Global Information Assurance Certification Paper

Gaudy Alvarez
January 27, 2001

HIPAA - Security Standard
How It Will Impact Healthcare & Security In Information Technology

The proposed Security Standard of the Health Insurance Portability and Accountability Act (HIPAA) signed into law on August 26, 1996 proposes to improve the quality of patient care by requiring the assurance of secure and confidential patient information that is electronically stored, maintained or transmitted. The standard is composed of administrative, physical, technical security services and technical security mechanism procedures and implementation features that will impact how the healthcare industry does business and the role of security in Information Technology within this industry.

The security standard will affect plans, providers, clearinghouses and any organizations that handle healthcare information and is composed of several procedures and implementation features that need to be implemented in order to comply with the security standard. Furthermore, the effected entities are responsible for ensuring that their business partners, including vendors, are in compliance with the security standard. If any affected organization fails to comply with any of the procedures and/or implementation features mandated by the security standard fines and penalties will be imposed upon such party.

To ensure that the standards can be met by all healthcare organizations, big and small, the standards are neither technology nor solution specific. The standards mandate that patient identifiable information be maintained confidential, integral and secure and has specific requirements that must be met in securing healthcare information but the standard does not regulate the methods and technologies used to accomplish such. Instead, the methods and technologies used must be determined by the affected entities since security practices are dependent on each organization's security needs and risks. Each entity must analyze their systems, network, data and physical layout so that their needs are met and the standard effective in safeguarding such data. All procedures and implementation features must be implemented, documented, reviewed and updated regularly.

Administrative Procedure

The first step in ensuring the confidentiality, integrity and availability of patient information will be documented administrative policies and procedures that will indicate the security measures that need to take place in order to accomplish this. The administrative procedure will introduce existing security practices that will be new for many of the affected entities and in many instances it will mean additional costs, resources and time.

Systems or network designs will have to be evaluated to ensure they meet the security standards and certified either internally or by an external audit agency. This process will have to take place regularly to ensure that security holes have not been created by intruders, employees or changes made to systems/networks during routine maintenance.

In instances where data is being shared between an organization and a third party, agreements that ensure the confidentiality and protection of the data being transmitted will have to be established or reviewed and updated to include the requirements of the standard. This will ensure that the data being exchanged is secure at all times and distribute responsibility amongst all parties involved.

The availability of healthcare data is crucial so a contingency plan that indicates how an organization would respond to a system emergency must be in place. This includes a documented applications and data criticality analysis that rates the importance of each system and it's data, the regular backup of systems and data, disaster recovery plans and emergency mode operation plans that specify how daily operations will continue and how data will be recovered in case of an emergency situation as well as the testing and revision of such to ensure everything is functional and to accommodate and any changes made to the systems and network.

Policies and procedures that ensure the proper handling, maintenance, transmittal and disposal of health information and that specify how access to healthcare information is to be granted must be developed and implemented. To ensure that this is accomplished the standard will require access authorization, establishment and modification policies and procedures.

An on-going internal audit process must be in place to help identify any security violations. The standard does not specify what needs to be audited, however, because of the authorization and access controls required, there are certain events that must be audited such as logins/logouts and system and data accesses, changes, deletions. Additional events to be audited will be determined by each entity and will be dependent on their needs. This audit process must be accompanied by a method that ensures the security and integrity of these audit logs by restricting access to these logs.

Anyone accessing health information will be required to have proper documented authorization to do so. Records of all access must be maintained, all personnel accessing healthcare information must have security training, policies and procedures for clearance must be implemented and security policies in place. Proper levels of access must be granted to all personnel and those providing maintenance services for technical systems must be properly supervised.

Policies and procedures must be developed and implemented to ensure the security of Information Systems. These policies and procedures are to be integrated with change control to ensure that the changes being made to software/hardware do not create security holes. Documentation, hardware/software installation and maintenance review and

testing for security features, inventory procedures, security testing and virus checking must be part of these policies and procedures.

Policies and procedures to report and respond to security incidents must be in place to ensure that security breaches and violations are reported and handled promptly. It also requires policies be created, administered and overlooked to prevent, detect, contain and correct security breaches. Risk analysis and management as well as sanction and security policies are required to establish a formal security management process to address all security issues.

To ensure the proper removal of a terminated employee's access termination procedures must be implemented. Changing combination locks, removing users from access lists and accounts and confiscating keys, tokens or cards that allow access must be a part of these procedures.

A formal security-training program to educate all users on the protection of all health information must be developed and implemented. This training program must include periodic security reminders, virus protection, monitoring login success/failure, reporting discrepancies and user education in password management.

Physical

The standard will require the effected entities to designate security responsibility to either a specific individual or organization. This individual or organization will be responsible for the management and supervision of the use of security measures to protect healthcare information and personnel's access to this information.

