Global Information Assurance Certification Paper

Health Insurance Portability and Accountability Act: Security Standards; Implications for the Healthcare Industry

Terri Gohri

SANS Security Essentials GSEC Practical Assignment Version 1.3

Summary

Computer and networking technology is being used more and more in the healthcare industry in order to improve efficiency, reduce costs and decrease paperwork. As a result privacy concerns have been increasing due to the more rapid availability of sensitive patient information. In response to these growing concerns the US Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. HIPAA mandated that the Department of Health and Human Services (DHHS) establish a set of rules under the subheading Administrative Simplification. One of those rules includes Security and Electronic Signature Standards.

The security standards proposed by DHHS are the subject of this paper. Federal security standards and the increased use of the Internet and web technologies in healthcare will require changes in the healthcare industry's information security practices. This paper provides some background information about the emerging Federal requirements, industry implications, and the actions that will be required.

Background

The Health Insurance Portability and Accountability Act (HIPAA) was passed on August 21, 1996. The HIPAA legislation contained a section called Administrative Simplification, which states that it is:

"intended to reduce the costs and administrative burdens of health care by making possible the standardized, electronic transmission of many administrative and financial transactions that are currently carried out on paper."

The Administrative Simplification provisions of HIPAA call for: Electronic Data Interchange (EDI) transaction standards; unique health identifiers for each individual, employer, health plan and healthcare provider; security standards; and privacy legislation. The logic behind the set of requirements was that standards and unique identifiers would facilitate the exchange of information needed throughout the care delivery system. Making these transactions easier, however, may increase the risk of inappropriate access to sensitive information. Consequently, HIPAA also calls for security standards and privacy legislation.

According to the HIPAA legislation the security standards apply to claims clearinghouses, health plans, employers and healthcare providers; i.e., "any other person furnishing health care services or supplies" (other than those under the statutory definition of "provider") that maintain or transmit automated health information.

In the current documents, all requirements, except cryptography and digital signature, must be addressed for "All entities, regardless of size, involved with electronic health information pertaining to an individual". Recognizing that an industry consensus on security standards does not exist, the Healthcare Financing Administration (HCFA) is trying to establish a flexible framework for security practices that meet the goals of security without prescribing the means. Proposed rules codifying the matrix were published on August 12, 1998. Final rules had a statutory deadline of February 21, 1998 but the agency has let the time frame slip and final rules have yet to be published. Depending upon their size, plans and providers will have two or three years from the date the final rules are published to comply. Small plans as defined in the rules will have 36 months to comply. HCFA also has discretion to take into account the needs and capabilities of small and rural healthcare providers (to be defined in the rules) in adopting the security standards.

Administrative Simplification

The Health Care Financing Administration, in the Department of Health and Human Services, is responsible for implementing the Administrative Simplification requirements through notice and comment rulemaking. HCFA developed a draft security matrix and proposed rules that capture the requirements and implementation features the healthcare industry will be expected to meet. HCFA has categorized these requirements as –administrative procedures; physical safeguards; technical security services to guard data integrity, confidentiality and availability; technical security mechanisms to guard against unauthorized access to data that is transmitted over a communications network; and electronic signatures. Although the requirements in these categories overlap, they are intended to help organizations understand the different types of requirements needed for a comprehensive security approach.

A number of consulting companies such as IBM, e-fense Services, RSA etc. are marketing services to the health care industry to help them comply with HIPAA. They basically all agree on a core set of requirements that must be implemented. Those core requirements are: Certification, Media Controls, Chain of Trust Partner Agreements, Physical Access Controls, Contingency Plan, Policy Guidelines on Work Station Use, Secure Locations for Work Stations, Formal Mechanisms for Processing Records, Security Awareness Training, Information Access Control, Access Control (context based), Internal Audit, Audit Controls, Personnel Security, Authentication, Security Configuration Management, Authorization Control, Security Incident Procedures, Cryptography, Termination Procedures, Unique User Identification, Training, Communication Network Controls, Assigned Security Responsibilities, and Digital Signatures.

Administrative Procedures to Guard Data Integrity, Confidentiality and Availability

This section includes the requirements for formal documented policies and procedures such as certification (self or third party), chain of trust partner agreement,

contingency plan, formal procedures for processing records, information access control, internal audit, personnel security, security configuration management, security incident procedures, security management processes, termination procedures and training plans. Organizations must perform risk analysis and develop security policies for their organizations.

