Information Security—An Overview (2010 update)

Save to myBoK

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

Editor's note: This update combines and replaces the November 2003 practice brief "Information Security-An Overview (Updated)" and the January 2000 practice brief "Information Security: A Checklist for Healthcare Professionals (Updated)."

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 and a checklist (see appendix A) also are provided 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 that were physically attached to a designated processor so end users could be limited to specific applications. User access to protected health information (PHI) 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 monitored closely. Functionalities such as computerized physician order entry have increased the risks to healthcare organizations, their systems, and their patients. For example, computerized physician order entry increases risk because orders can be carried out on patients without alerts and safety checks, which will ultimately impact patient safety.

The increasing number and use of health information systems across the spectrum of care settings, including inpatient, outpatient, and physician practice 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 serve the needs of hospitals, home health agencies, long-term care facilities, ambulatory care services, physicians, payers, employers, and others simultaneously. System boundaries that historically were contained within the walls of an institution may now span multiple states or even nations. The influence of health information exchanges including the Nationwide Health Information Network, an initiative for the exchange of healthcare information being developed under the auspices of the Office of the National Coordinator for Health Information Technology, bring additional challenges, such as the privacy and security of real-time ongoing PHI in transit.

Electronic health records offer the potential for maintaining health information about individuals across all care settings and throughout their lifetimes via longitudinal records. With proper design and monitoring, electronic health records can offer controls that provide greater safeguards for protected information than paper-based patient records afforded in the past. These safeguards include the ability to know who has viewed, modified, or accessed a specific record. Despite providing the potential for greater protection, there are also new risks to the data. If a breach of information occurs, the number of individuals affected could be much greater in an electronic world than in a paper-based one. The loss of vast amounts of information stored within a system can be costly to an organization in the event of a breach. In addition, the complexity of security controls and the sophistication of security threats make this a difficult task.

The HIPAA security rule established a baseline for securing health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act in the American Recovery and Reinvestment Act (ARRA) provides the most significant change to the healthcare privacy and security environment since the original HIPAA privacy and security rules. The HITECH Act expands the HIPAA security rule requirements to include business associates and their agents and

subcontractors. The regulations include enhanced criminal and civil penalties and more stringent breach notification requirements. However, there is flexibility for covered entities to choose security measures in accordance with their risks and operational needs. The need for risk analysis and risk management are basic steps all organizations must take. In addition, the stage 1 meaningful use measures states, "Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process." The need for risk analysis and risk management will continue to increase and are the foundation of any information security program.

Basic Concepts

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

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 on the probability and effect of those risks. A risk analysis may include a cost-benefit comparison to justify and determine appropriate security controls. Risks may be mitigated, transferred, researched, or accepted, depending on which option is the most reasonable for the organization. Researched decisions are typically temporary decisions that are used until additional information can be gathered about possible solutions, controls, or tools. Researched decisions should lead to a final risks strategy to mitigate, transfer, or accept the risks.

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, so 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. Good security measures do not have to be 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 its systems.

Separation of duties ensures that checks and balances are designed into the system to limit the effect of any given end user to control the entire process. 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/minimum necessary 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 restriction 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, cryptography (encryption), firewalls, intrusion detection and prevention systems, virus protection, access (port) point security, audit logging and reporting, and many other controls.

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.

Information security officers should provide regular reports to senior management about the effectiveness of the information security controls based on periodic audits. Information security officers also should ensure that the information 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, enforcement, and review of security policies, standards, guidelines, and procedures.

Application and system 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. Application and system owners also should assist in designing audit systems for their systems. They accept the risk for their systems in the organization's current configuration.

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. Users are responsible for following established policies and procedures and for alerting managers, data owners, or security officers of security breaches.

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 secure systems and networks appropriately 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.

Threats and Vulnerabilities

Threats are potential events or dangers that may cause damage or inappropriate access 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 reduce the risk and impact of threats to the system significantly.

