

## Information Systems Security: a Model for HIPAA Security Compliance

Kathleen M. Bravo

### Abstract

*The healthcare industry is currently faced with the challenge of implementing the Health Insurance Portability and Accountability Act (HIPAA) security requirements. The HIPAA security regulations went into effect on April 21, 2003, and set forth a 24-month period for organizations to become compliant. The mandatory compliance date was April 21, 2005, for most covered entities (April 21, 2006 for small health plans). Although the April 21, 2005, deadline has passed and the April 21, 2006 deadline is drawing near, covered entities are struggling with preparedness.*

*HIPAA security differs from current security measures that organizations have in place in that organizations cannot pick and choose which measures to implement but, instead, must adhere to set guidelines in order to achieve compliance. Secondly, the HIPAA security rule is a mandate that all healthcare providers must follow; there is no participation waiver.*

*HIPAA security differs from other federal security regulations in a number of significant ways. First, unlike other federal information technology security regulations which affects only a few, the HIPAA security final rule is far-reaching and affects almost every individual residing in the United States. All hospitals, health care providers, insurance companies, financial billing companies, and anyone seeing or under a physician's care are subjected to adhere to or be protected by the set of safeguards that have been mandated by the final rule.*

*Secondly, the HIPAA security final rule differs from other federal security regulations in that it outlines specific safeguards that must be implemented. Other federal regulations either make vague references to necessary safeguards for compliance, require organizations to adopt a recognized framework, or offer organizations implementation flexibility based on internal risk assessments.*

*This research looked at all state contracted mental healthcare providers in New Jersey. The study had a number of major findings, namely,*

*how the survey results compared to the requirements of the final security rule, the factors affecting compliance, whether common compliance practices exist, security auditing/evaluation for compliance, and the use of the diamond model in validating findings, assessing the alignment of IT and organizational needs and in constructing a proposed compliance model.*

*The researcher sent a survey questionnaire to key IT professionals at the covered entities. Analysis of the survey resulted in descriptive statistics. These statistics and related graphs were developed for the entire group and were broken down by culture. When the results of the data analysis were compared to the final security rule and the diamond model, it was found that the majority of the covered entities surveyed were not ready for HIPAA security compliance. The research resulted in a proposed model for HIPAA security implementation and a number of recommendations.*

### 1. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a set of regulations that was designed by the Clinton Administration to protect the privacy rights of patients. Specifically, these regulations require doctors, hospitals, insurance companies, and pharmacies to obtain written consent from patients before disclosing medical information to anyone for any reason, document any access to that data, hire a full-time privacy officer, and provide patients with access to their own data and the ability to make corrections.

The Administrative Simplification subtitle of HIPAA is composed of a set of regulations that includes a number of separate and distinct components, namely, transactions and code sets, identifiers, privacy, and security. The transactions and code sets standards require all payers--Medicare, Medicaid, Blue plans, and other insurers--as well as nearly all providers, to adopt new standards for electronic financial and administrative transactions and code sets. The

identifier standards call for standard identifiers to be used in financial and administrative transactions.

Although the privacy component covers a patient's right over the use and disclosure of his or her personal health information, the security component, on the other hand, adopts standards for the security of electronic protected health information (ePHI) to be implemented by health plans, healthcare clearinghouses, and certain healthcare providers. The HIPAA security regulations went into effect on April 21, 2003, and set forth a deadline for organizations to become compliant. The mandatory compliance dates are April 21, 2005, for most covered entities and April 21, 2006, for small health plans. Small health plans are those that paid premiums or claims of \$5 million or less in their most recent plan year.

According to the Department of Health and Human Services, "The use of the security standards will improve the Medicare and Medicaid programs, and other Federal and private health programs, as well as the effectiveness and efficiency of the healthcare industry, in general, by establishing a level of protection for certain electronic health information" [2]. Furthermore, the benefits will be as follows: simplification of the administration of health insurance claims, lower costs, more control and access for patients and protected health information (PHI).

## **2. HIPAA Security Guidelines**

The Act [2] provides that covered entities that maintain or transmit health information are required to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information. These safeguards must also otherwise ensure compliance with the statute by the officers and employees of the covered entities.