All of these security policies and technologies will require security training for employees (most of which have never concerned themselves with security in the past). Most people want to do the right thing in terms of security and patient privacy, however, it is human nature to cut corners. Therefore, HIPAA carries a big stick in the form of penalties for non-compliance. The HIPAA statue establishes two sets of penalties: one set is for "failure to comply with requirements and standards" and the second set is for "wrongful disclosure of individually identifiable health information." Penalties for noncompliance are a maximum of $100 for each violation not to exceed $25,000 per year. However, a person who knowingly discloses individually identifiable health information, the penalties range from $50,000-$250,000 in fines and one to ten years in prison. It remains to be seen whether "knowingly" ignoring the rules and failing to establish a security program might be interpreted as "knowingly" causing such a disclosure if it were to occur.

Physical Safeguards to Guard Data Integrity, Confidentiality and Availability

Each organization must determine what physical safeguards are appropriate for their own environment. The intent of the legislation is not to dictate a minimum set of physical security safeguards. That would not be practical since there are a multitude of different environments in the health care community. For example, it may not be feasible for a hospital to implement many of the physical security safeguards that a doctor's office or health insurance company should or could because the hospital is typically a public access building. This section of the Administrative Guidelines does provide suggestions on how to physically secure the computer systems and files, delegate security responsibility to an individual, provide physical access controls, document policies and guidelines on workstation use, secure workstation location, and security awareness training.

Physical safeguards to be considered are data backup systems and disaster recovery plans. Tamper resistant storage materials should also be considered. Larger organizations may need to make arrangements for an off site location to store back up materials.

Technical Security Services to Guard Data Integrity, Confidentiality and Availability

Technical security requirements include access control, audit controls, authorization controls (i.e., obtaining consent for use and disclosure of health

information), data authentication (i.e., data integrity), and entity authentication otherwise known as non-repudiation.

HIPAA requires entity authentication in order to prevent the improper identification of the entity i.e., the physician of record or technician reviewing/analyzing lab results, that is accessing secure data. The implementation must support automatic logoff and unique user identification. This requirement may be accomplished by using a variety of technologies. The most simplistic form and by the way the weakest is userid strings whose authenticity is established by user supplied passwords. Automated password generators are a method to strengthen a password however some feel (this author for one) that automated password generators weaken security. I believe that people should be encouraged and forced from an automated stand point to create strong passwords versus being provided with a computer generated one that they cannot remember and will most likely write down. For stronger assurance methods, I recommend technologies such as two-factor authentication, digital certificates, and/or smart cards. Like the physical safeguards this is an area that must be assessed by each organization.

HIPAA also requires access control to restrict individual access to resources, allowing access only by privileged entities with a business need to access it. Organizations can use user-based, role-based or context-based access. Some technological developments may significantly change the way people access systems, such as biometric authentication. It will not be required by the standards, but may emerge as a health care industry preference for controlling access by unauthorized users. The advantage of the biometric access control is that it can't be lost, doesn't require memorizing one of many access codes, and can be linked to site security as well as system security. It is clear that technical breakthroughs such as this will continue to offer methods for addressing inappropriate access once an organization has determined who is or is not authorized. What works for one may not work for all. Biometrics is most likely a great option for the office environments of an insurance company but most likely won't work in a hospital where doctors, nurses and technicians are often wearing protected gear such as gloves and eye wear.

Technical Security Mechanisms to Guard Against Unauthorized Access to Data Transmitted Over a Communications Network

This section covers the requirements for technical security mechanisms including communications/network controls, integrity controls, message authentication, access controls, encryption, alarm, audit trail, entity authentication and event reporting.

HIPAA requires controls to ensure that communications over open networks such as the Internet cannot be easily intercepted and to protect the system from intrusion. When transmitting patient data via the Internet, encryption is mandatory. Provisions must be made for integrity controls, message authentication, access controls, audit trails, entity authentication and event reporting.

Access control limits access to only those individuals with the necessary access privileges. From a technical standpoint, it can be provided with strong authentication methods such as digital signatures or a minimum of two-factor authentication. However, the first step to effective access control is a matter of determining who requires access to what information and documenting it as policy.

Electronic Signatures

This section contains electronic signature requirements including digital signature, message integrity, non-repudiation and user authentication.

