be implemented, maintained, and evaluated. According to Amatayakul, implementation of effective and efficient policies and procedures for HIPAA security incident reporting involve three basic steps: (1) clearly define for the medical staff what constitutes a “security incident,” (2) institute procedures to collect and document each security incident, and (3) respond to the reported incidents in a timely and appropriate manner.⁷ Others have provided tools to help organizations gauge progress toward security compliance, perform reassessment, and make appropriate changes to insure HIPAA compliance beyond the 2005 deadline.⁸⁻¹⁰

In regard to the status of HIPAA compliance, one recent study identified in the literature was the 2005 American Health Information Management Association (AHIMA) study, which was based on 1,140 responses, with 51 percent from the hospital setting. Full security compliance was reported by 17 percent; however, 12 percent still felt they were less than 50 percent compliant as of January 2005.¹¹ The Healthcare Information and Management Systems Society (HIMSS) and Phoenix Health Systems have also conducted regular surveys of their members and newsletter subscribers to analyze HIPAA compliance. Their winter 2005 report (conducted in January 2005), which consisted of 318 provider participants and 82 payer participants, reported 18 percent of providers to be fully compliant with HIPAA security regulations. In fact, HIMSS and Phoenix Health Systems found that the number of organizations that expected to be compliant by April 2005 actually dropped from the number reported six months earlier. “Only 74 percent of providers (down from 87 percent) indicated they [would] be compliant on or before the deadline.”¹²

The 2005 AHIMA study also found that 89 percent of the facilities surveyed had a designated security officer; 42 percent of respondents said the role of the security officer was full-time, and the

majority (61 percent) of the respondents filling this role were information systems (IS) or information technology (IT) employees. There were multiple other self-described roles reported, each with a frequency of less than 10 percent. As suggested in the AHIMA report, “The relatively high number of ‘other’ responses reflects small institutions’ need to share the load among administrators and individuals with skills in organization, auditing, and so forth.”¹³

The objectives of this study were to answer the following research questions:

1. What are the organizational strategies employed by U.S. hospitals as they adapt to the HIPAA security requirements?
2. What are the perceptions of the HIPAA compliance officers regarding their facility’s current administrative, physical, and technical HIPAA security compliance status?
3. Is there a significant difference in perceptions of HIPAA security compliance at different hospitals based on their size?
4. What do HIPAA compliance officers see as their facility’s greatest information security threats and what solutions do they suggest to solve and/or prevent these threats?

Methodology

After a thorough review of the literature and study of the HIPAA regulations, a pencil-and-paper survey instrument was developed to examine the privacy and security policies used by hospitals in the United States. There were four main parts to the survey: (1) the demographic characteristics of the respondents, (2) the facility’s strategies for achieving HIPAA compliance, (3) the perceptions of the respondents (HIPAA officers) regarding their level of compliance with the security requirements, and (4) perceived threats, problems, and solutions related to electronic protected health information (EPHI) security. Upon receipt of institutional approval for research using human subjects, the survey instrument was reviewed for content validity by a panel of experts consisting of four medical and information systems personnel in local medical facilities and three participants at a HIPAA E-Security national conference. Upon appropriate revision, the survey was sent to 10 randomly selected hospitals from a national list of hospitals for pilot testing and final revision.

The survey was then mailed to the HIPAA officer at 1,000 hospitals randomly selected from a fiscal year 2001 American Hospital Association (AHA) database. Each participant received a cover letter stating the intent of the survey, a statement of voluntary participation, a notice of Human Subjects Committee approval, assurance of confidentiality, and contact information for investigators; the survey instrument; and a postage-paid return envelope. The initial mailing was sent during the first week of January 2004, and a second mailing was sent to nonrespondents during the second week of February. All responses were then converted to Scantron sheets for analysis (Scantron Corp., Irvine, CA). A coding accuracy test was performed on a sample of the responses. Data were analyzed using SAS Version 8.

