Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Preparing for HIPAA: Privacy and Security Issues to be Considered

The Health Insurance Portability and Accountability Act (HIPAA) is imposing privacy and security regulations on health plans, health care clearinghouses, and health care providers. Although not explicitly stated, this also includes medical schools and research institutions. For medical schools, HIPAA's challenges are different from those of other healthcare organizations due to multiple roles of faculty as educator, researcher and clinician. Because so many people need access to different portions of patient health inf...

Copyright SANS Institute
Author Retains Full Rights

AD

Preparing for HIPAA: Privacy and Security Issues to be Considered

Sherry Fischer
January 5, 2003
GSEC Practical
Assignment Version 1.4b
Option 1

Abstract

The Health Insurance Portability and Accountability Act (HIPAA) is imposing privacy and security regulations on health plans, health care clearinghouses, and health care providers. Although not explicitly stated, this also includes medical schools and research institutions. For medical schools, HIPAA's challenges are different from those of other healthcare organizations due to multiple roles of faculty as educator, researcher and clinician. Because so many people need access to different portions of patient health information (PHI), administration of privacy and security is difficult. Therefore, the privacy and security regulations focus on achieving data integrity, confidentiality, and availability through four main areas: administrative policies, physical safeguards, technical security services and technical security mechanisms.

New regulations mean new processes and procedures that must be followed. Because HIPAA's regulations are so comprehensive, a multitude of perceived barriers to compliance must be addressed. The barriers can also be broken down into four main areas: cultural, administrative, technical, and physical. Examining these barriers as well as ways some organizations in the healthcare industry have dealt with them provides insights into ways compliance can be attained. What is learned from examining the regulations, barriers, and other organizations is that although becoming HIPAA compliant will involve a major initial effort and ongoing maintenance, once these barriers have been overcome, the healthcare industry will be better able to protect patient health information.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is imposing many changes on institutions housing protected health information (PHI). HIPAA's rules provide generalized information about how changes are to be made, but for universities with medical schools, these rules can be confusing and unclear.

Medical schools and other research institutions seem to have been overlooked by HIPAA's writers. Regulations state that they cover "health plans, health care clearinghouses, and health care providers" ("Standards for Privacy of Individually Identifiable Health Information." Federal Register. §160.102.), and a medical school does not manage PHI as its primary business function. However, due to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the multiple roles of faculty as educator, researcher and clinician, the medical school finds itself housing PHI in many distributed and unexpected locations.

Health care presents a challenge to privacy and security administration because so many people need to access different portions of PHI in order to perform tasks specific to a variety of jobs. Because medical schools are so different from the other covered entities, the perceived barriers to implementing HIPAA's privacy and security requirements are different too, and in many ways, more difficult to overcome.

Question

The question this paper attempts to answer is, "Given that faculty are involved in education, research and clinical practice at a variety of affiliated medical and research institutions, and data containing PHI resides in a distributed fashion in a variety of databases on a variety of platforms, what are some of the ways that a large medical school can begin to implement HIPAA's controls and overcome the many potential barriers to compliance?"

To answer the question, a brief description of HIPAA's privacy and security requirements and possible barriers to implementation are examined. At the end of this paper is a discussion of how a few agencies are moving toward HIPAA compliance.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Brief Description of HIPAA's Privacy and Security Requirements

Development of the Regulation

The Health Insurance Portability and Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986, is also known as the Kennedy-Kassebaum Act. (HIPAA Primer.) The act added a new part to Title 45 of the Code of Federal Regulations (CFR) for health plans, health care providers, and health care clearinghouses in general. ("Standards for Security and Electronic Signatures: Proposed Rule." Federal Register.)

"The new regulation reflects the five basic principles:

- **Consumer Control:** The regulation provides consumers with critical new rights to control the release of their medical information.
- **Boundaries:** With few exceptions, an individual's health care information should be used for health purposes only, including treatment and payment.
- **Accountability:** Under HIPAA, for the first time, there will be specific federal penalties if a patient's right to privacy is violated.
- **Public Responsibility:** The new standards reflect the need to balance privacy protections with the public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care, and fighting health care fraud and abuse.
- **Security:** It is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure." (HIPAA Primer.)