Threats to information security include but are not limited to:

- **Authorized users:** The greatest number of security breaches involves authorized users who use information inappropriately, such as viewing records without a business need. Examples would include breaches of privacy or confidentiality or identity theft.
- **Theft or loss:** Desktop and laptop computers and the data they contain are vulnerable to theft and/or loss from inside and outside the organization. The increasing use of laptops, tablets, smartphones and other handheld devices, along with portable media such as external hard drives and USB thumb drives, makes potential inappropriate access to PHI a greater threat, especially if these devices lack encryption. Measures must be implemented to ensure that patient and corporate data are protected in the event devices are lost, stolen, or misplaced by users. Measures such as encryption and limiting USB usage are strongly recommended practices to enhance information security.
- **Disgruntled employees:** The greatest risk of sabotage to computer systems may come 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.
- **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, e-mail, and the Internet provides fertile ground for the development of new strains of viruses and other malicious code. It is critical that antiviral or antimalware software be kept up-to-date.
- **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. Although 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 remote access are particularly vulnerable to hacker activity.
- **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.
- **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.
- **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 must be promulgated, stakeholders must follow the policies, the policies must be monitored, and the policies must be enforced. A selective set of information security policies should apply to all members of the workforce, including medical staff, volunteers, students, independent contractors, and vendors. Policies must document clearly the procedures and expectations of all staff within an organization. They should not be confused with IT security procedures that provide greater detail and may change frequently.

Organizations must issue security policies to:

- Create their information security program and assign responsibility for it
- Outline their approach to information security
- Address specific issues of concern to the organization
- Outline decisions for managing a particular system
- Define sanctions
- Set expectations for all staff

The table below identifies some specific issues that should be addressed when developing organizational and departmental policies and procedures. It is not meant to be exhaustive. Multiple issues may be included in a single policy or procedure if appropriate. Many of the policies would be directed at the individuals responsible for the administration and support of information systems and could be assimilated into some type of information security manual.

Issues to Address in Organization/Department Policies and Procedures

Access controls Acquisition of hardware Acquisition of software Antiviral software use Audit controls, trails, and system logs Audit procedures to avoid discrimination Audit trail retention Backup, archive, and restore procedures Bringing in software, discs, 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 Laptops, smartphones, and mobile devices 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 Unauthorized software Use and monitoring of security alarms Use of electronic mail (including the level of privacy users can expect) Vendor access to information systems Workforce security Workstation use and security

References

Cooper, Ted. "Managing Information Privacy & Security in Healthcare: CPRI Guidelines-Information Security Policies: Guidelines for Establishing Information Security Policies at Organizations with Computer-based Patient Record Systems." January 2007. Available online at www.himss.org/content/files/CPRIToolkit/version6/v7/D38_CPRI_Guidelines-Information_Security_Policies.pdf.

Healthcare Information and Management Systems Society Computer-based Patient Record Institute Work Group on Confidentiality, Privacy, and Security. "Managing Information Privacy & Security in Healthcare: Guidelines for Managing Information Security Policies at Organizations Using Computer-Based Patient Record Systems." January 2007. Available online at www.himss.org/content/files/CPRIToolkit/version6/v7/D42_Guidelines_Managing_Information_Security.pdf.

National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995. Available online at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

Krutz, Ronald L., and Russell Dean Vines. *The CISSP Prep Guide: Gold Edition*. Somerset, NJ: 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*. Rehovot, Israel: Hypermedia Solutions Limited, 2003.

"Take Four Steps to Address 'Addressable' Implementation Specifications." *HIPAA Security Compliance Insider*. New York: Brownstone Publishers, 2003.

US Department of Health and Human Services. "Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, no. 34 (Feb. 20, 2003). Available online at http://aspe.hhs.gov/admnsimp/final/fr03-8334.pdf.

US Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 65, no. 250 (Dec. 28, 2000). Available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2000_register&docid=page+82461-82510.pdf.