One year later, a shortened version of the initial survey instrument was sent to all respondents to the 2004 study for the purpose of determining (1) changes in perception of compliance with the HIPAA security rule and (2) strategies for achieving HIPAA compliance and commonly stated security threats, problems, and solutions. The contents of the mailing, the process of sending a second mailing to nonrespondents, and data collection and analysis procedures mirrored the methodology of the 2004 study.

Results

The results of the 2005 survey reflect the status of the responding hospitals ($n = 144$) with a time frame of less than three months remaining to comply with the established security standards section of the HIPAA mandate. Nearly half of the reporting hospitals (45 percent) had fewer than 50 beds. The percentage of hospitals with fewer than 150 beds was 71 percent. Complete demographics by number of beds are listed in Figure 1.

Organizational Strategies

To identify some of the organizational strategies for achieving HIPAA compliance, respondents were asked if their facility had a full-time person acting as security officer and from what department the

individual in charge of security originated. Sixty percent of the individuals responsible for fulfilling the security requirements originated from the IS department, but only 17 percent reported a full-time security officer position for their facility. On average, 64 percent indicated that 0 to 25 percent of the security officer's time had been devoted to HIPAA-related duties during the previous year (2004). The next largest group (28 percent) indicated that 26 to 50 percent of their time was applied to HIPAA-related duties.

When asked which of the listed titles best matched their job description, the largest number of respondents (30 percent) indicated the titles of HIM officer or director. The second largest group (22 percent) marked the "other" option. Among those who marked "other," the most common responses were administrative positions or job combinations indicating dual responsibility, such as compliance privacy officer/manager of compliance; privacy and internal audit; or risk management/administration.

Level of Compliance with Security Standards

In regard to overall HIPAA security compliance, 29 percent indicated they were 76 to 100 percent compliant. A slightly larger number (38 percent) were 51 to 75 percent compliant. Twenty-four percent indicated 26 to 50 percent compliance, and the smallest group (8 percent) was 25 percent or less compliant.

The respondents were asked to indicate the level of compliance attained for each of the security standards on a scale of 1 to 5 (with 5 being the highest level of compliance). Based on the mean score of each standard, the highest level of compliance (mean = 4.22) was for policies and procedures for obtaining required business associate agreements. The standard with least compliance (mean = 3.34) was for policies for performing a periodic technical and nontechnical evaluation of security practices governed by the security rule. Table 1 shows the percentage of response for each level on the Likert scale.

Differences Based on Size of Hospital

An analysis of variance (ANOVA) was performed to determine if the level of perceived compliance varied according to facility size. The overall *F* test using an alpha level of 0.05 indicated that only one security standard was significant by size of facility. This standard dealt with policies and procedures for the security management process including risk analysis, risk management, sanction policies, and review of IS activities. Table 2 lists each standard with the *F* value and probability.

Threats, Problems, and Solutions Related to Compliance

The majority (70 percent) of respondents considered employee error to be the greatest threat. The specific group of employees believed to be the greatest threat to EPHI security was support staff (46 percent).

When respondents were posed the open-ended question "What area(s) of compliance did you find the most problematic?" the two recurrent themes in their responses were (1) employee education and adherence issues and (2) security issues pertaining to access, networking between facilities, and password protection. The majority of the respondents (54 percent) felt the most effective strategy for limiting threats to security of EPHI in their facility to be education of medical/support staff.

Discussion

This study is not without limitations. The data are only as good as the self-reporting of the respondents, and certainly a larger number of respondents would have strengthened the findings of the study. As described in the methodology section, surveys were sent to 1,000 randomly selected hospitals in early 2004. In order to maintain consistency in evaluating progress toward security, a shortened version of the survey was sent in early 2005 to the original 286 respondents. The second survey yielded a 50 percent return rate ($n = 144$).