"45 CFR includes a section called Administrative Simplification, which requires:

- Improved efficiency in healthcare delivery by standardizing electronic data interchange, and
- Protection of confidentiality and security of health data through setting and enforcing standards.

Therefore, HIPAA calls for:

- Standardization of electronic patient health, administrative and financial data
- Unique health identifiers for individuals, employers, health plans and health care providers
- Security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future.

The four parts of Administrative Simplification are (one to two year extensions exist for some of these compliance dates):

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Electronic Health Transactions Standards (compliance date 10/16/02)
2. Unique Identifiers (publication date 7/30/02)
3. Security and Electronic Signature Standards (proposed)
4. Privacy and Confidentiality Standards" (compliance date 4/14/03) (HIPAA Primer.)

As each part of the HIPAA regulation is published, covered entities will have two years plus two months to comply. To be considered compliant, a covered entity must satisfy each of the regulations in a reasonable and appropriate manner.

This paper will address only Parts 3 and 4 of the Act.

Part 3, Security and Electronic Signature Standards, will contain provisions specific to securing health information used in any electronic transmission or stored format. The proposed rule is comprised of widely accepted information practices that are followed in other industries and are endorsed by many standards organizations.

Part 4, Privacy and Confidentiality Standards, establishes that health plans, health care clearinghouses, and health care providers must have standards in place to comply with the statutory requirements, including HIPAA awareness training, disclosure of only the minimum necessary patient information, accounting for disclosures of health information, and safeguarding of PHI. HIPAA was passed in response to the concerns about the confidentiality of personal medical information. The standards contain administrative, physical, and technical security measures that are technology-neutral to allow an entity to design appropriate and reasonable solutions.

The Difference between Privacy, Confidentiality and Security

HIPAA regulations cover both security and privacy; confidentiality is part of the privacy rule. Security and privacy are distinct but related. Privacy is the right of an individual to control the use of his or her personal information. It should not be divulged or used by others against his wishes. Confidentiality becomes an issue when an individual's personal information is received by another entity. Confidentiality means protecting the information by safeguarding it from unauthorized disclosure. Security refers to all of the physical, technical and administrative safeguards that are put in place to protect the information. Protection of a system from unauthorized access, whether external or internal, stored or in transit, is all part of security.

Requirements of Privacy and Security Rules

For an institution to be considered compliant with the HIPAA regulations, many requirements must be met. The Privacy Rule focuses on the way PHI is handled

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

within an organization and between the organization and other covered entities, and includes both paper and electronic records.

Among the Privacy regulations are:

- Disclosure of only the minimum information necessary
- Accounting for those disclosures
- Safeguards, which are comprised of many of the components found in the Security Rule
- Staff HIPAA awareness training
- Sanctions/penalties for abuse of these rules

In order to comply with the Privacy Rule, the organization must implement reasonable and appropriate security practices. The Security Rule focuses on both external and internal threats, security threats and vulnerabilities, and includes the protection of computers or workstations used to view, transmit, and store patient medical data and related information. Other covered subjects are formalization and documentation of policies, logging to create audit trails in order to know who is accessing or modifying PHI. The Security Rule addresses only information stored in an electronic format.

External threats, or threats from outside the organization, can result in a denial of service or theft and misuse of proprietary information, including individual health information. These attacks can also affect the integrity of information by corrupting data that is being transmitted. Internal threats, many of which are addressed in the Privacy Rule, include careless staff or staff unaware of security issues, and curious or malicious insiders who deliberately take advantage of system vulnerabilities to access and misuse personal health information.

"Covered entities are required to:

- Assess potential risks and vulnerabilities by performing gap or risk analysis
- Protect against threats to information security or integrity, and against unauthorized use or disclosure
- Implement and maintain security measures that are appropriate to needs, capabilities and circumstances
- Ensure compliance with these safeguards by all staff." (Meyer, Stanton. HIPAA: What it Means for Privacy and Security.)

The emphasis is on protecting "data integrity, confidentiality and availability" of individually identifiable health information. Several components have been identified and/or mandated to ensure the security of this information. They are grouped into four main categories. The first three include administrative procedures, physical safeguards and technical security to ensure availability, confidentiality and integrity of the data. The fourth category includes additional

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

technical security measures to ensure the reliability of transmitted data. Each of these categories have specific requirements.

