Global Information Assurance Certification Paper

Impact of HIPAA Security Rules on Healthcare Organizations

Tim Ferrell

October 4, 2001

Introduction

HIPAA, the Healthcare Information Portability and Availability Act of 1996, became law on August 21, 1996 and with it, came the promise of sweeping changes to the management and operation of security for healthcare organizations and the data they possess. The primary focus of HIPAA was to mandate that healthcare information become "portable" and "available" by legislating the use of uniform electronic transactions and other administrative measures. In forcing the healthcare industry to adopt uniform electronic transaction standards for Healthcare information, it was also necessary to protect that same information by including rules for how the information would be secured and safeguarded. The HIPAA regulations contain a section called *Administrative Simplification* (Title II, Subtitle F) that articulates the Security rules (along with the Transaction and Privacy rules) for healthcare organizations that transmit or posses *protected health information*. This paper focuses on the impact of the Security rules.

For those organizations that have already implemented strong security policies and practices, the HIPAA Security rules will not impose extensive change. The most severely impacted organizations will be those that have lax or weak security polices and practices, which as a result, must undergo an extensive and costly compliance effort.

HIPAA Security Rules

The portion of the HIPAA law that most impacts technology interests is the section on *Administrative Simplification* (Title II, Subtitle F). Administrative Simplification seeks to force uniform standards in the electronic interchange of health information (through the Transaction Rule) and also mandates guidelines for the security (Security rules) and privacy (Privacy rules) of that information whether in transit or stored. The HIPAA Security regulations apply to that protected health information that is *electronically maintained or used in an electronic transmission*[1]. Administrative Simplification is divided in to Transaction, Security and Privacy Rules. This paper deals specifically with the Security Rules.

The HIPAA Security rules are divided into four sections:

- Administrative Safeguards

[1] Rada, p. 128

- Physical Safeguards
- Security Services
- Security Mechanisms

Administrative safeguards deal with those administrative policies, procedures and practices that are used by a covered entity to handle protected health information. These generally take the form of written policies and procedures that are practiced in normal day-to-day operations. Physical safeguards deal with physical access to data and facilities within that contain protected health information. Security services and security mechanisms specifically address technical systems, networks and applications that possess or transmit protected health information.

The HIPAA Security rules mandate that if healthcare information (also referred to in the HIPAA text as protected health information) is stored or processed electronically, then the security rule applies to that covered entity. This would seem to exempt pure paper-based operations from the Security rules, but even these organizations likely use fax technology, which *is* covered by the HIPAA security rule. Accordingly, there are very few healthcare organizations that will escape the grasp of the HIPAA regulations as very few are entirely paper-based.

HIPAA Security rules essentially resemble a collection of the recommended best practices for security management and operations. For this reason, if the healthcare organization has already adopted sound security practices, the HIPAA-compliance effort should be minimal. Given that Security is not a prime concern for many healthcare organizations, especially smaller organizations, the cost and effort to become HIPAA compliant will be staggering. The U.S. Government has placed the cost of the HIPAA compliance effort at $5.8 billion, but industry analysts believe that this figure is low and the cost may be closer to $25 billion.[2] According to Fitch IBCA, most of the costs associated with HIPAA will be in modifying existing information technology systems or purchasing new ones, hiring and retraining staff, and changing existing processes for maintaining patient privacy.

Interestingly enough, HIPAA is technology –neutral in that it does not mandate any specific technology from any vendor. It specifies the policies, procedures, services and mechanisms that must be in place and leaves the underlying technology choices to the individual organization.

HIPAA places heavy emphasis on the creation and documentation of policies and procedures. It will not be enough under HIPAA law to simply have an ad-hoc or commonly used process in place to address HIPAA-compliance; the process (including the supporting policy and procedures) *must be fully documented* to adequately meet most HIPAA regulations. In this regard, HIPAA

[2] Lageman and Melick, p. 3

is in effect legislating security best practices into the healthcare industry. To complicate matters, the Department of Health and Human Services (DHHS) has imposed compliance deadlines for organizations to become HIPAA compliant.

The following section steps through the primary areas of the HIPAA Security Rules and explain in plain English what they mean and how they are expected to impact covered entities (a.k.a. Healthcare providers, payers and clearinghouses).

It is worth noting that as of October 2001, DHHS had not yet published the final rules for HIPAA Security. The final Security rule is expected to be published sometime before the end of 2001.

Certification

The HIPAA law requires each covered entity to assess their HIPAA compliance posture. This may performed by an internal or an external agency. The purpose of the assessment is to require each covered entity to examine their security practices against the HIPAA guidelines to determine where they are deficient. Once this gap analysis is complete, the organization can determine where changes are required to reach a HIPAA-compliant state. Ideally, this assessment process will be a continuous process that allows the organization to identify deficiencies and correct them on an ongoing basis.