The most recent AHA statistics for hospital size in the United States by number of beds were consulted to determine if the study sample provided a qualitative representation of U.S. hospitals. Forty-five percent of the hospitals responding to the survey reported 50 beds or fewer, while the 2003 AHA statistics reported approximately 26 percent of hospitals having fewer than 50 beds.¹⁴ However, all other

categories of hospital size by number of beds were very comparable. Therefore, information presented in this study may be slightly more applicable to the smaller hospitals throughout the United States.

While the survey was addressed to the hospital's HIPAA officer, most of the respondents (30 percent) described the job title/description that best matched their position as "HIM officer or director." In regard to security responsibilities, HIPAA mandates that there be an individual assigned the role of security officer. Whereas this study found 17 percent of respondents indicating that their hospital had an individual in a full-time security position, the 2005 AHIMA study found that 42 percent had a full-time security officer. The AHIMA study, however, also included other types of covered entities, not just hospitals. Both studies found that approximately 60 percent of those responsible for HIPAA security were IS/IT personnel.¹⁵ When looking at the proportion of the HIPAA security officer's time that was devoted to HIPAA-related duties, this study found that most (65 percent in 2004 and 64 percent in 2005) averaged less than 25 percent of their time in this capacity. This information is displayed in greater detail in Figure 2.

There was an overall trend toward increased security compliance from 2004 to 2005 as seen in Figure 3. While the percentage of respondents indicating their perceived level of compliance to be 0 to 25 percent was reduced by half (from 15 percent to 8 percent), there was a total of 32 percent in 2005 who indicated, within three months of the April 2005 deadline, that they were still less than 50 percent compliant. It is also possible that some in this group may have been among those who faced a 2006 date for compliance. As expected, the AHIMA report also indicated good progress toward compliance with the security rule, reporting 12 percent of facilities being less than 50 percent compliant.¹⁶

In Table 1, the security standards have been listed in order from highest to lowest mean score, based on the Likert scale of 1 to 5 (5 being the most compliant). This mean score arrangement implies that compliance with standards for obtaining business associate agreements and establishing a security officer was not as difficult to accomplish as compliance with other standards. The level of difficulty appears to culminate with those tasks that are ongoing and must be continually assessed. The three standards with lowest means—security management process (including risk analysis, risk management, sanction policies, and review of IS activity), security awareness and training for hospital personnel, and periodic technical and nontechnical evaluation—involved areas of low status predictability and high maintenance. Consistent and regular monitoring of these variables will be the key to successful compliance. It is interesting to note that the size of the hospital (based on number of beds) had very little effect on the perceived level of compliance. The only standard that varied by facility size pertained to security management (risk analysis, risk management, sanction policies, and review of IS activities). One might speculate that the IS/IT skills and equipment necessary to fulfill this standard might be financially challenging for the smaller facilities.

With the development of policies and procedures to achieve HIPAA security compliance firmly established in most facilities, a number of issues remain to be resolved. Because many hospital personnel are involved in the total care of a patient, it is no surprise that above the fears of natural disaster, equipment compromise, or even terrorist attack, the greatest threat to security of EPHI was perceived to be employee error, with the employee group most named as a concern being "support staff." This finding supports the statement by Amatayakul that "a large percentage of security incidents are the result of human error, not machine error."¹⁷ Hospitals are in the business of providing patient care and services 24-7. These tasks are often performed with short staffing and unplanned emergency situations that can quickly divert staff members from tasks involving patient records. This type of environment contributes to the reason why the areas named as "most problematic" involve (1) employee education and adherence issues and (2) security issues pertaining to access, networking between facilities, and password protection. Fifty-four percent of respondents indicated the most effective strategy for limiting threats to security of EPHI to be education of medical/support staff. Not only must all current hospital workers be routinely reminded of this important issue, but care must be taken that every new employee receive the same quality of training that was administered to attain initial compliance.

