Information Security—An Overview (2014 update)

Save to myBoK

Editor's note: This practice brief supersedes the December 2010 publication with the same name that combined and replaced two previously-published practice briefs: "Information Security—An Overview (Updated)" (November 2003) and "Information Security: A Checklist for Healthcare Professionals (Updated)" (January 2000).

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 as well as a list of specific policies and procedures that should be considered when developing an organizational security program. References, a checklist (see Appendix A), and assistance in developing policies and procedure (see Appendix B) are also provided to assist readers in the actual development of a security program.

Background

In the past, maintaining the security of health information was fairly straightforward. When most clinical information systems were introduced, they were implemented using limited-function workstations that were physically attached to a designated processor. This meant that end users were limited to specific applications. Unauthorized user access to protected health information (PHI) was generally prevented using the security administration available in most health information applications.

Today, powerful workstations are attached to networks on which multiple applications reside. End users are simply 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 (CPOE) 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.

Interoperability and consolidation make information security even more challenging. Information systems that once resided in a single facility are expanding and integrating with other systems to serve the needs of hospitals, home health agencies, long-term care facilities, ambulatory care services, physicians, payers, employers, and others simultaneously. System boundaries now span multiple states or even nations. The Nationwide Health Information Network (NwHIN), --an initiative developed by the Office of the National Coordinator for Health Information Technology (ONC), as well as other state and regional health information exchanges pose additional challenges related to the privacy and security of real-time PHI in transit.

Electronic health records (EHR) can potentially enable providers to maintain longitudinal records—i.e., health information about individuals across all care settings throughout their lifetimes. With proper design and monitoring, EHRs can provide greater safeguards for protected information that were essentially impossible when using paper-based patient records. These safeguards include the ability to determine any individuals who view, modify, or access a specific record. Despite providing the potential for greater protection, EHRs also pose new security risks to the data. If a breach of electronic information occurs, the number of individuals affected could be significant. The loss of vast amounts of information stored within a system can be costly to an organization. In addition, the complexity of security controls and the sophistication of security threats make this a difficult task.

The HIPAA security rule establishes 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 were published. First, the HITECH Act expands the HIPAA security rule requirements to include business associates and their agents and subcontractors. Second, the regulations include enhanced criminal and civil penalties as well as more stringent breach notification requirements. Covered entities have flexibility in choosing how to implement security measures in accordance with their unique risks and operational needs. All organizations must perform risk analysis and management. In addition, Meaningful Use, stage 1, 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 management will continue to grow and serve as the foundation of information security programs.

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 that is acceptable to the organization. Prevention of inappropriate access, creation, or modification of PHI is a major focus on information security. . The information maintained by an organization is an asset that it must be protect.

Risk assessment is the identification of information resources/assets, any threats to those resources/assets, and any vulnerability that may be exploited and subsequent exposed the resources/assets and result in a loss of confidentiality, integrity, or availability.

Risk analysis is the formal process of examining potential threats and vulnerabilities discovered during the risk assessment and prioritizing those risks based on the probability and potential effect of those risks to the organization and patient. 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 what option is most reasonable for the organization. Researching risks are typically temporary decisions that organizations use until additional information can be gathered about potential solutions, controls, or tools. This research should ultimately lead to a final risks strategy to mitigate, transfer, or accept the risks.

Risk management is the ongoing process of managing identified risks so they can be maintained at an acceptable level. The process includes application of security controls and measures to maintain a predetermined level of risk. Security systems cannot withstand every possible threat. Thus, organizations must not strive for absolute security. Instead, organizations must prioritize risk management according to the criticality and confidentiality of the information and focus on developing, implementing, and maintaining appropriate security controls.

Cost-effective security controls and safeguards are used to mitigate security risks to PHI. These controls and safeguards should be appropriate for each level of risk. . 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. Strong security measures do not necessarily require a significant financial investment. These measures should not significantly affect system speed or performance or make legitimate access to systems difficult.

Separation of duties ensures that checks and balances are incorporated into the system to disallow any given end user to control the entire process. Divide roles and responsibilities so that a single end user cannot subvert a critical process. This practice divides the tasks related to maintaining system security among different personnel so no single individual can compromise system security.