Chain of Trust Partner Agreements

HIPAA holds businesses liable for associations with partners who may not, themselves, be HIPAA compliant. Covered entities must develop a chain of trust agreement with each party with which protected health information is shared. Contracts with business associates should include contract language that requires the partner to maintain the confidentiality and integrity of the data. Each covered entity's legal counsel should be involved in the development of these contracts. In the event of litigation, the covered entity could be protected by a well-written contract with its business associates.

Contingency Plan

HIPAA requires all covered entities to maintain and routinely update a comprehensive plan for responding to system emergencies. The plan must include polices and procedures for

- Data criticality analysis
- A data backup plan
- A disaster recovery plan
- An emergency mode operations plan

- Procedures for testing and revision of the plans

Larger healthcare organizations generally do have emergency mode operations plans, but they must be evaluated to ensure that contain provisions for the five elements outlined above. For those who do not have comprehensive contingency-mode operations plans, achieving compliance with this rule will be an expensive and tedious process.

Formal Mechanism for Processing Records

HIPAA requires all covered entities to have formal policies and procedures for *the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of protected health information*[3]. Once again, this is an administrative procedure that specifies how organizations must deal with health care data from its inception to its disposal and all points in between. Most organizations have informal practices for processing their health data. This section of the law requires all organizations to take a hard look at how data gets created, where it stored is, who can modify it and who can delete it. For large organizations, this will force a review of workflow processes and security roles to assure that only certain systems can possess certain data and that data is not moved to locations and systems that are not part of the formalized process. This control must extend to include smaller ad-hoc (decentralized) systems also, such as copies or extracts of data that resides on desktop and laptop systems.

Information Access Control

An administrative procedure, this section of the HIPAA rules, requires the organization to have formalized procedures in place for how access to data is granted, modified or revoked. This seeks to eliminate the possibility of an unauthorized party receiving unauthorized access to protected health information by establishing a process that is documented, understood and followed.

Internal Audits

HIPAA regulations require regular *in-house review of records of systems activity (such as logins, file accesses, and security incidents) of the maintained by an organization*[4]. Plainly stated, all system logs must be reviewed for abnormal and suspicious activity on a regular basis. Most organizations maintain logs of events, but few actually audit the logs for specific activity. There are many tools available on the market that will scan logs and raise alerts if certain key words are present or conditions exist. All organizations should evaluate such tools and

[3] US Department of Health and Human Services NPRM for Security and Electronic Signatures
[4] Ibid

subsequently add one to their HIPAA toolkit. Ideally, all security-related events should sink (aggregate) to a secure location that can only be accessed or modified by authorized security personnel. The policy and procedure for this process must be fully documented. Remember that the logs themselves may contain protected health information, and if so are subject to HIPAA rules and regulations.

Personnel Security

Covered entities are required to establish a personnel security clearance process. The process must include provisions for:

- Supervision and monitoring of maintenance personnel
- Monitoring of granted access
- Procedures for determining and granting access
- Access levels are periodically reviewed
- Security awareness training

Most organizations have some process in place to evaluate and grant security access, but this process may not be documented. As with most other HIPAA regulations, the mere existence of the process is not sufficient – it must be documented and periodically reviewed for operational compliance.

Security Configuration Management

HIPAA regulations require covered entities to establish and document a process for managing the security configuration of the environment. The Security Configuration Management process must, at a minimum, address:

- Documentation of all facets of the organization's security operation
- Procedures for installing and testing hardware and software for compliance with security policies
- A complete inventory of all systems and applications
- A security testing process that assure that new systems meet HIPAA security requirements
- Virus checking software

This section seeks to ensure that all covered entities exercise due diligence in adding new systems and modifying existing systems and applications within the environment.

Security Incident Procedures

Organizations are required to formalize their procedures for dealing with security incidents (a.k.a. incident handling). Many organizations do not have formalized

procedures for dealing with security incidents, though as of late this may be changing due the impact of the Code Red and Nimda worms. Each covered entity is required to have a documented process that describes how they will respond to security incidents, including the roles and responsibilities of various divisions of the organization. Employees should be trained on how to report potential and real security incidents.

