



HIPAA Challenges for Information Security: Are You Prepared?

White Paper

**by Jonathan Bogen
2001**

Phone: 781.585.6002 • Email: Info@HealthCIO.com • www.HealthCIO.com

HEALTH INSURANCE PORTBILITY AND ACCOUNTABILITY ACT

Challenges for Information Security: Are You Prepared?

At the beginning of the new century, the patchwork of state and federal regulations regarding health information is coming under a set of federal regulations representing a national information infrastructure. Increasingly sophisticated technology presents opportunities in advancing integrated healthcare, improving access and quality of care, and reducing administrative costs. Today, health information is accessed from multiple locations by multiple healthcare providers or health plans. Along with this great promise, however, come increased threats in terms of privacy and security of medical information. HIPAA promotes adoption of lower cost Internet technology. The Internet will probably be the platform of choice in the near future for processing health transactions and communicating information and data. Therefore, information security is of paramount importance to the future of any health care program.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA PL 104-191) was passed with provisions subtitled Administrative Simplification. The purpose of this Act was to improve Medicare under title XVIII and XIX of the Social Security Act as well as the efficiency and effectiveness of the healthcare system through the development of a health information system with established standards and requirements for the electronic transmission of health information. HIPAA is the first ever national regulation on medical privacy and is the most far-reaching federal legislation involving health information management affecting the use, release and transmission of private medical data. Health care providers will need to be in compliance with HIPAA as penalties are significant for non-compliance.

HIPAA has important implications for all healthcare providers, payers, patients, and other stakeholders. The Administrative Simplification standards are lengthy and complex, with immediate impact being placed on the following areas:

- Standardization of electronic patient administrative and financial data
- Unique identifiers for providers, health plans, and employers
- Changes to most healthcare transaction and administrative information systems
- Privacy regulation and the confidentiality of patient information.
- Technical practices and procedures to insure data integrity, security, and availability of healthcare information.

HIPAA SECURITY REQUIREMENT

If the security fails, a breach of confidentiality can occur, and the privacy of the individual may be compromised. (HealthCIO Inc.)

HIPAA mandates a set of rules to be implemented by health providers, payers, and government benefit authorities as well as pharmacy benefit managers, claims processors, or other transaction clearinghouses. HIPAA security and privacy requirements may be separate standards but they are closely linked. *Privacy concerns what information is covered, and security is the mechanism to protect it.* The privacy and the proposed security standard of HIPAA apply to any individual health information whether it is oral or recorded in any form or medium. The information identifies the individual or can be used to identify the individual. This is a significant departure from the draft rules that covered only electronic information. This is much broader than the specific transactions defined in the law. As such it will require a significant change in the way health information is handled, disseminated, communicated, and accessed. The electronic signature standard applies only to the transactions adopted under HIPAA. However, none of the HIPAA-related transactions require electronic signatures at this time. The security standard was developed with the intent of remaining technologically neutral in order to facilitate adoption of the latest and most promising developments in evolving technology and to meet the needs of healthcare entities of different size and complexity. As of December 28, 2000 the privacy standards have been published but the security standards are still awaiting finalization (**Federal Register** / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations). The standard is a compendium of security requirements that must be satisfied. The solution will vary from provider to provider, but each provider must meet the basic requirements. A concern expressed by healthcare providers is the cost of addressing all or some of the standard, especially when compliance requirements are vague.

The security standard mandates safeguards for physical storage and maintenance, transmission, and access to individual health information. The standard also requires safeguards, such as encryption for Internet use as well as security mechanisms to guard against unauthorized access to data transmitted over a network.

INTERNET INSECURITY

A hacker called “Kane” managed to download admission records for four thousand heart patients in June/July 2000. (Security Focus, December 6, 2000)

The recent incident at the University of Washington Medical Center highlights the sensitivity as well as the vulnerability of health care data systems connected to the Internet to outside threats. A hacker called “Kane” managed to download admission records for four thousand heart patients in June/July 2000. The hospital would have faced stiff penalties if HIPAA had been enforced.

The risks to a healthcare provider of inadequate computer security include harm to a patient, liability of leaked information, loss of reputation and market share, and fostering public mistrust of the technology. Access to health information must be based on certain “roles” such as primary care physician, nurse, pharmacist or administrator.