### **2.1 Administrative Safeguards**

Administrative safeguards are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that

information. HIPAA's administrative safeguard includes the following categories: security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, and business associate contracts or arrangements subsections [3].

### **2.2 Physical Safeguards**

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards along with hazards caused by unauthorized intrusion. HIPAA physical safeguards requirements include the following categories: facility access controls, workstation use, workstation security, and device and media controls [4].

### **2.3 Technical Safeguards**

Technical safeguards refer to the technology, and policies and procedures for its use that protects electronic protected health information (ePHI) and controls access to it. HIPAA's technical safeguards require entities to adhere to the following measures: access control, audit controls, integrity, person and entity authentication, and transmission security [3].

As it is true for the Administrative and Physical safeguards, Technical safeguards also have implementation specifications that are categorized as either "Required" or "Addressable." "Required" implementation specifications indicate that a covered entity must implement the implementation specification "exactly" as identified in the Security Rule and there is no flexibility permitted as to their implementation. [2]

If an implementation is "Addressable" the covered entity may use discretion in achieving compliance with the standard. Furthermore, a covered entity may consider issues such as:

- Its size, complexity, and capabilities;
- Its technical infrastructure and capabilities;
- The cost of security measures; and
- The probability and criticality of potential risks to electronic "PHI."

## **2.4 Technologies to Address HIPAA Security Technical Safeguards**

A number of federal regulations in various industries have forced organizations to implement security standards, policies, and solutions. As such, software and security vendors have focused their radar on providing solutions to meet such a growing demand. As a result, there are a number of emerging technologies that can assist organizations in meeting HIPAA's Technical safeguards. These safeguards require entities to adhere to the following measures: access control, audit controls, integrity, person and entity authentication, and transmission security.

### **2.4.1 Access Controls**

Restricting access to ensure that access to PHI is provided only to authorized users, is a requirement of the HIPAA Security Technical Safeguards. Hansche, Berti and Hare [5] believed that access controls are the collection of mechanisms that specify what users can do on the system, such as what resources they can access and what operations they can perform. They are the countermeasures for ensuring that only users with the proper need and authority can access the system, are allowed to execute programs, and can read, edit, add, and delete the appropriate information on that system. There are a number of solutions that can assist health care organizations in this endeavor, namely access control methods, restricting administrative privileges, and automatic logoff.

#### **2.4.1.1 Various Access Control Methods**

The most common access control methods are: UBAC (user-based access control) and Role-based access controls (RBAC). RBAC is a more sophisticated approach that more closely reflects the Security Rule's Minimum Necessary Use requirements.

#### **2.4.1.2 Restricting Administrative Privileges**

Administrative privileges are assigned automatically to a built-in Administrator account. The access privileges accompanying such an account are unlimited and must be secured in order to reduce system vulnerability.

#### **2.4.1.3 Automatic Logoff**

Automatic logoff is another form of access control. Computer workstations placed in high-traffic areas are vulnerable to unauthorized users and to screen viewing by patients or visitors. To address this implication specification, establish

controls that automatically activate after a predetermined period of inactivity. This can be accompanied by having the application automatically time out to a password reentry screen and using a password-protected screen saver.

### **2.4.2 Audit Controls**

Audit controls provide management with a level of assurance that users are complying with policy. Audit trails are an audit control measure that can be used to keep track of who accesses data and engages in transactions. Audit trails can be used to monitor logon attempts and failures, and file and folder access. These logs will not only give some indication of who attempted or successfully gained access, but it will also give the time of access and additional details, if required. Operating systems like Microsoft Windows 2000 include application, security, and system logs [1].

### **2.4.3 Integrity**

As more and more data travels from network to network, data integrity becomes a concern. System administrators must ensure that data has not been tampered with or changed in any fashion by unauthorized users during transmission. There are a number of emerging technologies available to ensure data integrity, namely, digital signatures, encrypted file system (EFS), and virus protection.

### **2.4.4 Person and Entity Authentication**

There are a number of options for implementing authentication controls, namely, using a Password System, Single Sign On, Smart Cards, Biometrics, Electronic and Digital Signatures, Kerberos, SESAME, remote authentication.