Documented policies and procedures that establish media controls will also be required to ensure further protection of healthcare information when contained in any type of media. The controls that must be included in these policies and procedures are controlled access to the media, asset tracking, data backup, storage and disposal.

Documented policies and procedures that provide physical access controls which include disaster recovery, emergency mode operation, equipment controls, security facility plan, verification of authorization prior to granting physical access, maintenance records, procedures for access on a need-to-know basis, sign-in for visitors and testing and revision will be required.

All personnel accessing healthcare information is responsible for the appropriate use of the resources used to access such data and so documented policies and procedures that detail proper workstation use and proper login and logout of systems will be required. In addition, all workstations will be required to be in secured locations to minimize theft and the viewing or accessing of information by unauthorized users.

Security awareness training will be part of both the administrative and physical

procedures of the standard and requires security training for all personnel having access to healthcare information so that this information is handled properly and in compliance with the standard.

Technical Security Services

Access control methods will need to be in place to ensure access is granted on a need-to-know basis to authorized and privileged entities only. A procedure for granting emergency access must be in place and access must be granted using role-based, user-based or context-based authentication, leaving encryption optional.

Audit controls to monitor system activity and accesses to healthcare information will be required to ensure that all systems and data are secure and all suspect activity is responded to accordingly.

Some type of authorization control must be implemented, a documented method of authorizing access to healthcare information to ensure only authorized personnel have access using either role-based or user-based access.

A method that ensures data integrity will be required, the method used in doing so will be determined by each entity. Also, a method that guarantees the entity logged in or accessing data is who the login says it is will be required. In order to accomplish this the standard requires the use of automatic logoff and the use of unique user identification and either biometric, password, personal identification number, telephone callback or a token system.

Technical Security Mechanisms

If an organization uses a network to store or transmit electronic healthcare information the standard requires that features preventing data from being intercepted, interpreted by unauthorized parties and accessed by intruders be implemented. Alarm, audit trail, entity authentication and event reporting are security technologies that must be implemented to comply with the standard. Integrity controls, message authentication and either access controls or encryption are additional features that need to be implemented when using open networks such as the Internet or dial-in lines.

All procedures and implementation features will mean major changes for most if not all entities affected by the security standard and the role of security Information Technology will become more important and involved. Security technologies will need to be implemented with any new systems and changes to existing systems or network requiring additional time and money to be allocated for all projects to allow for the integration of these procedures and implementation features.

The security standard will effect the decision-making process, the vendor and business partner selection process, what systems to implement, what features of a system to

implement, redesigning the physical layout of an office space or unit, moving or placing a computer, implementing new technologies and processes to facilitate healthcare information etc., will no longer be decisions made without the involvement of the party or organization responsible for security.

Policies and procedures will need to be developed, implemented, maintained and reviewed. Existing contracts with vendors and business partners will have to be reviewed and modified to ensure the requirements outlined in the standard are met. Complying with the security standard will require the use of security technologies to control and monitor access, the evaluation of existing systems and network design to ensure they meet the requirements and in instances where existing systems and/or network designs do not meet these requirements the enhancement or replacement of existing systems must be made.

Complying with HIPAA's security standard will have a significant financial impact on the effected entities in the short term but standardization will allow healthcare information that is electronically stored and transmitted to be more secure and inaccessible to unauthorized users and intruders while facilitating access to authorized users thus improving the overall quality of patient care.

Sources

Bronco, Marcia. "Overview of HIPAA's Security Concepts." GSEC – GIAC LevelOne Security Essentials Certified Graduates. 13 April, 2000. SANS Institute.
URL: http://www.sans.org/infosecFAQ/legal/HIPAA.htm (16 January 2001)

"HIPAA Insurance Reform." Health Care Financing Administration.
URL: http://www.hcfa.gov/medicaid/hipaa/content/more.asp (18 January 2001)

"Notice of Proposed Rule Making for the Security and Electronic Signature Standards." 12 August, 1998. U.S. Department of Health and Human Services.
URL: http://aspe.hhs.gov/admnsimp/bannerps.htm#security (16 January 2001)

"Standards for Security and Electronic Signatures." HIPAA Advisory.
URL: http://www.hipaadvisory.com/regs/securityandelectronicsign/index.htm (21 January 2001)

Rhodes, Harry B. "The High Cost of Privacy." IN Confidence. Vol. 9 No. 1 (2001): 3-4.

Sobel, David A. "The Information Security Manager: Three Key Responsibilities." IN Confidence. Vol. 9 No. 1 (2001): 1-2.

Jones, Rys W. "Doing Business in the Healthcare Privacy Era." IN Confidence. Vol. 9 No. 1 (2001): 7-9.