Implementing HIPAA Security Standards -- Are You Ready?

by Sandra Fuller, MA, RHIA (formerly RRA)

When the final security standards related to HIPAA are published later this year, the race to implement them will be on. Are you prepared? The author offers a handy set of guidelines.

The wait is almost over for the final security standards required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Final security standards are expected to be published in December of this year.

For organizations that have been waiting for "official" regulations before shoring up their information security programs, it's nearly time to begin. If, however, your organization has taken the opportunity provided by the original regulations to build an information security program, you're ahead of the game—and you're not alone. For example, at Group Health Cooperative (GHC) in Seattle, WA, plans are already in progress. "We've started now so that our directors can allocate sufficient resources for the 2000 budget," says William Thieleman, RRA, GHC health information administrator. "We'll need to do our in-depth assessment and work plan in 2000."

HIPAA is a landmark development for a number of reasons, not the least of which is that as healthcare played catch-up with other industries in the deployment of computer technology, it fell behind in information security. Driven by the need to transmit claims transaction data and set a security framework that would support transmission of even more information to support those claims, HIPAA-related proposed regulations sought to put healthcare on the right track. The regulations apply to all individual health information maintained or transmitted in electronic form. They do not apply to paper-based information.

What's more, the regulations required by HIPAA are a new breed of rules. The Department of Health and Human Services sought industry input on them from the beginning of development. The department held public forums, worked with the National Committee on Vital and Health Statistics, and brought together experts. The result: rules based not on what the government thought the industry should do, but on what the healthcare community knew should happen.

Regardless of what the final rules are (the best guess is that they won't dramatically depart from proposed rules), they will reflect a consensus of expert opinion. For most healthcare organizations, there is no better place to start to sort out information security issues. The regulations are technology neutral—meaning that they do not mandate what system, hardware, or software organizations use—and they address policy and accountability over technology. The best news is that even if you haven't started (or intended to start), you may already have completed at least the first few policies.

Information Security and Y2K

It's no surprise that the Y2K "bug"—which could render systems and data flawed or potentially inoperable—poses huge information security problems. A fortunate byproduct of the problem, however, is that in addressing the Y2K issue, organizations may have inadvertently begun developing an information security program.

Y2K is unique because organizations have had advanced warning about it, and they have had time to develop contingency plans. The information security regulations require contingency planning in three areas:

- applications and data criticality analysis
- data backup plan
- disaster recovery plan

- emergency mode operation plan
- testing and revision

To assess the Y2K risk, most healthcare organizations determined a methodology for identifying systems and data most crucial to their business. Critical systems for the direct delivery of care, life support, or vital environmental systems probably top that inventory. This methodology and the resulting prioritized list constitute an application and data criticality analysis—the first required policy under the proposed regulations. Done well, this policy should direct other information security efforts by identifying the data and applications most critical to the business.

The next required policy is a data backup plan. Driven by the inventory, documentation should be developed detailing frequency, extent, storage, and the responsible party. It should also explain how backups performed under tests, because even the best systems fail. The extent that failure inhibits the performance of the mission may rest on system backups working.

In addition to data backups, an emergency mode operation plan is required. This, too, may have been developed as an element of Y2K preparedness. An emergency mode operation plan should address how the enterprise would operate in the event of fire, vandalism, natural disaster, or system failure. Other questions to ask include:

- what systems are supported by emergency power, and how long does that power last?
- does a "hot site" (a replication of your critical systems in a remote location) exist, and how long does it take to bring it online?
- what hardware alternatives can be employed?
- is replication built into the network?
- can the vendor supply new hardware within hours, or will it take days?
- finally, what is the process for switching back to manual procedures? Are those procedures documented? Are staff aware of and trained in manual backup procedures? Do adequate resources exist for the staff to use during an emergency that requires manual operation?

Although information security can seem like an intangible issue, there are certain physical elements of a computer system that should be safeguarded by physical access control policies. Theft of a personal computer may be an annoyance, but it is likely to be less expensive then the value of the data stored on that computer. In addition, physical maintenance of hardware and the network should be performed and documented in a standardized manner. Questions to ask include:

- what precautions are taken for a physical disaster, (e.g., fire, flood, earthquake)?
- how will this physical type of emergency affect computer operations?
- what safeguards are in place to protect equipment from theft or vandalism?
- are special physical security procedures in place for computer rooms or network closets? Are these locked? Are a limited number of people given access?
- finally, are these physical precautions tested and are the results of these tests used to improve the security going forward? (This is another piece of the contingency plan and completes a cycle of activities that assure data integrity.)

Once a contingency plan is in place, there must be a documented process of periodic testing to identify weaknesses in that plan and its subsequent revision.

Beyond specific Y2K solutions, organizational processes developed to address Y2K may outlive January 1. At Group Health, "We plan to capitalize on our Y2K experience and organizational processes to address HIPAA," Thieleman says.

