

REFERENCE 5

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

Shannah Koss, Program Manager, IBM Government and Healthcare

This white paper is for general informational purposes only and does not constitute advice by IBM as to any particular actual set of facts, nor does this white paper represent any undertaking by IBM to provide customers with legal advice. Instead, this white paper is designed only to get customers started in understanding the *Health Insurance Portability and Accountability Act (HIPAA) Security Standards*. Therefore, IBM encourages customers to seek competent legal counsel for advice. Note that there is no established schedule for updating this white paper, and IBM is not responsible for the content or frequency of updates.

HIPAA Security Standards

Introduction

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. Whether we like it or not, these changes are inevitable. This paper provides some background information about the emerging Federal requirements, industry implications, and the actions that will be required.

Background

Why focus on Healthcare Security now? The regulatory climate and the increasing use of the Internet

The Health Insurance Portability and Accountability Act (HIPAA), perhaps better known as the Kennedy Kassebaum bill, was passed on August 21, 1996. HIPAA contained a section called Administrative Simplification, which was:

“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 manually on paper.”

The Administrative Simplification provisions of HIPAA call for: 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.

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. The purpose section, the security subsection, and the wrongful disclosure penalty section of HIPAA are contained in Appendix A.

The Health Care Financing Administration (HCFA), 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 and technical mechanisms — to guard data integrity, confidentiality and availability. 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.

The core requirements are as follows:

Certification	Media controls
Chain of trust partner agreement	Physical access controls
Contingency plan	Policy/guideline on work station use
Formal mechanism for processing records	Secure work station location
Information access control	Security awareness training
Internal audit	Access control (context based)
Personnel security	Audit controls
Security incident procedures	Authorization control
Security configuration management	Data authentication
Termination procedures	Entity authentication
Training	Communication network controls
Assigned security responsibilities	Digital signature

In the current documents, all requirements, except 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, 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. The public comment period ended October 13, 1998. Final rules had a statutory deadline of February 21, 1998, 18 months after the law was passed, the agency has let the time frame slip, but it appears we could have final rules by mid to late 1999. Depending upon their size, plans and providers will have 2 or 3 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; however, the proposed rules did not include any distinct treatment with respect to the compliance time frame.

The HIPAA statute 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. For “a person who knowingly” discloses individually identifiable health information, however, 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.

Coincidental to the changing regulatory environment, the healthcare industry is moving toward consumer and provider online exchange of information. The Internet and intranets are increasingly part of the healthcare IT environment. The use of the Internet in healthcare has heightened anxieties about inappropriate access to healthcare records. The preamble of the proposed rule states: “When using open networks some form of encryption should be employed.” Consequently use of the Internet warrants closer scrutiny of the security between internal and external networks.

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 patient's rights to confidentiality, and what constitutes inappropriate access to health records. Security establishes how the records should be protected from inappropriate access, in other words the means by which you ensure privacy and confidentiality.

HIPAA called for the Secretary of Health and Human Services to submit recommendations to Congress “on standards with respect to the privacy of individually identifiable health information.” Congress has until August 21, 1999 to pass privacy legislation pursuant to HIPAA, otherwise the Secretary shall issue final privacy rules by February 21, 2000. The Secretary's recommendations were submitted to Congress on September 11, 1997. They can be downloaded from the HHS website at <http://aspe.os.hhs.gov/admnsimp/pvcrec0.htm>. Several bills have been introduced in Congress; passage of a law may occur during the current Congress. In any case, it is likely there will be Federal privacy requirements by the year 2000.

Regardless of the timing for Federal privacy requirements, 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 in their information systems. Yet many organizations do not have written policies or procedures for their employees that are authorized to access the information, such as 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. This is not a criticism of the industry, but rather an observation. It describes the extension of information systems into areas that were once paper-based where there was less concern for security because people believed only authorized personnel had access. Automating paper records didn't naturally call for security that wasn't there in the first place. The fear that automated records will make inappropriate access easier for someone intent on gaining access is what has driven the industry to start developing comprehensive security programs.

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 the 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 10 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 as great an 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 healthcare organizations to determine the appropriate technical solutions on the basis of their risk analysis and the 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. Effective on November 24, 1998, the HCFA Internet Security Policy removes the prior ban on use of the Internet for transmitting Medicare beneficiary information. However, policy guidelines require that encryption and authentication or identification procedures be used for Internet transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information. These added requirements may tip the balance of the decision in favor of a private network.