HIPAA requires that if used, an electronic signature must be a digital signature (cryptographically-based) and must support message integrity, non-repudiation and user authentication. DHHS requires cryptographically-based digital signatures since there are no other standards that provide non-repudiation in an open network environment. Public Key Infrastructure (PKI) is a potential way ahead for implementing digital signatures. According to RSA Security, PKI is a system whereby each end-user is issued a private/public key pair (pair of numbers with a unique mathematical relationship). The keys are used for encryption and decryption and digital signing. Data that is encrypted with a public key can only be decrypted with the corresponding private key. Private keys are used to generate and attach a digital signature to a file, document or message and the corresponding public key is used to verify that signature. Public keys are also embedded in a data file called a digital certificate, which is used as a form of electronic identification. PKI is probably the most feasible way to implement digital signatures and provide non-repudiation. There are a number of vendors who can provide this technology.

Privacy, Confidentiality and Security

There is often confusion about the difference between privacy, confidentiality and security. In the context of HIPAA, privacy determines who should have access, what constitutes the patients rights to confidentiality, and what constitutes inappropriate access to health records. Under HIPAA's privacy regulations the patients must sign consent forms allowing disclosures of their information for billing and treatment and be told how their information is being used and by whom. The privacy rule also covers the policy and procedures that must be in place to ensure that the patients' health information is protected and their rights are upheld. The Security Standard is a companion to the privacy rule. Security establishes how the records should be protected from inappropriate access, in other words the means by which you ensure privacy and confidentiality.

Healthcare organizations will need to develop their own confidentiality and privacy policies to have a meaningful security program. In other words, healthcare organizations have to decide who is authorized to have access to identifiable healthcare information, for what purposes, and under what conditions if security plans, policies and procedures are going to have any meaning. Even with a Federal law the level of

specificity will not be determined at the institutional level. Developing these policies will facilitate the development of a healthcare organization's security program.

Implications of the Security Standards for the Healthcare Industry

The healthcare industry, like most industries with the possible exception of banking, has not addressed information security in a comprehensive manner. Most healthcare organizations have security features that are built into their information systems, however, they are not activated. Additionally, most organizations do not have written policies or procedures for their employees that are authorized to access the information. Policies on disclosure of sensitive information or personnel policies dictating the types of personnel actions that will be taken if staff members violate the policies need to be implemented in order to comply with HIPAA standards.

Automated medical information also highlights concerns about information availability, particularly as more clinical information is stored electronically. Ensuring information availability through appropriate access and data integrity (i.e., knowing that the information in an organization's systems has not been inappropriately or inadvertently changed and that it is not at risk of being lost if the system fails) may be as important as confidentiality. Part of the Administrative Simplification provisions' stated purpose is "encouraging the development of a health information system." Such a system is intended to support access to critical health information when and where it is needed. Automated information systems can support the real-time availability of information on drug allergies, current complicating illnesses and urgent lab results in a way that paper records never could. Information systems can only ensure availability if the systems are working and the information is not easily changed. The goal of information availability supports the proposed HCFA requirement for a contingency plan that includes disaster recovery, an emergency mode operation plan, and a data backup plan.

HCFA's proposed standards imply that healthcare organizations will develop security programs that include technological solutions, but recognize that the persistent risk, regardless of the level of technical security, is through the people who have authorized access rather than "hackers". Consequently a number of standards address personnel and physical site access, e.g., personnel security, training, termination procedures for both physical and system access and physical access controls.

The planning, policies and procedures driven by the standards will perhaps have the most dramatic effect on healthcare organizations because they will have to develop enterprise wide security programs and gain organizational support for the programs. It will not be sufficient to have a variety of policies and procedures in each department that may or may not be explicit, documented or known by the rest of the organization. With or without privacy requirements, organizations should review more closely who has access to which information and establish policies and accountability for these decisions. With potential penalties as high as $250,000 and ten years in prison, not to mention the negative publicity, it behooves everyone to take a proactive approach to security.

The new security standards, once finalized, will probably not have a great impact on information systems. Most of the technologies needed for compliance are readily available. HCFA has made a conscious decision to not specify technology. HCFA expects health care organizations to determine the appropriate technical solutions on the basis of their risk assessment and level of vulnerability the organization is willing to tolerate. More complex information technology environments may require more attention and internally developed systems may require custom solutions.