- Administrative Procedures - documented, formal practices to manage the selection and execution of security measures, including the limitation of information access to appropriate parties only and the guarding of information from all others.

    - "Certification - technical evaluation of the compliance of data systems through a "pre-specified set of security requirements."
    - Chain of Trust Partner Agreements - an agreement between a covered entity and all other entities with whom health information is shared, to "protect the integrity and confidentiality" of the data they exchange.
    - Contingency Plan - a documented plan to maintain continuity of operations in an emergency or disaster, and to enable recovery of data following disaster.
    - Formal Mechanism for Processing Records - policies and procedures for the receipt, handling and disposal of health information.
    - Information Access Control - policies and procedures for allowing different levels of access to health information.
    - Internal Audit - regular review of systems access patterns.
    - Personnel Security - policies, procedures such as security clearances, access record maintenance, and staff training.
    - Security Configuration Management - procedures that coordinate overall enterprise security.
    - Security Incident Procedures - measures for reporting and responding to security incidents.
    - Security Management Process - establishing a process to "ensure the prevention, detection, containment and correction" of security breaches.
    - Termination Procedures - procedures used when terminating employees or users to prevent continued access to health information.
    - Training - security awareness training for all personnel and specific training of users on system security protocols." (Gue, D'Arcy Guerin. The HIPAA Security Rule (NPRM): Overview.)

- Physical Safeguards - protection of computer systems, buildings housing PHI, and computer and networking equipment from hazards and intrusion. These safeguards focus on preventing unauthorized individuals from gaining access to electronic information.

    - "Assigned Security Responsibility - officially assigning responsibility for information security.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Media Controls - setting up formal procedures for controlling and tracking the handling of hardware and software, and for data backup, storage and disposal.
- Physical Access Controls - developing a facility security plan, and setting up disaster recovery, emergency modes, and other access and handling controls.
- Workstation Use - policies and procedures to prevent unauthorized access to protected information on workstations and terminals.
- Security Awareness Training - awareness training for all employees and others with physical access to protected health information." Gue, D'Arcy Guerin. The HIPAA Security Rule (NPRM): Overview.)

- Technical Security Services - processes that protect and monitor information access and balance the need for timely access to needed health information with the need to protect its confidentiality and integrity.

  - "Access Control - providing controls limiting access to health information to those with valid needs and authorization.
  - Audit Controls - setting up system mechanisms that record and monitor activity.
  - Authorization Control - obtaining and tracking the consents of patients for use and disclosure of their health information.
  - Data Authentication - ensuring that data is not altered, destroyed or inappropriately processed.
  - Entity Authentication - employing mechanisms such as automatic logoff, passwords, PINs and biometrics, which identify authorized users and deny access to unauthorized users." Gue, D'Arcy Guerin. The HIPAA Security Rule (NPRM): Overview.)

- Technical Security Mechanisms - processes that prevent unauthorized access to data that is transmitted over a network. Organizations that transmit health information over open networks must keep it from being easily intercepted by third parties via external entry points.

  - "Integrity Controls - internal verification that data that is being stored or transmitted is valid.
  - Message Authentication - assurance that the messages sent and received are the same messages.
  - Access Controls - such as dedicated, secure communications lines, OR
  - Encryption - transforming text into unintelligible ciphers through use of special algorithm processes.
  - If using a network, protections must also include Alarms, Audit Trails, Entity Authentication and Event Reporting.
  - Electronic Signature Standard: These are not required, but security regulations state that if an electronic signature is used, then a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

digital signature (PKI implied) must be used as the electronic signature implementation. Certain features must be implemented: message integrity, non-repudiation, and user authentication." Gue, D'Arcy Guerin. The HIPAA Security Rule (NPRM): Overview.)

All entities that create, modify, or store individually identifiable patient information will be required to ensure that this information is maintained in a secure environment. This means securing networks for any system that stores PHI in electronic form. It is essential that an organization provide a 'defense-in-depth' approach to security. In effect, HIPAA is legislating security best practices into the healthcare industry.