### **2.4.5 Transmission Security**

In light of the risks associated with online communication, it is imperative to not only use secure encryption technology when conducting online business, but to also be able to prove one's identity. Ensuring that data isn't intercepted during transmission over the Internet, LAN or WAN is becoming an increasing concern and a requirement for HIPAA Security Technical Safeguard compliance.

### 2.4.5.1 Securing Network and Information Systems

Amatayakul [1] believes that although there has been a shift in the computer industry toward making systems more secure by default, network and information systems are generally not configured securely by the vendors. This places the responsibility for securing systems on the owner. Therefore, at a minimum, the following should be observed:

- Remove any unused services;
- Remove any unneeded games;
- Close extraneous network ports; and
- Rename manufacturer's defaults for system administrator accounts and change associated passwords.

### 2.4.5.2 Securing Your LAN (local area network)

The most common way to lock your local area network (LAN) from external hackers is to install a firewall, router, or intrusion detection system. Encryption is also a common method used to secure a network. More recently, due to its lack of versatility, routers are rarely ever used to lock LANs.

## 2.5 Security Compliance Auditing and Evaluation Practices

According to the Department of Health and Human Services [2], there is no such thing as "HIPAA Certification". However, section 142.08(a)(1) of HHS Regulation requires covered entities (CE) to certify that they have met the security standards.

- One of the few audit practices is conducted in accordance with generally accepted auditing standards based on the Control Objectives for Information and related Technology (CoBIT) framework.

## 2.6 The Diamond Model

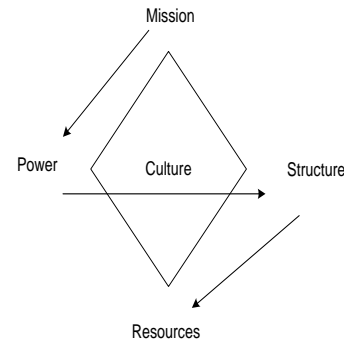
Although consumer surveys indicate that the public has a great deal of concern about security, it does not appear to be a concern of top management (in any industry) until it is brought to the forefront by litigation or new legislation. As a result, research on the topic of security is very limited. Most of the research done to date only looks at the effectiveness of certain policies, procedures, or physical designs of the work

environment. Only one researcher [8], looked at the comprehensive picture of how various types of industries manage privacy. Smith included the health care industry in his research, but it was represented by a very small number of interviewees. None of the research presents a model that could be used to look at how security programs are implemented in a given industry.

Merlyn [7] describes the Diamond Model that can be used to align information technology with organizational needs. Since security programs represent one aspect of information policy, this appeared to be an appropriate model for this study. The security programs required by HIPAA cross several functional areas of the organization. These include information services, human resources, health information management and financial services – just to name a few. As a result, it will be necessary to establish cross-functional committees to implement the programs. The Diamond Model presents a way to look at the security program and determine its readiness to meet the HIPAA requirements.

The Diamond model was adapted from the work of Robert W. Terry of the Reflective Leadership Center at Humphrey Institute of Public Affairs at the University of Minnesota and Kent Boesdorfer of Ernst and Young [7]. The Diamond model is illustrated as follows:

**Figure 1: The Diamond Model**



Meryl defines each element of the Diamond model as follows:

- Mission defines the purpose and direction for the organization, and answers the question "Why do we exist?"

- Power provides the energy to accomplish the mission, and determines how decisions are made and kept over time. The Power dimension answers the questions “Who has the power to make the mission happen? What commitment and sponsorship is required for the mission to be achieved?”
- Structure points to a form, plan, or regularized set of activities. This dimension provides the structural, procedural, and process elements needed for the mission. It answers the question “How is the mission carried out?”
- Resource addresses the time, money and people needed to complete the mission.
- Culture describes the shared values and basic beliefs of the organization. The Culture dimension answers the question “In what kind of environment must the other factors exist to achieve the mission?” [7].