Security Management Process

In order to be HIPAA compliant, the organization must have an overall Information Security Management process. HIPAA regulations define this as the *creation, administration, and oversight of policies to ensure the prevention, detection, continament and of security breaches involving risk analysis and risk management*[5]. In plain English, this means that organizations must have, document and use sound security policies. A good security policy establishes accountability, controls, physical security and appropriate penalties. The HIPAA regulations actually go on to require that an organization's security policy must contain certain elements:

- Ongoing risk analysis (cost of protection vs. cost of loss)
- Risk management (transferring or reducing risk)
- Sanctions and penalties for violations of policy
- Clear delineation of roles and responsibilities for security

Termination Procedures

Some of the most devastating security breaches can occur during employee termination when steps are not taken to remove access to resources in a timely manner. HIPAA guidelines specify that when employees are terminated, that certain steps, at a minimum, must be followed. These include changing locks, removal from access lists, removal of user account, and confiscation of keys, tokens and other access cards. Though these steps may seem to be common sense, some organizations may not have documented procedures to follow when an employee is terminated. Additionally, the responsibility for carrying out the termination procedures must be clearly assigned and documented.

Security Training

In order for a security program to work well, the employees must be educated in security practices such as password protection, monitoring login failures and other basic practices. A well-educated workforce can become an extension of the security group of any organization through simple awareness. The HIPAA regulations require a Security Awareness training program that includes:

[5] US Department of Health and Human Services NPRM for Security and Electronic Signatures

- Awareness training for all personnel
- Security reminders to the workforce
- Virus protection
- Failed login awareness
- Password management techniques
- How to report security discrepancies

Assigned Responsibility for Security

HIPAA requires covered entities to assign a security officer to oversee the security of protected health information. Most healthcare organizations will have a tendency to assign this role to an existing security officer – effectively augmenting current responsibilities. This will not be effective for purposes of complying with HIPAA. The task of managing an organization's HIPAA compliance efforts is simply too great to dealt with on a part-time basis. Additionally, this should not be confused with the HIPAA Compliance Officer and the HIPAA Privacy Officer which may be separate roles in large organizations.

Media Controls

Media controls must be in place in the form of formalized, documented policies and procedures. These policies and procedures must include specifics for handling data backups, data storage, disposal, access control and accountability for media that contains protected health information. Most organizations have backup procedures, but these may not link back to a parent security policy that addresses the handling of all media types. In order to meet HIPAA requirements, the policies and procedures for media handling must be clearly documented. Organizations should interpret this rule to include paper media also (or anything that could store protected health information).

Physical Access Controls

This section of the HIPAA security rules is very broad in scope and lays down stringent physical security requirements for those organizations that handle protected health information. As with nearly every other HIPAA guideline, this portion of the rules requires documented policies and procedures for the management of physical security. These policies and procedures must specifically contain or reference:

- A documented disaster recovery plan
- An emergency mode operations plan
- Equipment control (adding / removing equipment from a facility), including media protection

- A facilities security plan
- Procedures for verifying physical access authorizations
- Records for maintenance of facilities
- Procedure for handling need-to-know data
- Visitor sign-in / sign-out procedures
- Te restriction of testing and modification to authorized personnel

This portion of the HIPAA rules makes it clear that physical security is as important as data security. This rule also includes the security of portable devices such as laptops and handhelds that could be taken off-site. It would be prudent for all covered entities to consider all equipment that could be removed from the site and its protection.

Workstation Use Policy

This section of the regulations requires that covered entities take certain steps to protect and secure workstations to minimize opportunities for unauthorized use or viewing. Although specific actions are not put forth in the regulations, good practices would include the use of workstation covers, locking workstations to surfaces, biometric logons, and limiting logons to specific workstations on a per user basis. As with nearly all HIPAA regulations, there must be a written policy on workstation use.

Secure Workstation Location

Covered entities are required to implement physical safeguards to eliminate or minimize the possibility of unauthorized workstation access. Most organizations should have policies that govern workstation placement. These rules should, at a minimum, contain provisions for placing workstations in secure locations (not in open or public areas), orienting workstations to prevent viewing by non-authorized personnel and the installation of shields as necessary to protect screen contents. This section of the rules could be interpreted to include the use of password-protected screen savers and video surveillance of areas where workstations could be comprised (public or semi-public areas).

Security Awareness Training

The writers of the HIPAA law understood that in order for security to work, those who have authorized access to protected health information must be trained to protect it. Organizations will find that the most effective enforcer of the HIPAA guidelines is a well-educated workforce. HIPAA mandates on-going security awareness training to achieve this goal.

Data Access Controls

HIPAA requires that technical security services must include procedures for granting access to protected information that includes:

- A documented procedure for granting emergency access to data
- Role-based, user-based or context-based access
- The optional use of encryption

This rule requires that some basis exist for the granting of access to protected health information. The basis for granting access must be who the user is, the user's role in the organization, or the user's context. This implicitly forbids generic or shared logins as well as simultaneous concurrent logons.

If a user is required to access data on an emergency basis, a documented procedure must exist for evaluating the request (typically called a "break-the-glass" procedure). This procedure must be followed for all requesting information access regardless of rank, title or position.