Penalties

Civil and federal penalties are established by the Privacy Rule and include penalties for misuse or disclosure of patient information for all health plans, providers and clearinghouses. Civil penalties include a fine of $100 per person per incident with maximums of $25,000 per person for accidental disclosure, within a single year. Federal penalties of up to $50,000 and one year imprisonment can be imposed for knowingly obtaining or disclosing protected information. A penalty of up to $100,000 and five years imprisonment can result if the misuse is under false pretense; and up to $250,000 and 10 years of imprisonment for obtaining or disclosing protected information with the intent to sell, transfer, or use for personal or commercial gain or to cause malicious harm.

Potential/Perceived Barriers

The perceived barriers to compliance with HIPAA's regulations in a medical school environment can also be broken down into four main themes: cultural, administrative, technical, and physical. Barriers can run the gamut from too loud conversations to implementation of highly sophisticated technologies.

Cultural

Of these four, cultural may be the most difficult to overcome.

- We never had to do it that way before; "if it ain't broke, don't fix it;" people are not willing to cooperate; they want to "do their own thing," ignoring policies; "I don't do anything with PHI, so why do I need training?"; conversations in hallways, which may be overheard by others.
- Ability of faculty to purchase and set up non-standard computer hardware and software, ignoring security and installation policies; faculty and staff who purchase and install private wireless networks without implementing wireless security procedures; faculty who feel free to buy non-standard PDAs, but still expect service and support; faculty who keep unencrypted PHI on non-password protected PDAs.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Ownership issues - lack of trust in someone else's ability to keep data private; the ability of data owners to decide where to store information; either unwillingness to track disclosures and provide an accounting, or unwilling to cooperate with Privacy Officer to provide an accounting; data owners who do not see the importance of logging and keeping audit trails of access of critical information.
- Users who will not run anti-virus software on their systems, or will only run their own preferred product, despite policies; unwilling to use password protected screen savers on systems containing PHI; sharing of account names and passwords; wanting an open environment without a DMZ or firewall so they can freely and easily share information or download any type data.
- Users who call the Help Desk to change a password without providing adequate verification of identity.
- Casual attackers, like co-workers, who go through a colleague's desk uninvited, taking advantage of easy access even though it violates social and ethical standards.

A few of these issues can be addressed with HIPAA awareness training, and others can be resolved by information systems departments, with the support of senior administration, implementing secure networking procedures. Other issues are due to the unusual fiscal policies at medical schools and other research institutes – faculty receives semi-autonomous sources of funds, making them often feel independent of the institution. This grant funding frequently includes both computer hardware and software specifications and may stipulate that data be saved in a particular location or format. The independent behaviors encouraged by this funding model can be made compliant most of the time. The worst problems though, are caused by people who simply do not want to comply. Some may even force the issue to the point that sanctions must be invoked.

Administrative

Administrative barriers revolve around policy, procedures, training, documentation, and the economies of writing and maintaining them.

Policies need to be written for:

- Key security topic areas such as security risk management; determining acceptable and unacceptable media for storage of PHI; critical asset identification; physical security; system and network management; authentication and authorization; access control; transmission of data across internal and external networks; vulnerability management; incident management; awareness and privacy training; and disposal of health information, including destruction of media that contains health information.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Government of how health information will be disseminated within the organization and to other covered entities external to the organization; ensuring the enforcement and communication of sanction policies.
- Access of patient data by faculty who see patients in hospital clinics, use the data in their medical school offices, and distribute the information for research and/or teaching purposes; defining who is an information asset owner and who is responsible for performing risk assessments of critical data.