Merlyn used a diamond-shaped model because he believed that power gets its direction from the mission. Power gives authority to the structure and can modify the structure. The structure will determine the allocation of resources. In addition, “resources place limits on structure, structure constrains the exercise of power, and power restricts mission. All of this occurs in and affects the prevalent cultural context” [7]. The Diamond model is consistent with the findings of a study of 50 health care information systems implementation projects reported at conferences of Canada’s Health Informatics Association. The study supported the need for resources, a team approach and organizational commitment [6].

Healthcare organizations’ security programs can be examined by application of each component of the model: culture, mission, power, structure, and resources. As recommended by Merlyn, an analysis can then be performed to identify areas where changes may be useful.

### 3. Research Design and Method

This study used an original data instrument to survey a state-wide representative sample of contracted mental healthcare providers. The study examined HIPAA security technical safeguard readiness, factors affecting preparedness, and common compliance practices.

Quantitative research methods were utilized to uncover theoretical elements used in the formation of meaning. To utilize the data collected from this research to generate ideas, themes and categories, and to develop a theory on assessing HIPAA Security Technical Safeguard readiness, factors affecting preparedness, and common compliance being used, descriptive methods were employed. Similarities and differences, as well as determining if there were shared themes in different responses to common inquiries, provided the data for determining the nature of compliance preparedness, the effects of factors affecting preparedness, and common compliance practices.

### 4. Findings

This study had a number of major findings, namely how the survey results compared to the final security rule, the factors affecting compliance, whether common compliance practices are being used, security auditing/evaluation for compliance, and the use of the diamond model in validating findings. The first set of findings was uncovered by making a comparison between the HIPAA security final rule and organizations’ responses to questions geared at assessing compliance.

### 5. A Proposed Model for HIPAA Security Technical Safeguard Compliance

The diamond model provided a useful framework to examine HIPAA security preparedness. The diamond model is based on the premise that an organization’s mission drives the three other elements of the model (power, structure, and resources). Any weakness in any one of those elements weakens them all.

A proposed model for HIPAA security technical safeguard compliance (Figure 2) emanated from the diamond model and the findings of this study. The model outlines nine key areas that must be addressed in order to ensure the implementation of a security program and HIPAA compliancy. The nine areas of the proposed model are indicated below:

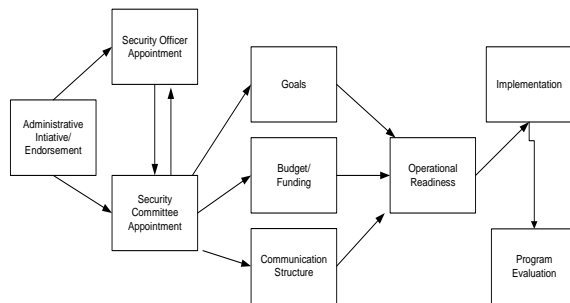
- Administrative Initiative/Endorsement

- Security Officer Appointment
- Security Committee Appointment
- Goal Setting
- Budget/Funding
- Communication Structure
- Operational Readiness
- Implementation
- Program Evaluation

The Administrative Initiative/Endorsement area of the proposed model directly correlates with the power, mission, and structure elements of the Diamond. It is during this phase of the process that the security programs mission is identified, program initiatives gain the support and “buy-in” of CEO and program structure is established.

Security Officer Appointment and Security Committee Appointment area of the proposed model directly correlates with the power, mission, and structure elements of the Diamond. It is at this phase in the process that key resources are identified.

**Figure 2: Proposed Model for HIPAA Security Technical Safeguard Compliance**



### 5.1 Validating the Proposed Model

Model validation is usually defined to mean substantiation that a computerized model within its domain of applicability possesses a satisfactory range of accuracy consistent with the intended application of the model.

During the validation process a number of techniques were used in order to facilitate the validation process. For the purpose of validating the proposed model, face validity and conceptual model validation was used.

#### 5.1.1 Face Validation

Face validity involves using people knowledgeable about the system in order to assess whether the model and/or its behavior are reasonable.

#### 5.1.2 Conceptual Model Validation

Conceptual model validation is determining that (1) the theories and assumptions underlying the conceptual model are correct, and (2) the model representation of the problem entity and the model’s structure, logic, and mathematical and causal relationships are reasonable for the intended purpose of the model. The theories and assumptions underlying the model were tested using mathematical analysis and statistical methods. This was achieved by using chi-square tests. Chi-square tests were also used to evaluate potential differences among the proportion of successes in any number of populations.

