Practice Brief: Information Security-An Overview (Updated)
Editor's Note: The following information supplants information contained in the June 1996 "Information Security—An Overview" practice brief.

This practice brief provides an overview of information security, including some of the background and basic concepts involved in securing the privacy of health information. Included are key roles and responsibilities and a list of specific policies and procedures that should be considered when developing an organizational security program. References are included to assist readers in the actual development of a security program.

Background

Maintaining the security of health information used to be a fairly straightforward process. When most clinical information systems were introduced, they were implemented using limited-function workstations, physically attached to a designated processor, so end-users could be limited to specific applications. User access to protected health information generally could be prevented through the security administration available in most health information applications.

Today, powerful workstations are attached to networks on which multiple applications reside, and end users are just a password away from accessing a wide variety of information. Inappropriate access to information could occur if security is not closely monitored.

The increasing use of health information systems in both inpatient and outpatient settings and the linking of systems as the healthcare industry consolidates bring still more challenges. Information systems that once resided in a single facility are being expanded and integrated to simultaneously serve the needs of hospitals, home health agencies, long term care facilities, ambulatory care services, physicians, payers, employers, and others. System boundaries that historically were contained within the walls of an institution may now span multiple states or even nations.

Electronic health records (EHRs) offer the potential for maintaining health information on individuals across all care settings and throughout their lifetimes. With proper design and monitoring, EHRs can offer greater protection for protected information than paper-based patient records afford today.

The Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule approved in February 2003 establishes a baseline for securing health information for covered entities. However, there is flexibility for covered entities to choose security measures in accordance with their risks and operational needs.

Basic Concepts

Information security is undertaken to preserve the confidentiality, integrity, and availability of computer-based information. Security controls reduce the effects of security threats and vulnerabilities to a level acceptable to the organization. A major focus of information security is preventing unauthorized individuals from accessing, creating, or modifying information.

Risk assessment is the identification of information resources, the threats to those resources, and the vulnerabilities that may be exploited by those threats, thus exposing the resources to a loss of confidentiality, integrity, or availability.

Risk analysis is the formal process of examining potential threats and identified vulnerabilities discovered during the risk assessment and prioritizing those risks based upon probability and impact. A risk analysis includes a cost and benefit comparison to justify and determine appropriate security controls. Risks may be mitigated, transferred, or accepted, depending upon which option is the most reasonable for the organization.

Risk management is the ongoing process of managing identified risks to an acceptable level by applying security controls and measures to maintain a predetermined level of risk. Security systems cannot withstand every possible threat, and therefore there is no such thing as absolute security. Instead, health information professionals must weigh risks to their systems against the criticality and confidentiality of the information they contain and focus on developing, implementing, and maintaining appropriate security controls.

Cost-effective security controls and safeguards appropriate to the level of risk should be implemented by covered entities. Good security measures do not have to be very expensive, and they should not affect system speed or performance or make legitimate access to systems a hassle. The HIPAA Security Rule clearly indicates that cost alone does not relieve a covered entity of the responsibility of applying appropriate security measures to their systems.

Separation of duties ensures that checks and balances are designedinto the system to limit the impact of any given end user. Roles and responsibilities should be divided so that a single end-user cannot subvert a critical process. This practice divides the tasks related to maintaining system security among different personnel such that no single individual could compromise system security.

Least privilege means users should be granted access to only the information and functions they need to do their jobs. Functions should be restricted according to the user's job duties. For example, many employees may need "read-only" access. If their jobs do not require them to enter, change, or delete information, copy files, or print reports, they should not be given those capabilities. This supports the 'minimum necessary' requirement of the HIPAA Privacy Rule.

Types of Controls

Broadly speaking, there are three types of controls used in information security: management controls, operational controls, and technical controls.

Management controls are issues that must be addressed by management in the organization's information security program. Generally, these issues focus on management of the information security program and the management of risk within the organization. Management controls include security policies, procedures, and plans that incorporate all applicable laws and regulations and meet the organization's needs.

Operational controls are implemented and executed by staff at all levels of an organization; sometimes consultants and vendors also are asked to do this work. Operational controls include contingency planning, user awareness and training, physical and environmental protections, computer support and operations, and management of security breaches.