Procedures need to be developed to:

- Protect critical assets; provide authorization and access control for users working on campus, remote users, temporary employees, and third parties such as contractors and service providers; use network-, system-, file-, and application-level access controls and restrictions; inventory hardware and software assets across the entire organization; use data encryption and virtual private network technologies; provide exception and emergency access; produce updated risk analyses.
- Create security incident reporting and response; manage anti-virus software, intrusion detection software, network software.
- Ensure backup and restore capabilities, to include frequency, scope of backup, offsite storage and length of time data will be stored prior to its being archived or destroyed.
- Manage password assignment including complexity, maintenance and change; forbid shared account IDs and passwords; provide access account IDs that are role- or context-based with ability to determine and document accountability.
- Govern the creation of health information, and how information is validated for accuracy; manage data created in multiple systems, including smaller, departmental systems, and determine the system of record; correct discrepancies.
- Manage terminations including timely removal of user accounts as well as user accounts for third parties; distinguish between employee and employer-initiated terminations.
- Manage change control; keep development and test systems separate from production systems; perform security testing prior to introduction of new systems or applications.

Training programs must address the following requirements:

- Development of HIPAA awareness training materials and training programs for diverse groups of people, which must be appropriate to the level of PHI accessed, delivered in a manner that is understandable with the message that these rules are not only important, but non-compliance carries heavy penalties, contains a timely process for ongoing training for

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

new hires and those whose access to PHI has increased; abbreviated training for third party agents and temporary employees.

- Proof that training is complete and tracking of training provided to faculty who move among multiple institutions, without forcing repeat training at each institution.
- Training programs for new hires that includes security content, education regarding protection against and reporting of viruses, managing passwords, and identifying and reporting potential security breaches; educate employees as to whom to contact when they notice suspicious behavior.

Documentation maintained for:

- Application and data criticality analysis; systems, applications and modules listed and ranked for continuity prioritization; sequential order for restarting systems affected by an emergency; disaster plan for enterprise systems; comprehensive contingency plan in effect for the entire organization.
- Access control for on-premise and remote access, for all media including computer-based, paper, voice, etc.; mechanism to grant access to health information on all media, including electronic and paper-based media.
- How data owners may or may not (policy dependent) determine or participate in determining who should have authorized access to their data; which systems and applications are subject to the access control policies and procedures.
- Data backup procedures; management of anti-virus software; audit and review of audit logs; actions for handling of security breaches; review of "lessons learned."
- Ensure that documentation is communicated.

Fiscal controls developed to prevent:

- Constrained resources that force staff to focus only on operations and ignore auditing, logging, intrusion detection systems, defense-in-depth logic.
- Lack of money to cover the cost of providing for changes to comply with HIPAA because much of the funding comes from grants; departments not budgeting for the changes.

The administrative aspect of privacy and security regulations are difficult and costly to implement and maintain because they are broad in scope, not definitive, and require constant vigilance for ongoing compliance.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Technical

Given the staff and monetary resources, time, and technology, technical barriers should be relatively easy to overcome. However, those are a lot of requirements, and many organizations lack the needed resources.

- Design, implement, and maintain an enterprise-wide security architecture, based on satisfying business objectives and protecting the most critical information assets; deploy a layered approach using diversity and redundancy solutions; security controls to protect assets residing on systems and networks; perimeter and internal security applications that implement security policy; access controls at network-, system-, file-, and application-levels; data encryption and virtual private network technologies for remote access.
- Periodic information security evaluations that identify critical information assets (e.g. systems, networks, data), threats to critical assets, asset vulnerabilities, and risks.
- Monitor, audit, and inspect facilities and designate assigned responsibility for reporting, evaluating, and responding to system and network events and conditions; use system and network monitoring tools, as well as filtering and analysis tools to examine the results; respond to events that warrant action.
- Use any of the following for authentication: password, PIN, secure-id token, digital certificate, for authentication that is strong enough to enable identification of someone for disciplinary action; prohibit simultaneous or concurrent connection access of the same user ID.
- Upgrade or replace applications that do not allow for use of IDs and passwords, have the capability of allowing both automatic logoff and generation of audit logs of system activity, or use reporting and alarm capabilities; put in place mechanisms to ensure the integrity of the data and mechanisms that alert when systems/databases have been altered; deploy a systematic discard process that eradicates all data from disks and memory prior to disposal.
- Levels of access should be based on data content and job function using context-based access, role-based access, and user-based access as needed; ability to consolidate all access for a single patient; procedures and technical mechanisms capable of matching release of data with patient consent; ability to track disclosures in order to provide accounting of disclosures, as needed.
- Authenticate outside entities communicating with the covered entities; produce and review an audit trail of access by outside entities; produce an alarm based on unauthorized access or unusual/inappropriate activities.
- Because the Internet is used to transmit patient information, technology capable of ensuring private transmission of email across public network must be developed; implement electronic signature once HHS has

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

published and finalized an electronic signature standard that will meet the consent and authorization requirements.