Prepared by

William M. Miaoulis, CISA, CISM

Acknowledgments

Angela K. Dinh, MHA, RHIA, CHPS
Margaret M. Foley, PhD, RHIA, CCS
Laurie Rinehart-Thompson, JD, RHIA, CHP
Margaret Schmidt, RHIA
Lou Ann Wiedemann, MS, RHIA, CPEHR, FAHIMA

Prepared by (original)

Mary D. Brandt, MBA, RRA, CHE (1996 original)
Carol Ann Quinsey, RHIA (2003 update)

Acknowledgments (original)

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

Appendix A

Information Security Checklist for Healthcare Professionals

The following list, although not exhaustive, outlines basic tenets of an information security program. Healthcare professionals may use this as a tool for evaluating their organization's information security program.

Access Control and Management

- Access control processes such as request, authorization, establishment, periodic review, and modification are addressed in policies and procedures.
- Access privileges are assigned based on a worker's role within the organization to ensure access is restricted to only the information needed to do the job.
- Access privileges based on roles are well documented and approved by management.
- Clinical applications have internal controls to limit the amount of patient information that the average user can print or download. Social Security numbers of patients are masked or not displayed to any worker who does not have a business need to see them.
- Password management rules (length, complexity, expiration, etc.) are consistent for applications and systems that process and store PHI. Exceptions to password rules are documented and approved by management.
- An individual's identity is verified before his or her password is reset. Wherever possible, avoid using or migrate away from using any part of an individual's Social Security number as an identifier for validating a user's identity to reset his or her password.
- Workers are logged off or locked out of a clinical application automatically after a predetermined period of inactivity, such as 10 minutes. This function triggers an event (audit) log entry that can be reviewed and reported.
- Access is removed or deactivated promptly when a user is terminated, resigns, or ends his or her affiliation with the organization and/or is disabled automatically after a predefined period of inactivity, such as 60 days. Ongoing monitoring of the termination process is used to verify that this process is being accomplished.
- Based on a report provided by the system administrator, managers periodically (at least annually) validate that worker access privileges are appropriate.
- Work with physician office managers on periodically reviewing user access privileges and roles to determine if access is appropriate; disable user accounts that have been inactive for long periods of time(e.g., 30 or more days). Management should review accounts that have been inactive for extended periods of time to determine if termination processes are not working effectively.
- Real patient identifiers are not used in test and training environments. If any test reports or temporary files use real patient identifiers, the files are deleted as soon as the testing or training is completed.
- IT personnel, including service (help) desk personnel, understand their responsibility for maintaining the confidentiality of patient information and cannot take control of a computer screen remotely without an individual's knowledge or permission.
- Appropriate mechanisms are in place to protect highly sensitive patient and employee health information, which may include information relating to HIV test results, lifestyle, substance abuse, psychological profiles, cosmetic surgery, or behavioral health records.
- Outside vendors and third parties can access only the information needed to perform their required service, and, wherever feasible, access to PHI or other confidential information is limited to read only.

Audit and Accountability

- Audit logs contain sufficient detail to verify which patient records were viewed or updated and by whom.
- The responsibility for reviewing audit logs has been assigned formally.
- Periodically, random audits of user activities are conducted to maintain a culture of accountability.
- Periodically, audits of particular activities are conducted to identify breaches of confidentiality; examples include, but not be limited to, VIPs, employees who are patients, audits of new employees, employees viewing records outside their area of responsibility (emergency room accesses), and when suspected activity occurs or a complaint has been filed.
- Ongoing audit log reviews are conducted for potential security breaches (such as failed log-in attempts) at the network, server, and application levels.
- Audit logs are secured and protected from unauthorized modifications so that only individuals with a job-related need can view the logs.
- Warning banners and/or other awareness methods are used to notify and remind workers that their activities are being audited and monitored.

Awareness and Training

- There are organizational records or documents demonstrating that information security awareness is being conducted. Annual refresher training is required. Issues involving individuals who have not completed their annual security

awareness training are brought to management.
- Security awareness is linked to user provisioning. Employees, temporary workers, contractors, and some vendors complete initial security awareness training before gaining access to PHI.
- Annually, management reviews and provides feedback for both the initial and the refresher security awareness training to ensure the content is current and addresses newly discovered threats or risks.
- All workers (employees and nonemployees such as students, volunteers, contractors, etc.) sign a confidentiality agreement.
- The organization's medical staff bylaws or rules outline physician responsibilities for protecting the confidentiality of health information.
- Staff members of physician offices with remote access are trained adequately on use of the clinical system and their responsibilities for protecting confidential information.
- Employees should be aware of the HITECH Act and HIPAA penalties and fines that could be levied on healthcare workers if they violate organizational policies and breach PHI with willful intent.