The security standards and HCFA's Internet policy may have a significant impact on one information system decision: whether to use the Internet or a private secure network. HCFA is in the process of revising its current Internet policy, which prohibits the use of the Internet for transmitting any Medicare Beneficiary information. The revised policy is expected to allow Internet policy with encryption and digital certificates. The preamble of the proposed security standards requires encryption for patient data that traverses the Internet. These added requirements may tip the balance of the decision in favor of a private network.

HCFA, at present, is not planning to require either encryption or digital signature under the security standard for non- Medicare information. Therefore the most significant technical requirements maybe the audit controls and the "accountability (tracking) mechanism." Industry representatives are already expressing concerns that a 100% audit trail of all actions affecting any identifiable records will add significant costs to automated health records. This issue is likely to be a topic of debate in the proposed rule public comment process with privacy advocates on the side of complete audit information and industry advocates calling for exception auditing, i.e., mechanisms that track actions that are not consistent with the expected uses of an application or system. At present HCFA is not planning to stipulate the extent of the audit requirement, again relying on the organizations determination regarding the level of appropriate auditing. Certain types of information may warrant 100% audit trail, for instance, organizations may want to closely monitor access to AIDS or substance abuse information. This is an age old question involving performance versus security that will require each organization to evaluate during their risk assessment.

Next Steps

Depending upon the scope and complexity of the health care organization and its information technology environment, compliance with the HIPAA security standards could be quite time consuming. Although the final technical solution may be relatively simple, the security program design and facilitating organization buy-in to security plans, policies and procedures suggest starting early.

How to Get Started

First, assign at least one individual with primary responsibility for security. The person should probably be one hundred percent dedicated, unless it is a very small organization. Although many organizations tend to choose someone in their IT

organization, I recommend thinking about someone with broader responsibilities that can speak to the personnel and administrative requirements as well as the IT solutions. In other words, select someone with authority and visibility in the organization or give them direct reporting responsibilities to a senior executive in the organization.

Next, create a security team that has representation from throughout the organization charging all relevant departments with responsibility for individually identifiable information. This team should help develop the security program and support buy-in within the organization. The team's first task should be to review current policies, procedures and solutions against the most current documentation regarding the emerging security standard to access how significant an undertaking compliance will be for the organization. Based on this assessment, determine if the organization has the skills and the resources to drive this effort internally or should seek external expertise. Compliance with the security standards has noted similarity to year 2000 preparations. Security skills and resources are scarce and demand only increases as the compliance deadlines approach.

Whether the organization chooses to implement HIPAA standards with in-house or outside expertise, a high level assessment of the present security status needs to be conducted. The gaps between the present system and what is required by the HIPAA initiatives and standards must also be completed. The next step should be a risk analysis. Risk analysis is a required implementation feature of the draft security management process standard which HCFA currently defines as:

"Identification and evaluation of types of security risks, their probability of occurrence, and their potential adverse impact of an automated system".

This step should help set parameters for an organization's security program and define its priorities. With these initial steps and all subsequent steps, be sure actions and decisions are documented. It will be only through documentation that an organization can demonstrate it has addressed many of the requirements.

Summary

The health care industry as a whole has a lot of work to do in order to comply with HIPAA. Fortunately the technology is there and the consultants have programs in place ready to come in and help (for a small fee of course!). In my mind this legislation was written for INFOSEC professionals in the sense that it touches on nearly every aspect of Information Assurance and the principles and technologies associated with it.

References

Administrative Simplification, US Department of Health and Human Services (HHS) website, http://aspe.hhs.gov/admnsimp/

HIPAA Comply, "The Definitive Source for information on HIPAA security and privacy compliance", http://www.hipaacomply.com/

HIPAA News, "The Latest about HIPAA, http://www.hipaadvisory.com/news/

HIPAA Security Matrix, http://www.ibm.com

Koss, Shannah, "Getting Ready for HIPAA Security Compliance", 1999, http://houns54.clearlake.ibm.com/solutions/healthcare/helpub.nsf/Files/HIPPAA/$File/HIPPAA.pdf

RSA Security web site, www.rsasecurity.com

The Healthcare Financing Administration (HCFA) web site: http://www.hcfa.gov/

The Health Insurance Portability and Accounting Act of 1996 Public Law 104-191.

The Health Insurance Portability and Accounting Act of 1996 (HIPAA) Page, http://www.hcfa.gov/hipaa/hipaahm.htm