- Provide Help Desk technicians a way to verify the identity of the individual calling to have a password changed.
- Mandate a regular schedule of backups with validation before and after backup; verify the ability to restore from backups; regularly check for and eradicate all viruses, worms, Trojan horses, other malicious software, or any unauthorized software; apply patches to correct security and functionality problems; perform vulnerability assessments on a periodic basis, and address vulnerabilities when they are identified; regularly verify the integrity of installed software; ensure secure configuration of all deployed assets throughout the life cycle of installation, operation, maintenance, and retirement; regularly compare all file and directory cryptographic checksums with a securely stored, maintained, and trusted baseline; establish and maintain a standard, minimum essential configuration for each type of computer and each type of service.

Implementation of network- and host-based intrusion detection systems that can defend against both casual attackers and determined attackers are essential. Role-based access control of users of centralized databases, with a distinct role defined for each group of users having common access requirements, or context-based access control, taking into account the person who needs to access the data, the type of data being accessed and the context of the transaction in which the access attempt is made, would resolve many of the issues of providing proper access control and the ability to account for disclosures. Once electronic signature, which is still an immature technology, can ensure data integrity, and an Internet encryption application has been implemented to ensure reliability of data, people will be able to safely send PHI across the Internet.

Physical

Physical barriers are probably the easiest to resolve, but are also the ones that are easiest to overlook.

- Servers in IT departments may be in physically restricted areas, but systems containing sensitive/critical data are distributed throughout the campus in locations either easily accessible or poorly protected; access to all critical hardware assets should be controlled.
- Use of password protected screen savers on desktop systems; install automatic logoff applications on shared systems; scan for viruses when using removable media or downloading files; password protect and encrypt data on laptops and PDAs; standardize on accepted and supported hardware, i.e. servers, desktops, laptops, PDAs, and software including business productivity applications, databases for manipulation and storage of patient information, and scientific applications, whenever possible; retire outdated hardware, operating systems and applications.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Lock up any removable media, i.e. diskettes, CDs, or tapes containing PHI, in fireproof/waterproof containers; move any fax machines or printers from locations where PHI could be seen; always use fax cover sheets requesting that if fax is received in error, it should be disposed properly; turn monitors away from public viewing; employ gatekeepers to work in front of areas where paper PHI is housed; always lock areas containing PHI after business hours.
- Retain signed consent and authorization forms, which allows for use or disclosure of PHI for purposes of treatment, payment or health care operations; obtain signed authorization to use or disclose PHI for other purposes, like marketing or fundraising.
- Remind people to lower voices when having conversations about patient information in public areas and could be overheard by others.

Preparation for HIPAA Compliance Implemented in Some Healthcare Organizations

This brief section demonstrates that other healthcare and related facilities are also grappling with some of the same barriers to HIPAA compliance as medical schools. It also describes some of the steps these organizations have taken to meet HIPAA's challenges.

1. To ensure that Medicare business partners, who contract with Medicare to process or support the processing of Medicare's fee-for-service claims, are HIPAA compliant, they must create and submit their system security policies. These business partners include Medicare carriers, fiscal intermediaries, standard claims processing system maintainers, regional laboratory carriers, and claims processing data centers. In order to qualify as a Medicare business partner, every system must have a system security plan that documents its security posture as it is currently operating. Business partners are required to perform a triennial risk assessment. All system and information owners must develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken. They must consolidate security documentation (paper documents, electronic documents, or a combination) into a system security policy. ("CMS Business Partners Systems Security Manual." Centers for Medicare and Medicaid Services (CMS) Security and Standards.)