Lastly, HIPAA does not require encryption for controlling access to data, but it could be considered as a form of access control due to non-readable nature of encrypted data.

Data Audit Controls

HIPAA requires that every technical system employ logging to record and permit later evaluation. HIPAA does not specifically require how logs must be parsed. It would behoove any organization to utilize automated log scanning tools to parse for certain conditions and to raise alerts when appropriate.

Logs themselves should be protected as they could contain protected health information and could be the target of unauthorized modifications by unauthorized entities to cover their tracks.

Data Authorization Controls

Consent and authorization mechanisms must be in place to control disclosure of data. Just as access controls must be in place for technical systems that utilize role-based or user-based mechanisms, so must authorization controls. This implies that once entities are properly authenticated to the systems, prudent steps must also be taken to verify that the entity is authorized to access (read/write, etc.) specific data elements. Similar to the authentication controls rules, role-based or user-based access must be used, but authorization should not be granted to generic and/or shared accounts.

Verification of Data

Steps must be taken to ensure that protected data has not been modified in an unauthorized manner. HIPAA rules specifically mention the use of checksums, double keying (for data entry), message authentications codes and digital signatures. Note that digital signatures are not required, but are mentioned as a possible solution.

When coupled with strong access controls and extensive logging, data verification schemes can virtually eliminate the possibility of an unauthorized data alteration occurring without being noticed.

Entity Authentication

HIPAA requires that organizations take steps to ensure that an entity is who or what it claims to be. This is quite different than the HIPAA regulations that call for user-based, context-based or user-based authentication or authorization. This section specifically deals with logon mechanisms such as biometrics, auto-logoffs, PINs, and other methods.

The HIPAA regulations on authentication methods specifically call for the use of at least one of the following for authentication:

- Biometric identification
- Password
- PIN
- Telephone callback procedure (for dial-up)
- Token

Additionally, automatic logoffs and unique user identifiers must be used.

Communications and Network Controls

This section of the HIPAA regulations applies only to those covered entities that transmit protected health information over a communications network. This is expected to be an overwhelmingly large percentage of healthcare providers, payers and clearinghouses. The rules vary depending on whether a private network (e.g. leased lines, VAN) or the public network (e.g. PSTN, Internet).

All networks, public and private, must at a minimum employ:

- Authentication of the entity at the other end of the wire
- Alarms to sense abnormal conditions
- Auditing to allow the reconstruction of events if required
- Event reporting to identify operational problems

For those organizations that utilize public networks (such as the PSTN or the

Internet), their security standards mechanisms must additionally include the following:

- Integrity controls to assure the authenticity and source of transmitted data
- Message authentication to ensure data integrity (such as digital signatures)
- Message access controls or encryption to prevent unauthorized viewing (and subsequent interpretation) of data
- Access controls (such as encryption)

Electronic Signature Standard

No HIPAA standard currently requires the use of an electronic signature (though it is anticipated that certain future HIPAA transactions types may). The Security regulations do state however, that if an electronic signature is used, then a digital signature (PKI implied) must be used as the electronic signature implementation. Furthermore, if digital signatures are used then certain features must be implemented: message integrity, non-repudiation, and user authentication. Other digital signature features may be implemented, but are not required. It is generally believed that DHHS did not force the use of digital signatures in HIPAA due to the enormous projected cost and impact of forcing a PKI implementation in every health care organization in the US.

References

Rada, Dr. Roy. "HIPAA@IT: Health Information Transactions, Privacy and Security". Hypermedia Solutions Limited. August 2001.

"Notice of Proposed Rule Making for the Security and Electronic Signature Standards". U.S. Department of Health and Human Services. URL: http://aspe.hhs.gov/admnsimp/nprm/seclist.htm (September 2001)

"HIPAA Security Matrix". IBM. URL: http://houns54.clearlake.ibm.com/solutions/healthcare/helpub.nsf/detailcontacts/HIPAA_SECURITY_MATRIX?OpenDocument (October 2001)

David C. Kibbe, MD, MBA, American Academy of Family Physicians. "A Problem-Oriented Approach to the HIPAA Security Standards". July/August 2001. URL: http://www.aafp.org/fpm/20010700/37apro.html (October 2001)

Phoenix Health Systems. "HIPAAdisory: Standards for Security and Electronic Signatures". URL: http://www.hipaadvisory.com/regs/securityandelectronicsign/ (October 2001)

Lageman, Rebecca C. and Jordan R. Melick. "HIPAA: Wake-Up Call for Health Care Providers". Fitch Ratings Health Care Special Report. September 15, 2000. URL: http://www.fitchratings.com/corporate/reports/report.cfm?rpt_id=79622