As noted previously, HCFA indicated encryption should be employed for open networks. In addition, although digital signature is optional, it is viewed as one of the best means of authentication. Given the pressure on the healthcare industry to enable Internet access, particularly for consumers and practitioners, encryption and digital signature will be a significant technical requirement. Establishing sufficient public key infrastructure and certificate management services that can readily operate across all information technology platforms will be an industry

challenge. Interoperability pilots are being developed pursuant to the HCFA Internet policy to help address this challenge.

Another significant technical requirement may be 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 organization’s 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.

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 healthcare industry preference for controlling access by unauthorized users. The advantage of a biometric access control is that it can’t be lost, does not 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 isn’t authorized.

For now, time is on the side of those in the industry that see these requirements as just an additional burden that the government has placed upon the industry. Some, however, see this as an inevitable evolution of the information age if we want and expect people to carry out routine and critical business in a network environment. Given that we have two years from the time final rules are issued and the public comment period for the proposed rules recently ended, we can estimate an additional six months to start planning. If healthcare organizations start building security into their strategic planning, they should be able to comply with the requirements without the added expense of a last minute rush.

Next Steps

Depending upon the scope and complexity of the healthcare 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 organizational buy-in to security plans, policies and procedures suggests starting now.

Getting Started

First, assign at least one individual with primary responsibility for security. The person should probably be 100% dedicated, unless it is a very small organization. Although many organizations will tend to choose someone in their IT organization, think 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 individual health 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 standards to assess how significant an

undertaking compliance will be for the organization. Based on this assessment, determine whether the organization has the skills and resources to drive this effort internally or should seek external expertise. Compliance with the security standards has one noted similarity to Year 2000. Security skills and resources are scarce and demand will only increase as the compliance deadline approaches.

Whether the organization chooses to do it in-house or with the help of outside expertise, once a high level assessment of the gaps between the present security initiatives and the standards is completed, a recommended step would be the risk analysis — a required implementation feature of the proposed security management process standard which HCFA currently defines as:

“a process whereby cost-effective security/control measures may be selected by balancing the cost of various security/control measures against the losses that would be expected if these measures were not in place”.

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 only be through documentation that an organization can demonstrate it has addressed many of the requirements.

To be notified regarding the HIPAA implementing rules including the security standards send e-mail to: listserv@list.nih.gov with “HIPAA-REGS *your name*” in the body of the text and no other text or trailers.

For more information on the Administrative Simplification standards go to <http://aspe.os.dhhs.gov/adminsimp>.

Appendix A

"SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the Medicaid program under title XIX of such Act, and the efficiency and effectiveness of the healthcare system, by encouraging the development of a health information system through the establishment of standards and requirements for electronic transmission of certain health information.”

SEC. 1173. *****

“(D) SECURITY STANDARDS FOR HEALTH INFORMATION.—

(1) SECURITY STANDARDS.—The Secretary shall adopt security standards that—

(A) take into account—

(i) the technical capabilities of record systems used to maintain health information;

(ii) the costs of security measures;

(iii) the need for training persons who have access to health information;

- (iv) the value of audit trails in computerized record systems; and
 - (v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and
- (B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.
- (2) SAFEGUARDS.—Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—
- (A) to ensure the integrity and confidentiality of the information;
 - (B) to protect against any reasonably anticipated—
 - (i) threats or hazards to the security or integrity of the information; and
 - (ii) unauthorized uses or disclosures of the information; and
 - (C) otherwise to ensure compliance with this part by the officers and employees of such person.”

“Wrongful Disclosure of Individually Identifiable Health Information

SEC. 1177. (A) Offense. - a person who knowingly and in violation of this part-

- (1) Uses or causes to be used a unique health identifier;
 - (2) Obtains individually identifiable health information relating to an individual; or ,
 - (3) Discloses individually identifiable health information to another person, shall be punished as provided in subsection (B).
- (B) Penalties.- A person described in subsection (A) shall-
- (1) Be fined not more than \$50,000, imprisoned not more than 1 year, or both;
 - (2) If the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and
 - (3) If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.”