2. In one state, policy development was handled in a collaborative manner. In 2000, the state created a HIPAA Readiness Collaborative comprised of major private sector hospitals, major health insurers, and the state hospital system. It received its direction from key CIOs and CFOs. The goal was to reduce the administrative costs of HIPAA implementation for participating organizations, and to improve interoperability between facilities in the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

community through the use of standard technologies. The HIPAA collaborative's ongoing effort to develop security policies and guidelines to meet HIPAA standards was based on a statewide understanding of the HIPAA security rule, shared among its participating members. (Sato, Miles M. HIPAA Security Policy Development: A Collaborative Approach.)

3. Hospitals must have technical security services which include: documented procedures for obtaining necessary information during a crisis, and at least one of the following: context-based access, role-based access, or user-based access. They must also have audit controls, mechanisms employed to record and examine system activity; authorization control, a mechanism for obtaining consent for the use and disclosure of health information; data authentication, a process to corroborate that data have not been altered or destroyed in an unauthorized manner; and entity authentication, a mechanism to confirm that an entity is the one claimed. (Technical Security Services – HIPAA.)

4. At a 350-bed hospital in California, a systematic approach to solving technology challenges was taken. HIPAA requires reasonable steps to fortify the security of the networks, applications and data. By deploying primary and secondary firewalls, intrusion detection, and network security software with biometrics, and moving to enterprise single sign-on to strengthen security, the hospital was able to increase convenience for users, and control IT support costs. (Shehata, Ash. "Strengthening System Security to Prepare for HIPAA." HIPAA Watch.)

5. The 380 members of a medical university faculty practice plan, and their staffs, are already up-to-date on many of HIPAA's regulations, particularly those dealing with privacy. HIPAA education and other resources were provided to physicians and to their practices, offering their physician members and practices the resources needed to ensure that they had systems, policies and procedures in place to make them fully compliant with HIPAA regulations. Although policies and procedures were already in place, they needed to be formalized to make them HIPAA compliant. Many challenges are still posed by the proposed security regulations. Existing software applications, particularly those that deal with individually identifiable health information, will need an appropriate level of security established for access for all users. Existing applications will be inventoried, and new software applications purchased to ensure compatibility with the existing technology infrastructure and in order to meet the intent of the proposed Security Rule under HIPAA. The privacy of health information must be protected by implementing appropriate security measures yet at the same time assure that access to the minimum amount of information necessary could be readily attained by those who needed it. ("University Hospital and UMAS preparing for HIPAA privacy compliance." Upstate Update Newsletter.)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6. In the nursing home industry, access control is of particular concern because the employee turnover is high. Careful consideration must be given to the overhead required to manage several access control methods that might apply to different systems. Organizations will have to choose between the administrative complexity of supporting several access control methods and the benefits of using similar control methods across several applications or systems. Tools already available through the Microsoft Windows 2000 Active Directory, like user-based and role-based access control, will help with this process, since these are effective, cost efficient, and already in place. (Cole, Kenneth. HIPAA Compliance: Role Based Access Control Model.)

Conclusion

To answer the question asked at the beginning of this paper, "Given that faculty are involved in education, research and clinical practice at a variety of affiliated medical and research institutions, and data containing PHI resides in a distributed fashion in a variety of databases on a variety of platforms, what are some of the ways that a large medical school can begin to implement HIPAA's controls and overcome the many potential barriers to compliance?" several separate areas were examined. First, the background and rationale for the HIPAA regulations, and then a description of the various requirements were delineated. Potential barriers to compliance were detailed, and finally, the ways a few healthcare-related organizations are proceeding to meet the requirements were portrayed.

Some of the barriers appear overwhelming, requiring not only technological changes, but also administrative and cultural, i.e.:

- Because data is stored on a variety of platforms, in a variety of applications, with no common format and no common fields that would easily allow joining of databases, migration of data to a centralized medium is very difficult. Without a centralized database, access control and tracking of disclosure becomes a monumental task.

What can be done on an organization-wide basis to ease the way?

- Top-down leadership.
- Mandate compliance.
- Provide appropriate funding.
- Determine what is reasonable and appropriate.
- Utilize cost-effective solutions.
- Use the technical resources already available on current systems.
- Educate to enhance personal and organizational awareness of HIPAA.
- Evaluate risk by performing a baseline HIPAA readiness assessment and study the organization's current and future system functionality.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Develop an action plan, incorporating the current security infrastructure and taking into consideration new technology/infrastructure.
- Implement the action plan. HIPAA compliance will require a well-coordinated, resource-intensive effort.
- Once achieved, HIPAA compliance must be maintained. Responsibility for monitoring HIPAA compliance must be assigned and a plan to monitor it put into place.