The Heart of It All: Record Processing

Recall that HIPAA was created to adopt national standards necessary for efficient electronic healthcare transactions. With electronic transactions at their core, it makes sense that record processing would play a significant role in the security standards. The regulations require that policies are in place to describe the processing of electronic records. These policies should address data receipt, manipulation, storage, dissemination, transmission, and disposal. Factors to consider include:

- how are electronic records handled? Who is responsible for the maintenance of electronic record systems? Are procedures in place to document receipt and transmission of electronic records?
- when records are transmitted, is there a record of the transmission?

Keep in mind that these regulations were drafted to first address the requirements of electronic transmission of billing data, but the policies adopted should apply to all of the electronic systems that handle individual health information.

A Matter of Authorization: Access Control

Up to this point, the required policies and procedures have dealt mostly with data integrity—making sure data and applications are secure from destruction or alteration. Next, the regulations turn to confidentiality and access.

Organizations that handle individual health information should have access control policies that govern appropriate access while assuring confidentiality. An access control policy includes the process in which authorization is granted and how and when it is modified. It should also determine the development of an access grid that clearly communicates which users have access to what elements of the system. Furthermore, the policy should include how other entities are granted access and how those privileges are modified or terminated. If your access system includes any enhanced features such as "breaking the glass" for emergency access or record lockout procedures, these also should be documented in your access control policy.

In addition, the access control policy should describe how access is technically maintained. Issues to consider are:

- are key cards, PINs or tokens used to authenticate users as part of access control?
- do menus limit access to applications?
- are employees educated as to which information, systems, and applications they can access to perform their jobs, and what their responsibilities are to limit their own access?

The access control policy also describes the authority to act within a system. For example, laboratory technicians may be authorized to update lab data, but the nursing staff may have view-only access. A policy should determine these authority levels. Frequently, access control is managed by an information security committee that can objectively weigh issues of security with access needs.

The user access system may be interfaced to an automated payroll system that can assist in establishing access, changing access when someone changes jobs, or in termination of access upon termination of employment. This interface may be electronic or can function through reports or e-mail notification forwarded to the security manager. Whatever the procedure for updating the access system, it should be documented in the policy. A record of security transactions that could verify granting, modification, and termination of privileges also should exist. This record should also reflect any individual's access at any point in time and should be maintained historically. If a security incident occurs, the trail would be useful in identifying who had access to which systems or functions at a given point in time.

A Watchful Eye: Internal Audit

Even the best security system will fail. With the amount of access to information required in healthcare, the extent of information available, and the diversity of users, it is essential that organizations continually audit system access. A policy to describe the internal audit procedures in the organization must be in place.

Who is responsible for performing audits? Audits must provide usable information, not mountains of data. The documentation of audits performed must be consistent with your audit policy and should provide information that supports action. Those actionable outcomes may take the form of training, technical enhancements, or disciplinary action, should be consistent with other personnel policies in the organization, and should be applied consistently throughout the organization.

Hello, Goodbye: Personnel Issues

Another facet of the security policies specified in the regulations includes personnel security. Personnel with access to health information should be supervised and trained in the appropriate use of that information. Either law or policy may require preemployment clearance checks of personnel employed by the organization. Documentation of these policies and demonstration that they are enforced should be maintained.

A personnel security policy should describe processes related to the termination of an employee, such as how access is denied including physical access (return of keys, key cards, tokens, or changing of combination locks to computer rooms). The policy should also identify the persons responsible for assuring that keys or cards are returned and should describe the procedure for logging the receipt of those items. Removal of an active user account on all systems must be done in a timely manner, and the expectations for the amount of time system access changes are made should be documented in the policy.

End of the Line: System Management

The security regulations require that a designated individual be responsible for an information security program. They do not, however, specify particular qualifications. Nevertheless, selecting a security manager may be one of the most important steps in complying with regulations and in building an effective security program. Look beyond technical expertise to someone with knowledge of information use and flow in the organization and understanding of the regulations pertaining to information security and confidentiality at both federal and state levels. A security manager should also be able to communicate with upper management to gain the necessary support for the program. He or she also must be comfortable drafting policy and working with a team of individuals throughout the organization in refining and implementing that policy. Perhaps most importantly, the manager should be prepared to lead the organizational effort based on respect for the value of information and confidentiality. (See "On the Job: Security Manager Position Description.")

The regulations also require a security management process that includes a risk analysis policy, a risk management policy, a sanction policy, and a general security policy. These more general strategies may be a starting point for some organizations, while others may come to their general philosophy by building from more specific policies. A review of existing confidentiality policies to support a paper-based system may be helpful in the development of these higher-level policies. Certainly, compliance with federal and state laws and the requirements of regulatory and accrediting body standards are key to the development of these policies.

