Updated Toolkit for Security Strategies

Save to myBoK

by Ted Cooper, MD

The first version of the Computer-based Patient Record Institute (CPRI) toolkit "Managing Information Security in Health Care" was published on the Web in May 1999 in response to the proposed HIPAA security and electronic signature standard of October 1998. The toolkit is intended to foster understanding of healthcare information privacy and security as well as provide guidelines and implementation tools that will aid healthcare organizations in reviewing the work of others, evaluating and implementing strategies around information systems, and measuring progress toward best practices.

Last December the Healthcare Information and Management Systems Society (HIMSS) published the fourth version of the CPRI toolkit. HIMSS continued this service as part of its electronic health record initiative when CPRI-HOST merged with HIMSS in 2002. A subcommittee of the HIMSS privacy and security task force oversees development of the toolkit, which is available at www.himss.org/asp/cpritoolkit_toolkit.asp.

What's New in the Toolkit?

In the new version, the work group updated each section and added a number of new ones. With the April 21, 2005, compliance date for the HIPAA security standard looming, the section "The HIPAA Final Security Rule in Plain English" will be of particular interest. The section includes an explanation of the general rules, each standard, and associated implementation specifications for HIPAA.

The standards and implementation specifications follow consecutively as found in the final rule. For each standard or implementation specification, the document provides the individual rule's identity, section number, title, compliance status, and the text of the rule in blue. Below this information, the document clearly explains the rule.

Security Function Guidance

Maintaining information privacy and security is the responsibility of all employees—not simply security specialists or information technologists. Healthcare organizations must ensure the confidentiality, integrity, and accessibility of their information as a matter of basic business practice in order to maintain the trust of patients, clinical and business partners, and the general public.

The toolkit guides organizations in achieving three basic security program functions:

- Monitoring changing laws, rules, and regulations
- Updating information security policies, procedures, and practices
- Enhancing patients' knowledge of their rights as well as the measures taken to protect them

These functions enable healthcare organizations to enhance their information privacy and security culture while subsequently building the foundations for a competent and defensible information assurance program. Organizations are encouraged to develop and maintain a security surveillance process that includes:

- Designating responsibility for information security management
- Developing and implementing a risk-management system to ensure confidentiality, integrity, and secure access to organizational information
- Evaluating the impact of administrative and technical countermeasures taken while executing an information security plan
- Modifying the plan periodically

Security surveillance is ongoing, and reevaluation should be viewed as a regular function of administrative operations. This type of broad-based approach builds administrative support and increases enterprise-wide awareness of the importance of information assurance. Both of these functions will be crucial in meeting the April 21, 2005, deadline for implementation of the HIPAA security regulations. This approach includes strategic health information security, which involves risk management, not avoidance. This method should facilitate HIPAA compliance as it enhances health information assurance for health-care organizations.

The CPRI toolkit suggests healthcare organizations focus on three security functions:

- Monitoring their federal, state, and professional regulatory and legal environment
- Updating their own internal environment of policies, procedures, and practices
- Communicating with their patients

As healthcare organizations work their way through the critical steps of the security surveillance process, they will find resources in the CPRI toolkit to achieve these steps. The resources come in several forms:

Function 1: Monitoring Laws, Regulations, Standards

Chapter 3 is devoted to the extensive HIPAA-induced federal activity in health information security and provides extensive materials about state and professional activities in health information assurance. Also included are summaries of all the HIPAA electronic transactions as well as privacy and data security regulations. A matrix provides links between the HIPAA requirements and pertinent sections of the CPRI toolkit. There is also a section on state law, which includes information on how to investigate legislative action in all 50 states.

Using the resources in this section of the CPRI toolkit, any healthcare organization can discover and track the various federal, state, and professional requirements in health information security and privacy to which they must comply. HIPAA gives this section special salience now; however, monitoring healthcare laws, regulations, and standards is an ongoing process for healthcare organizations.

Function 2: Updating Health Information Policies, Procedures, and Practices

Since 1993 the CPRI work group has published booklets on specific topics in health information security. Each booklet is reprinted in chapter 4 and is accompanied by samples and case studies illustrating the critical steps organizations should take to plan and implement a health information security program. Sample security policies illustrate how eight different health-care organizations addressed information security issues.

Section 4.5 contains an introduction to information security risk assessment as well as a case study on telemedicine. To learn more about assigning roles and responsibilities in health information security, consult section 4.4 and the guidelines for managing information security programs.

Information on enforcing security policies, sample confidentiality agreements, and a case study on securing user agreement is also available in the toolkit. A special section focuses on issues surrounding the electronic transmission of health information via e-mail, fax, and the Internet.

A discussion of patient-centered access to secure systems online—a project sponsored by the National Library of Medicine in order to give patients and providers secure remote access to computer-based patient records—is included as well. This section includes discussion of certain information security technologies such as firewalls and encryption.

Function 3: Enhancing Patient Understanding of Privacy and Security

Patients hold healthcare organizations accountable for many aspects of their business practice and medical care. The HIPAA privacy rule requires healthcare organizations to give patients the right to review and propose corrections to their medical record as well as document and permit patients to review lists of disclosures made for purposes other than treatment, payment, or healthcare operations. Chapter 5 includes procedures and forms illustrating how healthcare organizations might responsibly provide these services.

Institutionalizing sound security practices requires creating sustaining structures at all organizational levels. Security seminars routinely emphasize that CEOs need to publicly support information security programs, and confidentiality is every-body's business. However, questions about integrating information security into an organization's life are less frequent. Of particular concern is the tendency to isolate information security from clinical and business operations. Chapter 6 includes information on sharing responsibility for information security between information specialists, clinical users, and business users as well as a detailed discussion of the process and a sample agreement form.

Toolkit Best Practices

Available online, the CPRI toolkit functions both as an accessible guide to managing information security and a portal to additional resources. However, the toolkit should not be viewed as a simple method for HIPAA compliance or a foolproof security system. It does offer an extensive policy review, procedures, and practices. When used correctly, these policies, procedures, and practices offer the framework for a disciplined and defensible program.

No healthcare organization should rely on technology alone for a responsible security program. Each organization should develop its own combination of policies and procedures consistent with its mission and business philosophy. As with other industries, the nature of healthcare information security management requires controlling risks that will be unavoidable for the length of the business.

Risk management requires implementing sound judgment. The CPRI toolkit enables healthcare professionals to exercise competent administrative judgment in order to provide better patient care and protect their organizations.

Ted Cooper *(ted.cooper@sbcglobal.net) is a member of the HIMSS EHR steering committee and chair of the HIMSS privacy and security task force.*

Article citation:
Cooper, Ted. "An Updated Toolkit for Security Strategies." *Journal of AHIMA* 75, no.7 (July-August 2004): 42-43,55.