Moving Toward a Unified Information Security Program

by Michael Ruano

Is your organization up to the challenge of creating a unified information security program?

A unified information security program has been all but mandated for healthcare organizations by the federal government. HIPAA requires that electronic, paper, and oral patient identifiable information be protected to a prescribed minimum level. This regulation also calls for the creation of formal responsibility for these protections.

Prior to this legislation, healthcare organizations protected information through various mechanisms and many separate departments. These departments commonly created and policed their own security standards in relative autonomy. Now, HIPAA provides the challenge of gathering up these parts into a single system for the management of information security. This article presents guidance to help your organization navigate this challenge.

Up to the Challenge

Each department (such as HIM, information management services, human resources, compliance, and others) has already created a section of what must be coordinated. One critical success factor is effective communication among different departments. By now, you should have already started the process of **pulling together all critical departments** and processes into one newly coordinated information security management process. This is no simple task, especially within a defined time frame.

There will be issues to resolve concerning guidelines, incident response, and sanctions. Much discussion is needed to create workable new processes, as departments will have already developed their own processes concerning these issues. All departments must participate in discussions to reach a consensus on these issues.

Necessary Guidelines

Guidelines will be required to set an organization's internal standards for incident response, sanctions, and many other day-to-day operations affected by the HIPAA regulations. To provide direction and define intent, **high-level guidelines should be developed before detailed procedures are developed.** This will allow the creation of focused and consistent policies and procedures for both incident response and sanctions.

Examples of the types of guidelines that will be required are **defining what information is within the organization** and **developing a categorization scheme** of its criticality to the organization. A definition of information security incidents and the response to these incidents according to information criticality levels is also needed. Based on high-level statements for these issues, the creation of appropriate and consistent policies and procedures becomes much easier to accomplish.

Preparing an Incident Response System

Information security incidents that involve computers, networks, and other technical aspects of the organization may already be reported through the information management services department and might be the easiest to discover and document. Incidents that involve employees and medical staff will usually be reported to the human resources department or medical staff office. In these situations, notification of other departments and managers outside of human resources or the medical staff office may be minimal.

Current communications mechanisms were most likely developed from existing need-to-know standards. The list of those with a need to know must now include those individuals named responsible for privacy and security as required by HIPAA. They may be reluctant at first to share information concerning personnel with other departments or areas, including the new information security function.

HIPAA requires a **formally documented process for incident response and damage mitigation**. This must include the notification of the privacy and security officers when an information security incident occurs. HIPAA requires the officers to be responsible for the management of personnel in relation to privacy and security mandates. At a minimum, this will mean the input from the security officer on the new incident process as well as routine reporting of incidents to them for auditing and process improvement. At the maximum, the security officer will be involved actively in the incident response process and may in fact act independently of other areas in these situations.

Sorting out Sanctions

Sanction policies and processes related to **information security incidents will need to be reviewed and made cross relational**, meaning they need to be consistent with HIPAA regulations, with existing and newly HIPAA-required organizational policy, and with each other. These new sanction policies and processes will need to be formally documented and applied consistently.

They will apply to all personnel as well as to external organizations that may have access to the covered entity's facilities, information processes and systems, and information. In certain instances, coordination with other departments may become necessary, as is the case with incident response processes. These instances will include the participation of the security officer in the guideline and process redesigns required to comply with the regulations. There will also be additional issues to resolve with the legal department and other areas that are responsible for contracts with business associates, as sanctions are also necessary in some of these situations.

The sanctions put in place may vary from what each organization has in place today. It will be imperative to make every effort to **educate all staff, business associates, and others regarding expectations of the organization regarding sanctions**. If successful, this education will probably be the best and most cost-effective method of reducing the likelihood of personnel-related information security incidents.

Communication Is Key

In response to HIPAA regulations, healthcare organizations are challenged to create a single view for the management of information security. The HIM department and others will have to resolve issues concerning guidelines, incident response, and sanctions. Only through effective communications can these issues be resolved within these short time frames.

Michael Ruano *(ruano@rhsnet.org) is information security officer for Rockford Health System in Rockford, IL.*

Article citation:
Ruano, Michael. "Moving Toward a Unified Information Security Program." *Journal of AHIMA* 74, no.1 (2003): 66, 68.