Threats to health information security and privacy include:

- Intentional Misuse from Internal Personnel,
- Malicious or Criminal Misuse from Internal personnel,
- Unauthorized Physical Intrusion of the Data System by an External Person, and
- Unauthorized Intrusion of the Data System by an External Person via Information Networks.

HIPAA provides a “common sense” approach to implementing recommended and required security procedures. But according to DHHS, it is a recommended technology-neutral “floor” of security procedures and controls, and it does not provide explicit security standards for Internet use. The list of tools and techniques to protect Web-applications include authentication, encryption, smart cards or secure identification cards, and digital signatures.

HIPAA mandates that security standards must be applied to preserve health information confidentiality and privacy in four main areas (Table 1):

- Administrative Procedures: (personnel procedures, etc.)
- Physical Safeguards: (e.g., locks, etc.)
- Technical Security Services: To protect data at rest.
- Technical Security Mechanisms: To protect data in transit.

Authentication

Though HIPAA is about much more than information security procedures, complying with security and privacy regulations will be challenging to many healthcare organizations. Problem areas include the ease in compromising the front line security (i.e., usernames and passwords), which can result in easy interception of private data--not to mention hackers who can easily impersonate the intended user. For instance, it is not uncommon in a typical hospital to find passwords on notes stuck around computer systems. In addition, data integrity and cyber-terrorism are real threats as are the tremendous propagation of new and nasty computer viruses.

Authentication is the first line of protection to ensure secure access and communication of sensitive information or e-commerce transactions. Without properly verifying a user’s identity, all other security measures – authorization policies, data cryptography, secure session trusts – have limited benefits. The most reliable method of authenticating people is by using biometrics, the science of measuring physical characteristics or personal behavioral traits. With biometrics, a user’s identity becomes their password (i.e., the individual is authenticated not the machine). Biometrics avoids the common problem of passwords that have not been changed or have been shared among many users.

In terms of comparing various authentication mechanisms (e.g., hardware tokens, digital certificates, biometrics, secure ID passwords, and single passwords) perception of the relative cost and benefits varies widely by level of security. A common perception is that passwords are affordable and everything else is “high-tech” and therefore expensive. Tokens, PKI, and biometrics all can provide stronger authentication than simply a re-usable password. While PKI provides substantial authentication and cryptography protection for machines and data, it does not verify the identity of the end-user attempting to access such information. Likewise, while other forms of authentication provide certain advantages if used individually, they do not fully protect against the onslaught of new hacking techniques.

HIPAA requires the transmission of health-related information to include adequate encryption, authentication or identification of communication partners, and incorporate an effective password/key management system. Authentication is accomplished over the Internet and means proving who you are, which may involve one or more of the following factors: something you are; something you know; or something you have.

- ✓ One Factor: Something you know (eg., user name and password).
- ✓ Two Factor: Something you have (e.g., hardware authentication), and
- ✓ Three Factor: Something you are (biometric identifier such as a biologic or physical characteristic).

DUE DILIGENCE FOR HIPAA COMPLIANCE

A due diligence is expected of any business sharing health information and especially using the Web as a communication medium. HIPAA requires that the policies be recorded and audited for compliance. Vendors or outsourcing companies will be required to sign a Chain of Trust or business partner agreement. It protects the health care organization by assuring the vendor or subcontractor is complying with the requirements of HIPAA.

We recommend a business impact analysis and an assessment to determine compliance with HIPAA.

1. **Baseline Assessment:** The baseline assessment inventories an organization’s current security environment with respect to policies, processes and technology. This should include a thorough assessment of information systems that store, transact or process patient data.
2. **Gap Analysis:** The goal of the Gap Analysis is to compare the current environment with the proposed regulatory one in terms of level of readiness and the determine whether and how large the “Gaps” are. This should include a detailed listing of HIPAA security requirements, and those areas the organization and their *business partners* meets or fails to meet.