Technical controls focus on controls that are executed by information systems. These controls include user identification and authentication, access control, audit trails, and cryptography.

Roles and Responsibilities

Ultimately, everyone who interacts with a computer system is responsible for its security, but several groups have specific responsibilities.

Executives and senior managers have the overall responsibility for the security of information. They also must provide the necessary resources and support for the program.

Information systems security professionals have the technical expertise and knowledge of options available to ensure security. They are responsible for implementing and maintaining information security.

Data owners must assist in determining the data's sensitivity and classification levels and should have an active role in designing access controls for their systems. They should be accountable for the accuracy of the information. Data Owners should also assist in designing audit systems for their systems, and they accept the risk for their systems in the organization's current configuration.

HIM professionals should be an integral part of their organization's information security program because of their expertise in confidentiality and legal and regulatory compliance. They must be knowledgeable about the management, operational, and technical controls required to appropriately secure systems and networks and should help determine access control privileges. HIM professionals may design or assist in designing access control and other security policies, standards, guidelines, and procedures. They may serve as privacy or security officers for the organization.

Security officers should provide regular reports to senior management on the effectiveness of the security controls based on periodic audits. Security officers should also ensure that the security policies and procedures comply with industry standards. The information security program may have designated staff, or it may be handled through a committee or department. An officer's duties include design, implementation, management, and review of security policies, standards, guidelines, and procedures.

System managers and administrators program, operate, and fix computer systems. They are responsible for implementing technical security measures.

Users include individuals who are authorized to access a system for their own use as well as those who use information from reports and those who input data into the system. Users are responsible for following established policies and procedures and for alerting managers, data owners, or security officers of security breaches.

Threats and Vulnerabilities

Threats are events that may cause significant damage to information systems and the sensitive information they contain. Threats may be malicious or accidental, but they can damage a system or cause loss of confidentiality, integrity, or availability.

Vulnerabilities are system weaknesses that can be exploited by a threat. Reducing system vulnerabilities can significantly reduce the risk and impact of threats to the system.

Threats to information security include but are not limited to:

a.. Physical problems: Losses may result from power failure (including outages, spikes, and brownouts), utility loss (such as power, air conditioning, or heating), water outages and leaks, sewer problems, fire, flood, earthquakes, storms, civil unrest, or strikes.

b.. Disgruntled employees: The greatest risk of sabotage to computer systems comes from an organization's own employees and former employees. Sabotage may include destroying hardware or facilities, planting "logic bombs" that destroy programs or data, entering data incorrectly, crashing systems, deleting data, and changing data. Because of this threat, it is critical that system access and passwords be deleted immediately when an employee resigns or is discharged.

c.. Malicious code: Malicious code can attack both personal computers and more sophisticated systems. It includes viruses, worms, Trojan horses, logic bombs, and other software. Malicious code programs may play harmless pranks, such as displaying unwanted phrases or graphics, or create serious problems by destroying or altering data or crashing systems. The increasing use of corporate networks, electronic mail, and the Internet provides fertile ground for the development of new strains of viruses and other malicious code. It is critical that antiviral software be kept up to date.

d.. Hackers: Hackers are individuals who gain illegal entry into a computer system, often without malicious intent but simply to see if they can do it. While insiders constitute the greatest threat to information security, the hacker problem is serious. Other terms sometimes used in this context are "crackers" and "attackers." Actions taken by hackers, crackers, and attackers may be limited to simply browsing through information in a system or may extend to stealing, altering, or destroying information. Systems accessible via modem are particularly vulnerable to hacker activity.

e.. Theft: Desktop and laptop computers and the data they contain are vulnerable to theft from inside or outside the organization. The increasing use of personal digital assistants and other handheld devices makes potential inappropriate

access to protected health information a greater threat. Measures must be implemented to ensure that patient and corporate data are protected if devices are stolen or misplaced by users.

f.. Errors and omissions: End users, data entry clerks, system operators, and programmers may make unintentional errors that contribute to security problems by creating vulnerabilities, crashing systems, or compromising data integrity.

g.. Browsing: Legitimate users may sometimes attempt to access information they do not need to do their jobs simply to satisfy their curiosity. Extremely sensitive information such as human immunodeficiency virus test results may be vulnerable to this threat if not adequately protected in system or security design.