Implications for Directors of Health Information Management

While hindsight is always easier than foresight, it is important to realize that HIPAA compliance is not an achievement, but a process.¹⁸ Perhaps the most daunting task lies ahead. The challenge now is to establish a protocol for maintenance and reinforcement of security standards. All aspects of risk analysis, security incident reporting, and auditing should be meticulously documented on a daily basis. The importance of internal auditing must be stressed to ensure continued compliance.

It is recommended that a team of stakeholders in each facility work together to promote awareness and importance of the facility's security policies and procedures. These procedures must fulfill requirements for compliance without being impossible to achieve. Frequent interaction sessions by the team of stakeholders can facilitate the establishment of best practices and enhance two-way communication toward EPHI security. Dissemination of information from these key people to their co-workers may also provide a level of employee comfort in reporting potential security threats. Ongoing employee training and education are essential to achieving and sustaining HIPAA compliance. Possible training and awareness methods include computerized training modules, automated training programs, visual reminders, logos, and progress-toward-compliance bulletins. Emphasis should be placed upon positive recognition of employee participation toward achievement of security compliance.

So the question that arises is, What is the next step in perpetuating institutional security compliance? Some of the following tips may prove helpful:

- Seek administrative support throughout the process
- Tap the wealth of knowledge in periodicals and on the Internet
- Organize and prioritize initiatives
- Invest in the staff
- Educate personnel at all levels
- Maintain records of the process
- Maintain system logs and audits
- Identify and solve one problem before moving on to the next
- Be flexible and willing to modify policies and procedures
- Take small steps and do not overreact
- Keep it simple
- Make sure everyone is on the same page

Additional studies are recommended to identify successful strategies for maintenance of HIPAA security compliance. Further investigation of educational methodologies appropriate to the healthcare work force is recommended. Longevity studies could be conducted to verify DHHS's predicted cost savings over the next 10 years associated with HIPAA-mandated administrative processes and procedures related to EPHI. According to Halamka (as cited in Ferrarini), adhering to the HIPAA privacy and security rules is more than just about compliance, it is simply sound business sense.¹⁹

Karen Having, MS Ed, RT(R), RDMS, is an associate professor in the School of Allied Health at Southern Illinois University. Diane C. Davis, PhD, is a professor in the School of Information Systems at Southern Illinois University.

Notes

1. Fitzgerald, Todd. "The Final HIPAA Security Rule Is Here! Now What?" In H. F. Tipton and M. Krause (Editors), *Information Security Handbook*. Boca Raton, FL: CRC Press, 2004, p. 1921.
2. Fitzgerald, Todd. "HIPAA Security Rule 101: The Time to Act Is Now." *Security Management Practices*, March/April 2003, 44.
3. Birnbach, Deborah S., and Mayeti Gametchu. "How HIPAA's Security Rule Could Affect IT." *Computerworld*, 2003). Available at www.computerworld.com/printthis/2003/0,4814,80816,00.html.
4. Maddox, P. J. "HIPAA: Update on Rule Revisions and Compliance Requirements." *MEDSURG Nursing* 12, no. 1 (2003): 59–63.
5. Smith, Harry E. "The HIPAA Final Security Rule—More Than a New Security Standard." *ISSA Journal* (October 2003): 16–19.
6. Peled, Ariel, and Dr. Troyansky. "Twelve Steps for Compliance in a Convolved Regulatory Environment." *ISSA Journal* (March 2004): 8–11.
7. Amatayakul, Margret. "Reporting Security Incidents." *Journal of AHIMA* 76, no. 3 (2005): 60.
8. Woloszyn, William. "Reaffirming Your HIPAA Compliance Efforts." *Journal of AHIMA* 76, no. 4 (2005): 52–53, 65.
9. Amatayakul, Margret. "Putting the Finishing Touches to Security—Are You Ready?" *Journal of AHIMA* 76, no. 4 (2005): 56–57.
10. Walsh, Tom. "The 26.2-Mile Security Rule." *Journal of AHIMA* 76, no. 3 (2005): 24–27.
11. American Health Information Management Association (AHIMA). "The State of HIPAA Privacy and Security Compliance 2005." Chicago: AHIMA, 2005, p. 19. Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_026502.html.
12. Healthcare Information and Management Systems Society (HIMSS) and Phoenix Health Systems. "U.S. Healthcare Industry HIPAA Compliance Survey Results: Winter 2005." Chicago: HIMSS and Phoenix Health Systems, 2005, p. 2. Available at www.himss.org/Content/files/WinterSurvey2005.pdf.
13. AHIMA. "The State of HIPAA Privacy and Security Compliance 2005," pp. 18–19.
14. American Hospital Association (AHA). *AHA Hospital Statistics: The Comprehensive Reference Source for Analysis and Comparison of Hospital Trends*. Chicago: AHA, 2005, p. 10.
15. AHIMA. "The State of HIPAA Privacy and Security Compliance 2005," p. 18.
16. AHIMA. "The State of HIPAA Privacy and Security Compliance 2005," p. 20.
17. Amatayakul, Margret. "Putting the Finishing Touches to Security," p. 56.
18. Brown, Stephen C. "HIPAA Security: Don't Disband the Committee Just Yet." *Journal of AHIMA* 76, no. 5 (2005): 52–53, 57.
19. Ferrarini, Elizabeth. "Best Practices for Security and Privacy Make Good Business Sense." *Disaster Recovery Journal* 16, no. 2 (2003): 34–47.