### 6. Conclusion

As discussed in Chapter 4, this study had a number of major findings, namely how the survey results compared to the final security rule, the factors that are affecting compliance, whether common compliance practices exist, whether organizations were performing security audits/evaluations for compliance, and the use of the diamond model in validating findings.

#### 6.1 Comparison of Survey Results to the Final Security Rule

The first set of findings was uncovered by making a comparison between the HIPAA security final rule and organizations’ responses to questions geared at assessing compliance. In order to make a feasible comparison the various HIPAA security technical safeguards were reviewed. The safeguards include: Access Controls, Audit Controls, Integrity Controls, Authentication Controls, and Transmission Controls. The results of the data collection and its analysis revealed that the majority of the organizations surveyed were not HIPAA security compliant.

#### 6.2 Factors Affecting Compliance

The second set of findings revealed that there are a number of factors affecting HIPAA security compliance. The overall results of the data that assessed whether cost was a factor that impedes organizations’ ability to become compliant revealed that cost is indeed a major factor. Additionally, it was discovered that cost is an underlying factor, because when budgetary

constraints are present, organizations can not hire knowledgeable staff and, therefore, the organization's ability to become compliant is affected.

### **6.3 Common Compliance Practices**

The findings revealed common compliance practices that were used to validate its usage by various groups within the sample population. Urban, midsize (based on gross revenues), and large organizations all have one thing in common, they showed no deviation from the common compliance practices identified. The response rate to questions and answers geared at assessing common compliance practices, when compared to the set common compliance practices, revealed that organizations falling within the category of urban, midsize (based on gross revenues), and large organizations, indeed, share the same common compliance practices that were identified.

### **6.4 Security Auditing/Evaluation for Compliance**

The overall results of the questions geared at assessing whether evaluations/audits are being conducted, revealed that organizations have not implemented the necessary evaluation practices in order to become HIPAA compliant. 51.7% of participants indicated that a HIPAA audit had not been performed.

For those who had an evaluation/audit performed (48.3%) 61% concluded that a gap analysis was not conducted as part of the audit. When asked whether there was a significant disparity between the results of the audit and the organization's level of compliancy, at that time, 94.9% of participants either made no selection, indicated that they did not know, or selected no.

### **6.5 Use of the Diamond Model in Validating Findings**

The Diamond model was used to assess the alignment of information technology with organizational needs. Since security programs represent one aspect of information technology, this model seemed appropriate.

Merlyn [7] used a diamond-shaped model because he believed that power gets its direction from the mission. Power gives authority to the structure and can modify the structure. The structure will determine the allocation of resources. In addition, "resources place limits on structure, structure constrains the exercise of power, and power restricts mission. All of this

occurs in and affects the prevalent cultural context" [7].

The findings of the study were compared to the Diamond model and its five elements: mission, structure, resources, power, and culture. Responses were analyzed by groups indicative of the cultural context of the Diamond model. These groups were derived from the demographics of survey participants' and include business type, entity type, geographic location, and size of organization (based on number of employees and annual gross revenues). Cultures were the representation of the subsets of these groups.

A comparison of the two geographical locations in the context of the Diamond model, revealed that organizations residing in an urban setting were more likely to have a security oversight committee but less likely to have a full-time security officer and a dedicated budget. The opposite was true for organizations residing in rural areas. Although the rural organizations surveyed had no security oversight committee, they were more likely to have a full-time security officer and a dedicated budget.

A comparison of the organization size in the context of the Diamond model, revealed that large organizations (those with a large number of employees) were more prepared for HIPAA security compliance than small and midsize organizations. Furthermore, these organizations were more likely to have a security oversight committee and dedicated security program budget. These organizations were also as likely as midsize organizations to have a full-time security officer.

Additionally, a comparison of organization size (based on Annual Gross Revenues), in the context of the Diamond model revealed that large organizations, again, were more prepared for HIPAA security compliance than small and midsize organizations. Furthermore, these organizations were more likely to have a security oversight committee, a full-time security officer, and a dedicated security program budget.