Business Associates and Other Nonemployees

- Business associate agreements have been updated as a result of the HITECH Act to include the new HIPAA security rule requirements, the new definition of breach, and the details for breach notification, including:
    - How to report
    - When to report
    - Who to report to
- Satisfactory assurances of compliance are obtained from business associates and any of their agents or subcontractors (chain of trust agreement).

Computer Workstation

- Policies and procedures are in place that outline workers' responsibilities for securing workstations, laptops, and other portable devices.
- Security practices include workers consistently logging off before leaving their work area. Screen savers are activated after a predetermined period of inactivity to prevent incidental disclosure of PHI.
- An accurate inventory is maintained for computer equipment (laptops, desktops, tapes, flash drives, etc.) and biomedical devices that store PHI. General security safeguards and controls also are implemented for biomedical devices storing PHI to maintain security consistency.

Contingency and Disaster Recovery Planning

- Information systems are backed up periodically, and the back-up data is maintained off-site in a secure location. The frequency of the back-up procedure is determined by the organization's needs.
- Information needed to treat patients is available at the bedside in the event of a loss of data-processing capabilities.
- Departments have their own documented contingency plan in place in the event of planned or unplanned downtimes of critical applications and systems.
- A formal business impact analysis is conducted to identify critical applications and data. The business impact analysis identifies the recovery point objective and recovery time objective for each of the critical applications and systems.
- The disaster recovery plan meets the recovery point objective and recovery time objective for the organization.
- There is documented evidence of a recent exercise or a test of the disaster recovery plan.

Incident Reporting and Response

- Employees are instructed how to detect and report known or suspected information incidents and privacy breaches.
- The organization has an incident response team, and its core members have received training, especially on collecting and handling evidence during an investigation.
- A tabletop exercise is conducted periodically to test incident response capability.

- The organization follows breach reporting requirements as specified under the HITECH Act and has an objective process in place for analyzing the potential risk of harm in the event of an incident.

Media Protection and Controls

- PHI stored on media, including back-up media, is encrypted in accordance with the National Institute of Standards and Technology's Special Publication 800-111, "Guide to Storage Encryption Technologies for End User Devices."
    - **Note**: Although encryption is addressable and not required, it is highly recommended to avoid breach notifications and lower enforcement penalties by exercising reasonable diligence for protecting PHI.
- Voice technology that is produced digitally from or stored on an information system is included in policies, safeguards, and controls used to protect electronic media.
- Policies and procedures addressing patient requests to obtain copies of their medical information in an electronic format include appropriate media controls to reduce risks.
- When printed reports containing confidential information are no longer needed, they are disposed of in a manner that protects their confidentiality (shredding, pulping, or burning).
- Hard disk drives are sanitized, meaning all confidential information is erased permanently from the drive, before being disposed of or reused. Documentation of destruction is maintained.

Mobile and Portable Device Security

- An accurate inventory of laptops, tablets, and other portable devices that store PHI is maintained.
- Steps have been taken to secure laptops, tablets, and mobile devices, such as smartphones and flash drives, including the following security controls:
    - Power-on password protection or biometric authentication to prevent unauthorized access in the event the device is lost or stolen
    - Automatic lockout set to enable after a predefined period of inactivity, such as 10 minutes
    - Encryption to protect data at rest
    - Automatic synchronization of stored data
    - Memory wipe to erase all data automatically either after a predetermined number of unsuccessful log-on attempts or when a remote wipe command is issued

Personnel Security Procedures

- Photo identification badges are used to distinguish employees and workforce members from contractors, sales representatives, and visitors.
- Procedures are documented for performing background investigations of workforce members, including some nonemployees working in key positions, before allowing access to PHI. The types of background checks performed are appropriate to a worker's level of access to PHI and other confidential information.
- Additional background checks may be conducted for individuals in trusted positions, such as a system administrator or network engineer.
- A reinvestigation process is conducted for positions identified as high risk.