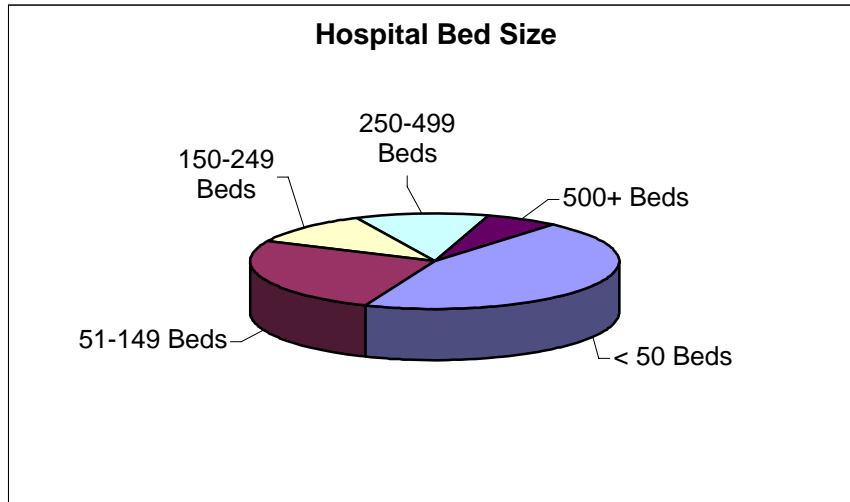
Figure 1**Size of hospitals responding in 2005**