The power element of the Diamond model gets its direction from the mission and power gives authority to the structure and can modify the structure. Additionally, the structure will determine the allocation of resources. A weakness in the resources and structure elements is, therefore, predicated on weaknesses in the mission and power elements. The Diamond model is mission-driven, the mission affects power, structure, and resources. Therefore, these organizations also possess weaknesses in the two

other key elements (mission and power) of the Diamond model. Overall, the Diamond model reveals that there is no alignment between information technology and organizational needs and therefore, the organizations surveyed are not ready to implement the HIPAA security technical safeguard rule.

Although the findings revealed that large organizations are doing more in an effort to become HIPAA security compliant, these organizations are not doing enough to establish compliancy. These organizations, along with the other organizations surveyed, must make greater strides in order to align information technology with organizational needs. Such an alignment is necessary to implement a security program.

## 6.6 Recommendations

Based on the research findings, the recommendations are that organizations: (1) adhere to the recommended HIPAA security technical baseline; (2) implement the proposed model for HIPAA security technical safeguard compliance; and (3) regularly conduct performance testing and evaluations.

### 6.6.1 Recommended HIPAA Security Technical Baseline

The recommended HIPAA security technical baseline is comprised of a list of the required HIPAA security technical safeguards that are necessary to achieve compliancy. The type of security solution and its configuration are also included in this baseline.

### 6.6.2 Proposed Model for HIPAA Security Technical Safeguard Compliance

The diamond model provided a useful framework to examine HIPAA security preparedness. The diamond model is based on the premise that an organization's mission drives the three other elements of the model (power, structure, and resources). Any weakness any one of those elements weakens them all.

A proposed model for HIPAA security technical safeguard compliance (Figure 2) emanated from the diamond model and the findings of this study. The model outlines nine key areas that must be addressed in order to ensure the implementation of a security program and HIPAA compliancy.

Organizations should implement the proposed model and its nine elements. Furthermore, rather than leaving it up to individuals to decipher how they will implement the security program and take the risk of security

program implementation failure, this model establishes a framework which can be used to ensure the successful implementation of the security program and the HIPAA security technical safeguards baseline.

### 6.6.3 Compliance Testing and Evaluation

Although the only reference made to conducting periodic technical and non-technical evaluations can be found in the Administrative Safeguards section of the HIPAA Security rule, compliance testing and evaluation is necessary to ensure that current countermeasures are effective.

Additionally, organizations should conduct regular penetration tests to determine organization's ability to withstand an attack. These tests and procedures can also be used to determine areas for improvement.

## References

- [1] Amatayakul, M., Lazarus, S.S., Walsh, T., & Hartley, C.P. (2004). *Handbook for HIPAA Security Implementation*. USA: The American Medical Association.
- [2] Department of Health and Human Services, Office of the Secretary, Part II, 45 CFR Parts 160, 162, and 164, "Health Insurance Reform: Security Standards; Final Rule", *Federal Register* / Vol. 68, No. 34 /Thursday, February 20, 2003 / Rules and Regulations
- [3] Gallagher, J. (2003, Aug.). HIPAA compliance eludes many carriers, *Insurance & Technology*, Vol. 28, Iss.8; pg. 43
- [4] Grove, T. (2003). *Summary Analysis: The Final HIPAA Security Rule*. Retrieved July, 26, 2004, from <http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm>
- [5] Hansche, S., Berti, J., & Hare, C. (2004). *Official (ISC)2 Guide To The CISSPE Exam*. New York: Auerbach Publications.
- [6] Lau, F. and Herbert, M. (2001). Experiences from health information system implementation projects reported in Canada between 1991 and 1997. *Journal of End User Computing*, 13 (4), 17-25.
- [7] Merlyn, V. (1992). (n.d.). *The Diamond Model: A Framework for Aligning IS Automation Initiatives with Business and Organizational Needs*. (Working Papers of the IS Leadership Program of Ernst and Young).
- [8] Smith, H.J. (1994). *Managing privacy: information technology and corporate America*. Chapel Hill, NC: The University of North Carolina Press.