Physical and Environmental Protection

- A facility security plan (also known as an *environment of care* plan) outlines the physical security procedures and controls for office buildings and addresses:
    - Access to restricted areas, such as the data center, network operations, and other areas where large volumes of PHI are stored in electronic or paper format
    - Equipment control into and out of the organization
    - Sign-in sheets for visitors to restricted access areas such as data centers
    - When and where visitors must be escorted

    - Maintenance records of changes or work performed on physical access controls (e.g., work on door locks, changing of combination door locks, etc.) that are related to security, which could be addressed by using copies of facility work orders
- Privacy and security walkthrough inspections are conducted and documented to ensure that PHI and electronic PHI are secured properly when not in use, to evaluate physical security controls, and to identify any issues or weaknesses in the implementation of the information security program.

Policies, Procedures, and Plans

- Information security policies are reviewed periodically by management to ensure that the policies are in line with accreditation standards and state and federal laws and that they are updated as needed.
- Tools may be used to manage and distribute policies and procedures centrally and to verify that workers have reviewed the policies that pertain to them.
- Periodic evaluations are conducted, either internally or by engaging a third party, to assess the effectiveness of policies and procedures and their compliance with the HIPAA security rule.

Remote Access

- Appropriate measures are in place to protect systems from unauthorized remote access.
- An automatic disconnect of a log-in session is enabled after a specific period of inactivity.
- Two-factor authentication may be used for remote connectivity, especially for anyone with system administrator privileges.

Risk Analysis and Management

- A well-defined risk assessment process is documented. The process is followed to identify threats and vulnerabilities and to present the results in a formal risk analysis report.
- Periodic risk analysis is conducted and covers systems and applications that store, process, or transmit PHI. Risk analysis is an ongoing process to evaluate which security controls are appropriate and should be accomplished whenever there is a significant change in the computing environment. The US Department of Health and Human Services released "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" in the summer of 2010, which states, "The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment."[1]
- Risk analysis reports (the findings and recommended corrective actions as a result of conducting a risk analysis) are reviewed and signed by management.
- The latest network vulnerability scanning and penetration test results are available for review. The risks associated with the discovered vulnerabilities are managed appropriately.

Transmission Security

- PHI and other confidential information being transmitted outside of the organization (via the Internet) are encrypted using a method that meets Federal Information Processing Standards 140-2.

    - **Note**: Although encryption is addressable and not required, it is highly recommended to avoid breach notifications and lower enforcement penalties by exercising reasonable diligence for protecting PHI.

- Outbound e-mail is scanned, and e-mails detected as containing sensitive and confidential information are encrypted automatically to protect them from unauthorized access, alteration, and disclosure.
- Wireless networks use Wi-Fi Protected Access (WPA2) encryption to secure transmissions from mobile devices such as laptops mounted on carts in clinical areas to the applications and systems within the internal network.

    - **Note**: As encryption technology continues to advance, WPA2 may be replaced in the future with stronger encryption standards when those are developed.

Note

1. US Department of Health and Human Services. "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." July 14, 2010. Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

Appendix Prepared by

Tom Walsh, CISSP

Appendix Acknowledgments

Angela K. Dinh, MHA, RHIA, CHPS
Margaret M. Foley, PhD, RHIA, CCS
Laurie Rinehart-Thompson, JD, RHIA, CHP
Margaret Schmidt, RHIA
Lou Ann Wiedemann, MS, RHIA, CPEHR, FAHIMA

Appendix Prepared by (original)

Mary D. Brandt, MBA, RHIA, CHE (1996 original)
Jennifer E. Carpenter, RHIA (2000 update)

Appendix Acknowledgments (original)

Donna Fletcher, MPA, RHIA
Sandy Fuller, MA, RHIA
Harry Rhodes, MBA, RHIA, CHP

Article citation:
AHIMA. "Information Security—An Overview (2010 update)." (Updated December 2010).

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.