Essential Elements: Hardware, Software, and Media

A policy covering the management of system configuration should be in place. This policy includes documentation of the entire system, specification for installation of new system elements, the entire inventory, and a description of the inventory management process, how system elements are tested prior to implementation, and how they are maintained, including virus-checking procedures. The network topography must be documented, including the scope of the system. This may be extremely useful where an organization's network is literally or functionally a piece of a larger network (one hospital in a chain or an academic medical center at a university). Describing the scope of the system clarifies the elements of the system for which the organization is responsible and where the policies apply.

A policy covering the receipt and removal of hardware, software, and data must exist. This is analogous to most facilities' current policies on removal of medical records. This policy should also spell out disposal procedures for hardware and data. Additionally, use policy should address the placement of workstations throughout the facility. For instance, what special precautions are taken with workstations located in high-traffic or public areas? Are automatic screen savers or application timeouts in place? Is staff trained in methods of concealing screen information from public view?

When the Worst Happens

Security incident procedures must be in place. These procedures define what events are reportable as an incident. The policy should explain who must report a security incident, how it should be reported, and to whom. The policy should also describe the appropriate response to an incident and how security incident reports are used to improve the overall security of the system.

More than Policies

Although the proposed regulations are heavily weighted toward the development, implementation, and documentation of policy, other requirements are also outlined. Training is required for all staff who have access to electronic information. That training should include both awareness training, highlighting the importance of confidentiality and information security to the organization, and job-specific training in information handling.

A number of the other requirements put in place the policies described above. The idea is that having a policy alone does not provide adequate protection, so the regulation spells out technical requirements in these additional areas:

- physical safeguards
- secure workstation location
- audit controls
- authorization controls
- technical security services
- technical security mechanisms for transmission

Sixty days after the final regulations are published, they have the weight of law, and most healthcare organizations have two years to comply. If no policies currently exist, they will need to be developed at the rate of more than one every 45 days. Consider how long it takes an organization to design a position description and fill a new position, or to alter someone's current position to take on the responsibility of information security. How ready is your organization? Can all of the staff with access to electronic information describe an information security incident? Furthermore, do they know what to do in response? Are the existing audit trails useful in identifying vulnerabilities or incidents of inappropriate access?

The Group Health Cooperative staff has begun developing a multi-year implementation plan. In 1999, they have educated leadership about HIPAA and its implications for their organization. They also have prepared a large-scale gap analysis to launch their planning and heighten awareness. Thieleman notes that healthcare organizations are just beginning to grasp the broader implications of HIPAA, including:

- implementing full access audit capability
- preparation to enforce policies
- retrofitting/replacing legacy applications to provide full access trail capability; many organizations have legacy systems that only track transactions, not read-only browsing
- developing the ability to create access trails for patients on demand; trailing access to paper records is also an issue
- developing authentication and encryption of internal and external electronic communications
- implementing electronic signature
- replacing multiple-application logon with a single quick logon to a user's tailored suite of applications to support accuracy of access trails

When all of these factors are taken into consideration, suddenly two years seems like a very short time. Come December, the clock will start ticking. Are you ready?

References

"HIPAA Security & Electronic Signature Standards—Glossary of Terms—Draft." Health Care Financing Administration, US Department of Health & Human Services. From "Steps Toward Compliance," jointly sponsored presentation, April 27, 1998.

"Are you Ready? Prepare Your Organization for HIPAA." AHIMA audio seminar, July 8, 1999.

Acknowledgements

Thanks to Kathleen Frawley, JD, MS, RRA, and William Theileman, RRA, for reviewing and participating in this article.

On the Job: Security Manager Position Description

Job title: Information security manager

Reports to: Director of health information management

General Purpose: The information security manager serves as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of patient, provider, employee, and business information in compliance with organization policies and standards.

Position Responsibilities:

- serve as an internal information security consultant to the organization
- document security policies and procedures created by the information security committee/council
- provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures
- initiate activities to create information security awareness within the organization
- perform information security risk assessments and act as an internal auditor
- serve as the security liaison to clinical administrative and behavioral systems as they integrate with their data users
- implement information security policies and procedures
- review all system-related security planning throughout the network and act as a liaison to information systems
- monitor compliance with information security policies and procedures, referring problems to the appropriate department manager
- coordinate the activities of the information security committee
- advise the organization with current information about information security technologies and issues
- monitor the access control systems to assure appropriate access levels are maintained
- prepare the disaster previous and recovery plan

Qualifications:

Baccalaureate degree in health information administration or related field; certification as an RRA or an ART; experience in project management

(Excerpted from *Security and Access: Guidelines for Managing Electronic Patient Information* by Sandra R. Fuller. Chicago: AHIMA, 1997. For ordering information, click here, then click on the Information Security link, or call (800) 335-5535.)

Sandra M. Fuller *is AHIMA's vice president of practice leadership. She can be reached at sfuller@ahima.org.*

Article citation:
Fuller, Sandra. "Implementing HIPAA Security Standards--Are You Ready?" *Journal of AHIMA* 70, no.9 (1999): 38-44.