3. Risk Assessment: The risk assessment should address the areas identified in the Gap analysis requiring remediation. A risk assessment should provide an analysis of both likely and unlikely scenarios in terms of probability of occurrence and their impact on the organization. *It is impossible to foresee every possible scenario but you must provide contingency planning.*

SOME SAMPLE SECURITY QUESTIONS TO ASK VENDORS

No technology alone will insure HIPAA compliance. However HIPAA will certainly require even small provider organizations (e.g. medical groups, small hospitals, long-term care facilities, etc.) to utilize some measure of technology to comply with HIPAA. To narrow the vendor selection process, some important questions include the following:

- ✓ Is the vendor familiar with HIPAA and understand the standards and requirements?
- ✓ Does the vendor provide any enhanced security features to comply with HIPAA?
- ✓ What type of access controls can be enabled (by role or user)?
- ✓ For Internet applications, what level of encryption is used?

CONCLUSION

In the era of managed care and thin financial margins, the competitiveness of providers may depend on the use of information technology to streamline clinical and other business operations. Nevertheless, increased computerization of medical information requires increased surveillance of policies and procedures to protect the confidentiality of private medical data. Failure to develop, implement, audit, and document information security procedures could result in serious consequences, such as penalties and loss of reputation, market share, and patient trust. It is recommended that providers learn more about HIPAA through publications, seminars, and related web sites.

Table 1: HIPAA Security Matrix
 From Proposed Rule Originally Published August 1998

A. Administrative Procedures to Guard Data Integrity, Confidentiality and Availability.

HIPAA Requirement	Implementation
Certification	<i>See footnote</i>
Chain of trust partner agreement	<i>See footnote</i>
Contingency plan (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Applications and data criticality analysis. • Data backup plan. • Disaster recovery plan. • Emergency mode operation plan. • Testing and revision.
Formal mechanism for processing records.	<i>See footnote</i>
Information Access Control (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Access authorization. • Access establishment. • Access modification.
Internal audit	<i>See footnote</i>
Personnel security (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Assure supervision of maintenance. • Maintenance of record of access authorizations. • Operating, and in some cases, maintenance personnel have proper access authorization. • Personnel clearance procedure. • Personnel security policy/procedure. • System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Documentation. • Hardware/software installation & maintenance review and testing for security features. • Inventory. • Security Testing. • Virus checking.
Security incident procedures (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Report procedures. • Response procedures.
Security management process (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Risk analysis. • Risk management. • Sanction policy. • Security policy.

Termination procedures (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Combination locks changed. • Removal from access lists. • Removal of user account(s). • Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Awareness training for all personnel (including mgmt). • Periodic security reminders. • User education concerning virus protection. • User education in importance of monitoring log in success/failure, and how to report discrepancies. • User education in password management.

B. Physical Safeguards To Guard Data Integrity, Confidentiality and Availability

HIPAA Requirement	Implementation
Assigned security responsibility	<i>See footnote</i>
Media controls (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Access control. • Accountability (tracking mechanism). • Data backup. • Data storage. • Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	<ul style="list-style-type: none"> • Disaster recovery. • Emergency mode operation. • Equipment control (into and out of site). • Facility security plan. • Procedures for verifying access authorizations prior to physical access. • Maintenance records. • Need-to-know procedures for personnel access. • Sign-in for visitors and escort, if appropriate. • Testing and revision.
Policy/guideline on work station use	<i>See footnote</i>
Secure work station location	<i>See footnote</i>
Security awareness training	<i>See footnote</i>

C. Technical Security Services to Guard Data integrity, Confidentiality and Availability

HIPAA Requirement	Implementation
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	<ul style="list-style-type: none"> • Context-based access. • Encryption. • Procedure for emergency access. • Role-based access. • User-based access.
Audit controls	<i>See footnote</i>
Authorization control (At least one of the listed implementation features must be implemented).	<ul style="list-style-type: none"> • Role-based access. • User-based access.
Data Authentication	<i>See footnote</i>
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	<ul style="list-style-type: none"> • Automatic logoff. • Biometric. • Password. • PIN. • Telephone callback. • Token. • Unique user identification.

D. Technical Security Mechanisms to Guard against Unauthorized Access to Data Transmitted over a Network.

HIPAA Requirement	Implementation
Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	<ul style="list-style-type: none"> • Access controls. • Alarm. • Audit trail. • Encryption. • Entity authentication. • Event reporting. • Integrity controls. • Message authentication.

Footnote

Intentionally left blank. DHHS (US Department of Health and Human Services) HIPAA security requirements of August 1998 provided a technology-neutral “floor” of security procedures and controls and did not provide explicit security standards for Internet use.