Violating the HIPAA regulations can lead to $250,000 in fines and up to 10 years imprisonment. Other sanctions include civil litigation, negative affect on accreditation status, damaged reputation and loss of contracts that require HIPAA compliance.

There are myriad barriers to the adoption of better information security practices and technology. The result of HIPAA compliance though, will be sound information privacy and security practices and a secure health information system.

References

"CMS Business Partners Systems Security Manual." Centers for Medicare and Medicaid Services (CMS) Security and Standards. February 13, 2002. URL: http://cms.hhs.gov/manuals/117_systems_security/BP_Sys_Security_Man.asp

Cole, Kenneth. HIPAA Compliance: Role Based Access Control Model. URL: http://www.giac.org/practical/Kenneth_Cole_GSEC.doc

Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices. Internet Security Alliance, First Edition, July 2002.

Draft HIPAA Security Summit Guidelines. June 26, 2000. URL: http://www.smed.com/hipaa/news/notes/draft.pdf

Fagin, Daniel. HIPAA Security Standards v1.2d. August 10, 2001. URL: http://rr.sans.org/standards/HIPAA_sec.php

Ferrell, Tim. Impact of HIPAA Security Rules on Healthcare Organizations. October 4, 2001. URL: http://rr.sans.org/policy/sec_rules.php

Gue, D'Arcy Guerin. The HIPAA Security Rule (NPRM): Overview. URL: http://www.hipaadvisory.com/regs/securityoverview.htm

HIPAA primer. URL: http://hipaadvisory.com/regs/HIPAAprimer1.htm

Meyer, Stanton. HIPAA: What it Means for Privacy and Security. March 3, 2001. URL: http://rr.sans.org/country/HIPAA_sec.php

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"Role-based access." Health Management Technology. July 2001. P.14. URL: http://www.peacefulpackers.com/it_solutions/hs17.htm

Romig, Tautra. HIPAA Compliance: Cost-Effective Solutions for the Technical Security Regulations. November 21, 2001. URL: http://rr.sans.org/legal/compliance.php

Sato, Miles, M. HIPAA Security Policy Development: A Collaborative Approach. April 30, 2001. URL: http://rr.sans.org/policy/HIPAA_policy.php

Shehata, Ash. "Strengthening System Security to Prepare for HIPAA." HIPAA Watch. September 2002. URL: http://www.healthmgttech.com/archives/hipaa0902.htm

Singh, Arun K. HIPAA Privacy and Security: what needs to be done? Infosys Technologies Ltd. 2001. URL: http://www.infosys.com/healthcare/pdfs/HIPAA-PrivacyandSecurityleaflet.pdf

Smith, Harry E., CISSP. A Context-Based Access Control Model for HIPAA Privacy and Security Compliance. July 18, 2001. URL: http://rr.sans.org/legal/control_model.php

"Standards for Privacy of Individually Identifiable Health Information." Federal Register. Vol. 67, No 157. August 14, 2002. URL: http://fr.cos.com/cgi-bin/retrieve?db=fr_2002&ac2=20020814a1

"Standards for Security and Electronic Signatures: Proposed Rule." Federal Register. Vol. 63, No. 155. August, 12, 1998. URL: http://www.hipaadvisory.com/regs/Regs_in_PDF/security_electronic_sign_stand.pdf

Technical Security Services - HIPAA. URL: http://www.peacefulpackers.com/it_solutions/hs15.htm

"Technical Security Services to Guard Data Integrity, Confidentiality, and Availability." NPRM: Security and Electronic Signature Standards. June 19, 2001. URL: http://aspe.hhs.gov/admnsimp/nprm/sec08.htm

"University Hospital and UMAS preparing for HIPAA privacy compliance." Upstate Update Newsletter. July 31-Augst 14, 2002. URL: http://www.upstate.edu/hr/update/archive_2002/020731.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced