Information Security: an Overview

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Background

Maintaining the security of health information used to be a fairly straightforward process. The limited accessibility of paper-based records made them relatively secure from widespread disclosure. Most electronic information systems used limited-function workstations physically attached to a designated processor, so end users could be limited to specific applications. User access to unauthorized data generally could be prevented through the security of a particular application.

But this is no longer the case. With more powerful workstations attached to networks on which various applications reside, end users are just a password away from accessing a wide variety of information. The use of modems may make remote access by unauthorized users all but invisible, particularly if a system is not well monitored.

The increasing use of computers to store detailed health information in both inpatient and outpatient settings and the linking of information systems as the healthcare industry consolidates bring still more challenges. Information systems that once resided in a single facility must be expanded and integrated to serve the needs of hospitals, home health agencies, long term care facilities, ambulatory care services, physicians, payers, employers, and others.

Computer-based patient records offer the potential for maintaining health information on individuals across all care settings and throughout their lifetimes. If these systems/networks are properly designed and monitored, they also can offer greater protection for sensitive information than paper-based patient records.

Information security is the protection of the integrity, availability, and confidentiality of computer-based information and the resources used to enter, store, process, and communicate it.[1] A major focus of information security, especially in systems with many users or access through communication lines, is to prevent individuals from accessing, creating, or modifying information they are not authorized to access.

Basic Tenets

There are several basic tenets healthcare information security programs should follow:

Risk management: Information security helps to manage risk, but it does not eliminate it. There is no such thing as absolute security. No security system in general use today can withstand every possible threat. Instead, health information professionals must weigh threats to their systems against the confidential information they contain and focus on developing, implementing, and maintaining an acceptable level of security.

Cost-effective security measures: Only cost-effective security measures, appropriate for the level of risk, should be implemented. Security measures that go beyond this may be very expensive, affect system speed, or make access too inconvenient for legitimate users.

Separation of duties: Roles and responsibilities should be divided so that a single user cannot subvert a critical process. Checks and balances must be designed into the system to limit the impact of a single user.

Least privilege: 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, most employees 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.

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 techniques and concerns that must be addressed by management in the organization's information security program. Generally, they focus on management of the information security program and the management of risk within the organization. Management controls include security policies that incorporate all applicable laws and regulations and are designed to meet the organization's needs.

Operational controls are implemented and executed by people. They include contingency planning, user awareness and training, physical and environmental protections, computer support and operations, and handling of security breaches.

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

Who's Responsible?

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

Executives and senior managers must establish an organization's information security program and policies. They also must provide the necessary resources and support for the program.

Functional managers are responsible for the management, operational, and technical controls of their systems. This includes implementing appropriate security controls in their areas of responsibility. The chief information officer is responsible for ensuring that systems include appropriate controls to comply with the organization's information security program.

Because of their expertise in confidentiality and legal and regulatory compliance, health information management professionals should be an integral part of their organization's information security program. They must be knowledgeable about the management, operational, and technical controls required to appropriately secure their systems/networks and help determine levels of access for all users.

The *information security coordinator* (and support staff) directs the day-to-day management of the organization's information security program. How this responsibility is handled may vary from organization to organization. The information security program may have designated staff or be handled through a committee or department.

Systems management/system ad-ministrators program, operate, and fix computer systems. They are responsible for implementing technical security measures.

Support functions for information security include auditors, physical security officers, disaster recovery staff, quality officers, procurement (or purchasing), trainers, human resources, risk management, and physical plant.

Users include people who use the system directly, as well as those who use information from reports and those who input information into the system. Users are responsible for consistently following established policy/procedure and letting the functional manager/ application owner know what their needs are for protecting information.

Common Threats

Computer systems are vulnerable to many threats, which can cause significant damage to the systems and the sensitive information they contain. Analyzing potential threats and a system's vulnerabilities is usually done when conducting a risk analysis. This process is fundamental to applying cost-effective security measures. Information security is not absolute, but healthcare systems should be designed with a high level of security to protect sensitive patient information.

Threats to information security include but are not limited to:

Physical problems: Losses may result from power failure (including outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes. More loss is associated with fires and floods than with computer viruses and other more publicized threats.

Disgruntled employees: The greatest risk of sabotage to computer systems comes from disgruntled employees. Such sabotage may include destroying hardware or facilities, planting logic bombs that destroy programs or data if the employee's name is removed from the personnel list, entering data incorrectly, "crashing" systems, deleting data, holding data hostage, and changing data. Because of this, it is important that passwords be deleted immediately when an employee resigns or is discharged.*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 data or crashing systems. The increasing use of corporate networks, electronic mail, software agents, and the Internet provide fertile ground for the development of new strains of viruses and other malicious code, outpacing the ability of antiviral software programs.

Hackers: Hackers, sometimes called crackers, are persons who gain illegal entrance into a computer system. Insiders constitute the greatest threat to information security, but the hacker problem is serious. Actions taken by hackers vary from simply browsing through the information in a system to stealing, altering, or destroying information. Systems that may be accessed via modem are particularly vulnerable to hacker activity.

Theft: Desktop and laptop computers and the data they contain are especially vulnerable to theft from inside or outside the organization.

Errors and omissions: 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.

Browsing: Legitimate users sometimes may attempt to access information they do not need just to satisfy their curiosity. Extremely sensitive information like human immunodeficiency virus (HIV) test results may be vulnerable to this if not adequately protected in the system's design.

Establishing Security Policies

Information security policies are required for every organization, and they 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 employees, medical staff members, volunteers, students, independent contractors, and agents. An organization will need to issue security policies to:

- Create its information security program and assign responsibility for it
- Outline its approach to information security
- Address specific issues of concern to the organization
- Outline decisions for managing a particular system

Specific issues to be addressed may include:

Access controls (including system logs or audit trails)
Access to information (including levels of access and access to other employees' files)
Access to information by patients and their family members
Access to information by physicians and their office staff
Access to information for research
Acquisition of software
Acquisition of hardware
Anti-viral software use
Audit trails
Back-up procedures
Bringing in diskettes from outside the organization
Dictation and transcription of patient reports
Home use of organization hardware or software
Internet access
Malicious code
Passwords and other access control measures
Privacy rights (including patients, employees, and caregivers)
Protection of confidential/proprietary information
Remote access to information systems
Retention, archiving, and destruction of electronic and paper-based information
Security breaches
Staff responsibility for data accuracy and integrity
Staff responsibility for data confidentiality and penalties for violation

Disaster recovery
Disposal of printed reports
Electronic data interchange
Encryption of files and electronic mail
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

Notes

[1] *An Introduction to Computer Security: The NIST Handbook*. Washington, DC: National Institute of Standards and Technology, 1994, p. 9.

References

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

CPRI Workgroup on Confidentiality, Privacy, and Security. *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems.* Schaumburg, IL: Computer-based Patient Record Institute, 1995.

CPRI Workgroup on Confidentiality, Privacy, and Security. *Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Record Systems*. Schaumburg, IL: Computer-based Patient Record Institute, 1995.

Endrijonas, Janet. *Data Security.* Rocklin, CA: Prima Publishing, 1995.Freedman, Alan. *The Computer Glossary.* New York: American Management Association, 1995.

LaFrance, Sara, Stan Krok, Richard Moore, and Robert Powell. "Security vs. Access: A New Health Care Dilemma." *Proceedings of the 1996 Annual HIMSS Conference*. Chicago, IL: Healthcare Information and Management Systems Society (1996): 1-9.

Wilke, John R. "How Scientists Stalk Crafty Computer Viruses." *The Wall Street Journal*, August 29, 1995: B1, B5.

Prepared by:

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

Acknowledgments

Assistance from the following individuals is gratefully acknowledged:
Kathleen Frawley JD, MS, RRA
Gwen Hughes, ART
Julie Kilchenstein, MBA, RRA
Deborah Kohn, MPH, RRA
Dale Miller
Mariann Ogilvie, RRA
Mary Payne, ART
Harry Rhodes, MBA, RRA
Kate Szilard, ART

Issued: June 1996