Figure 2

Percent of HIPAA officer's time spent on security compliance

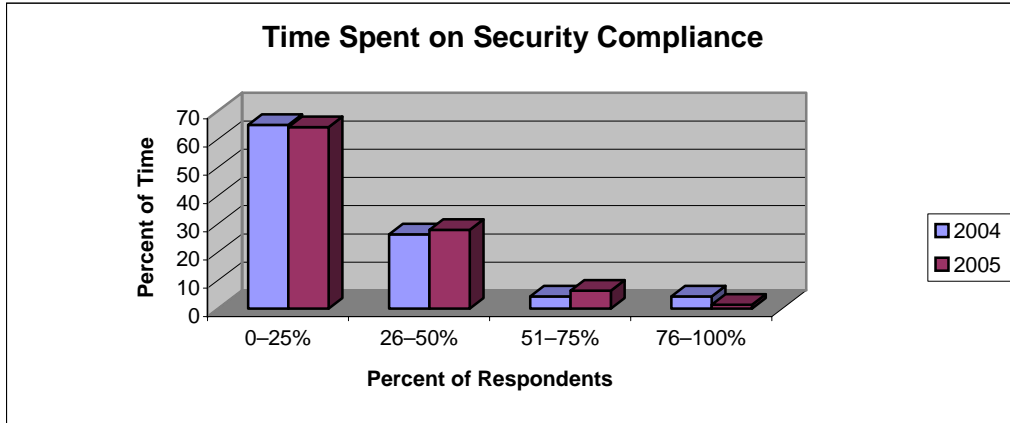


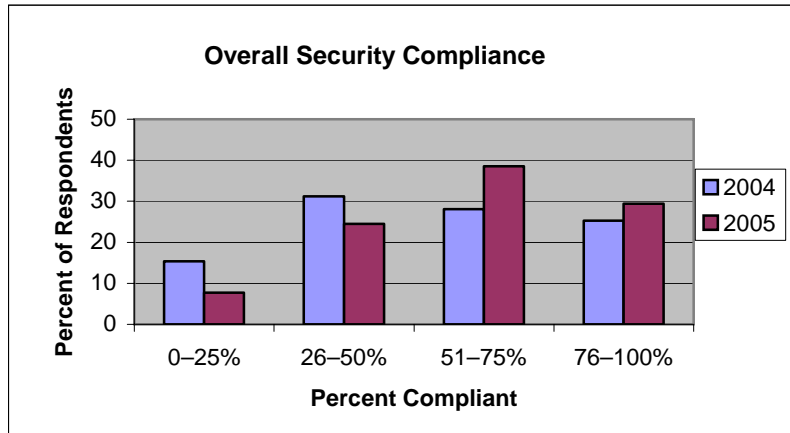
Figure 3**Overall security compliance reported by survey respondents**

Table 1
Percentage Reporting Each Level of Security Compliance

Security standard	Frequency of response* (as a percentage of all responses)				
	1	2	3	4	5
Policies/procedures for obtaining required business associate agreements	4	7	11	22	55
A security manager responsible for implementing and maintaining the requirements of the Security Rule	6	5	14	27	48
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	3	6	14	44	32
Policies/procedures for technical safeguards to provide access control, audit controls, integrity, person or entity authentication, and transmission security	4	9	17	47	22
Policies/procedures for information access management (authorizing access to electronic protected health information [EPHI] consistent with requirements)	2	10	24	38	23
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)	4	8	24	38	25
Policies/procedures for addressing security incidents (a response and reporting plan)	5	13	25	29	28
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)	6	11	26	36	21
A security management process including risk analysis, risk management, sanction policies, and review of IS activities	6	12	28	36	18
Program for security awareness and training for hospital personnel (including protection from malicious software and monitoring log-in attempts and password management)	9	15	23	30	23
Policies/procedures for performing a periodic technical and non-technical evaluation of security practices governed by security rule	10	13	28	29	19

* 1 being least compliant, 5 being most compliant

Table 2**Differences of Compliance Level Based on Size of Hospital**

Security standard	<i>F</i> value	Probability
Policies/procedures for obtaining required business associate agreements	1.10	0.36
A security manager responsible for implementing and maintaining the requirements of the security rule	1.66	0.16
Policies/procedures for physical safeguards	1.39	0.24
Policies/procedures for technical safeguards	2.26	0.07
Policies/procedures for information access management	0.28	0.89
Policies/procedures for workforce security	1.95	0.11
Policies/procedures for addressing security incidents (a response and reporting plan)	2.01	0.10
A contingency plan for responding to an emergency or other occurrence of damage	1.76	0.14
A security management process including risk analysis, risk management, sanction policies, and review of IS activities	3.24	0.01*
Program for security awareness and training for hospital personnel	0.95	0.44
Policies/procedures for performing a periodic technical and nontechnical evaluation	0.82	0.52

^a df = 4

* $p < 0.05$