Establishing Security Policies

Information security policies are required for every organization and form the basis for an information security program. To be effective, policies must be issued at the highest level of the organization and apply to all units of the organization. Security policies should apply to all members of the workforce, including medical staff, volunteers, students, independent contractors, and vendors. Organizations must issue security policies to:

a.. Create its information security program and assign responsibility for it

b.. Outline its approach to information security

c.. Address specific issues of concern to the organization

d.. Outline decisions for managing a particular system

The table below is not meant to be exhaustive but to identify some specific issues which should be addressed when developing organizational and departmental policies and procedures. Multiple issues may be included in a single policy or procedure if appropriate.

Access controls
Acquisition of software
Acquisition of hardware
Anti-viral software use
Audit controls, trails, and system logs
Audit procedures to avoid discrimination
Audit trail retention
Back-up, archive, and restore procedures
Bringing in software, diskettes, or other media from outside the organization
Business associates
Change management
Configuration management
Contingency plan
Dictation and transcription systems
Disaster recovery
Disposal of media (including disks, hard drives, computers, and printed reports)
Electronic data interchange
Encryption of files and electronic mail
Facility security plans

Firewalls
Home use of organization hardware or software (such as telecommuting)
Internet access
Malicious code Media reuse
Passwords and other access authentication measures
Personal digital assistants
Privacy rights (including patients, families, caregivers, employees, and research)
Protection of confidential and proprietary information
Remote access to information systems
Retention, archiving, and destruction of electronic and paper-based information
Risk analysis
Sanctions and penalties for violations of privacy and confidentiality
Security incident reporting and response
Staff responsibility for data accuracy and integrity
Termination procedures
Training and awareness
Use and monitoring of security alarms
Use of electronic mail (including the level of privacy users may expect)
Unauthorized software
Vendor access to information systems
Workforce security
Workstation use and security
Conclusion

Organizational policies and procedures regarding security must be reasonable, cost effective, and appropriate to the risks identified through the risk assessment and analysis process. Keep in mind that good security does not have to be very expensive, nor should it hinder business operations. In fact, security practices may be implemented in a way that enhances business operations. The references included below are a valuable source of additional information on this subject.

References

An Introduction to Computer Security: The NIST Handbook. Washington, DC: National Institute of Standards and Technology, 1994.

"Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems." Schaumburg, IL: Computer-based Patient Record Institute, 1995.

"Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Record Systems." Schaumburg, IL: Computer-based Patient Record Institute, 1995.

"Health Insurance Reform: Security Standards." Final Rule. 45 CFR Parts 160, 162, 164. Federal Register 68, no. 34 (February 20, 2003). Available at www.hhs.gov/ocr/hipaa.

Krutz, Ronald L., and Russell Dean Vines. The CISSP Prep Guide: Gold Edition. Wiley Publishing, 2003.

Margret\A Consulting, LLC. "Maps of Final Security Rule to Proposed Rule: Final Security Rule to NPRM and NPRM to Final Security Rule." Copyright 2003. Unpublished.

Rada, Roy. HIPAA @ IT Reference, 2003: Health Information Transactions, Privacy, and Security. Hypermedia Solutions Limited, 2003.

"Standards for Privacy of Individually Identifiable Health Information." Final Rule. 45 CFR Parts 160 and 164. Federal Register 65, no. 250 (December 28, 2000). Available at www.hhs.gov/ocr/hipaa.

"Take Four Steps to Address 'Addressable' Implementation Specifications." HIPAA Security Compliance Insider, April 2003. Brownstone Publishers.

Updated by:

Carol Ann Quinsey, RHIA

Originally Prepared by:

Mary D. Brandt, MBA, RRA, CHE, Professional Practice Division

Acknowledgments

Assistance from the following individuals is gratefully acknowledged:
Margret Amatayakul, RHIA, CHPS, FHIMSS
Beth Hjort, RHIA, CHP
Gwen Hughes, RHIA, CHP
Don Mon, PhD
Carole Okamoto, MBA, RHIA
Harry Rhodes, MBA, RHIA, CHP
Tom Walsh, CISSP

Issued: June 1996
Updated: August 2003

Source: Quinsey, Carol Ann, and Mary D. Brandt. "AHIMA Practice Brief: Information Security--an Overview" (Updated November 2003)