Least privilege/minimum necessary refers to the standard practice that users should be granted access to only the information and functions required to perform their jobs or assigned responsibilities. Functions should be restricted based on the user's job duties. For example, many employees may require read-only access. If individuals' roles do not require them to enter/change/delete information, copy files, or print reports, they should not be given the ability to do so. 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 those that generally 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 that meet the organization's unique needs. Management controls also include audit log monitoring and reporting to appropriate levels within the organization's management.

Operational controls are implemented and executed by staff at all levels of an organization. Consultants and vendors may also be required to implement and execute these types of controls. ; Operational controls include contingency planning, user

awareness and training, physical and environmental protections, computer support and operations, and management of security breaches.

Technical controls are executed by the members of the information systems department. 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 more.

Roles and Responsibilities

Ultimately, everyone who interacts with an information system [containing PHI] is responsible for the security of that PHI. However, several groups have specific responsibilities. These groups include the following:

Executives and senior managers. These individuals have the overall responsibility to secure PHI. They must also provide the necessary resources and visible support for the program.

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

Information security officers. These individuals should provide regular reports to senior management about the effectiveness of the information security controls based on periodic audits. Information security officers should also ensure that the information security policies and procedures comply with industry standards. The information security program may include designated staff, or the program may be handled via 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. These individuals must assist in determining the data's sensitivity and classification levels (roles based access) and should play an active role in designing system access controls for their systems. They should be accountable for the accuracy of the information. Application and system owners should also assist in designing audit systems and accept the risk for their systems in the organization's current configuration.

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

Users. These individuals include those who are authorized to access a system for their specific job role or assigned responsibilities. Users also include 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 and the Privacy Officer. These individuals are an integral part of their organization's information security program. They possess expertise in confidentiality as well as legal and regulatory compliance. They must be knowledgeable about the management, operational, and technical controls required to secure systems and networks appropriately. They should help determine access control privileges. HIM professionals may design or assist in designing access control and other security policies, standards, guidelines, and procedures.

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. 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, the following:

- **Authorized users:** The greatest number of security breaches involves authorized users who use information inappropriately, such as viewing records without a business need. Examples include breaches of privacy or confidentiality as well as identity theft.

- **Theft or loss:** Desktop and laptop computers, as well as 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 (i.e., external hard drives and USB thumb drives) makes potential inappropriate access to PHI a greater threat, **particularly if these devices lack encryption**. Measures must be implemented to ensure that patient and corporate data are protected in the event that 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 stem from an organization's own employees and former employees. Sabotage may include destruction of hardware or facilities, planting logic bombs that destroy programs or data, entering data incorrectly, crashing systems, deleting data, or changing data. System access and passwords must be deleted immediately when an employee resigns or is discharged. Possible solutions include working with HR to develop a process that ensures timely notification to Security Administrators of an employee's departure.
- **Malicious code:** Malicious code can attack both personal computers as well as 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 it may 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 it may extend to stealing, altering, or destroying information. Systems accessible via remote access are particularly vulnerable to hacker activity.
- **Physical and facility threats:** Losses may result from power failure (i.e., outages, spikes, and brownouts), utility loss (i.e., loss of 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. These errors create vulnerabilities, system crashes, and compromise data integrity.
- **Browsing:** Legitimate users may sometimes attempt to access information they do not need to do their jobs simply out of curiosity. For example, users may inappropriately access information about family members, co-workers, celebrities, or prominent citizens. 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

Every organization must implement information security policies. These policies 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, and all policies must be monitored and 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 specify the procedures and expectations of all staff within an organization. They should not be confused with IT security procedures that provide greater detail and that may change frequently.

Organizations must issue security policies to:

- Create and assign responsibility for the information security program
- Outline an 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

Refer to Appendix B for a list of specific issues that should be addressed when developing policies and procedures for security compliance.

References

AHIMA. “HIPAA Security Overview (Updated).” (Updated December 2013).

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.

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.

National Institute of Standards and Technology. “An Introduction to Computer Security: The NIST Handbook.” Special Publication 800-12. January 2013.

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

U.S. Department of Health and Human Services. “Health Insurance Reform: Security Standards; Final Rule.” *Federal Register* 68, no. 34 (Feb. 20, 2003).

U.S. Department of Health and Human Services. “Standards for Privacy of Individually Identifiable Health Information; Final Rule.” *Federal Register* 65, no. 250 (Dec. 28, 2000).

“Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.” 45 CFR Parts 160 and 164. *Federal Register* 78, no.17 (January 25, 2013)

Prepared by

William M. Miaoulis, CISA, CISM

Assisted by,

Tom Walsh, CISSP

Acknowledgments

Barbara Beckett, RHIT, CHPS
Becky Buegel, RHIA, CHP, CHC
Dana DeMasters, MN, RN, CHPS
Kathy Downing, MA, RHIA, CHPS, PMP
Brian Evans, CISSP, CISM, CISA, CGEIT
Elisa Gorton, RHIA, CHPS, MAHSM
Lesley Kadlec, MA, RHIA
Kelly McLendon, RHIA, CHPS
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA

Prepared by (2010)

William M. Miaoulis, CISA, CISM

Acknowledgments (2010)

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 outlines basic tenets of an information security program. Healthcare professionals may use this as a tool for evaluating their organization's information security program. Note: This is not a complete list.

Access Control and Management

- Ensure that policies and procedure address access control processes (e.g., request, authorization, establishment, periodic review, and modification).
- Assign access privileges based on a worker's role within the organization. This ensures that access is restricted to the information that the worker requires to perform his or her job.
- Clearly document role-based information access privileges and ensure that management or the data owner approves these privileges.
- Create security groups to ensure role-based access and privileges.
- Include internal controls within clinical applications to limit the amount of patient information that the average user can print or download. Ensure that Social Security numbers of patients are masked or do not display to any worker who does not have a business need to see them.
- Ensure that password management rules (e.g., length, complexity, expiration, etc.) are consistent across applications and systems that process and store PHI. Exceptions to password rules are documented and approved by management.
- Require an individual to verify his or her password before resetting it. Wherever possible, avoid using any part of an individual's Social Security number or birth date as an identifier for validating one's identity to reset a password. Use information that others would not be expected to know. A series of challenge questions is the best method. A security control could include notifying an individual via text message or personal email that his or her password had been reset. The notification should instruct the individual to contact the security office or his or her supervisor if the password reset was not requested.
- Ensure that users 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. Sanctions for continued inactivity may need to occur. Users should be trained to log off their system and not rely on inactivity timeout for compliance. When users leave terminals unattended, the terminals may be subject to hijack by another individual.
- Remove or deactivate access for users who are terminated, resign, or end their affiliation with the organization. Access should also be 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.
- Annually validate the appropriateness of worker access privileges based on a report provided by the system administrator and managers.

- Periodically review user access privileges and roles to determine whether 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 whether termination processes are working effectively.
- Refrain from using real patient identifiers in testing and training environments. Delete any test reports or temporary files that use real patient identifiers immediately after any testing or training using such reports or files is completed.
- Ensure that IT personnel, including service (help) desk personnel, understand their responsibilities for maintaining the confidentiality of patient information. These individuals cannot take control of a computer screen remotely without an individual's knowledge or permission.
- Implement appropriate mechanisms to protect highly sensitive patient and employee health information. Such information may include HIV test results, information about substance abuse, psychological profiles, information about cosmetic surgery, or behavioral health records.
- Ensure that outside vendors and third parties can only access the information necessary to perform their required service. Wherever feasible, ensure that access to PHI or other confidential information is limited to a read-only format.

Audit and Accountability

- Ensure that audit logs include sufficient detail to identify the patient records that are viewed or updated and by whom.
- Formally assign the responsibility for reviewing audit logs to a particular individual.
- Periodically conduct random audits of user activities to maintain a culture of accountability.
- Periodically conduct audits of particular scenarios to identify breaches of confidentiality. For example, periodically audit access to information for VIPs or employees who are also patients. Also periodically audit new employees as well as those who view records outside of their department (e.g., those who work in the ER). It's also important to audit individuals who " break the glass" to access records not assigned to them.
- Conduct ongoing audit log reviews to identify red flags of a potential security breach (e.g., failed log-in attempts). Review audit logs at the network, server, and application levels.
- Secure and protect audit logs from unauthorized modifications so that only individuals with a job-related requirement to view these logs can do so.
- Use warning banners and/or other awareness methods to notify and remind workers that their activities are being audited and monitored. Ensure periodic monitoring of workforce members (security administrators) who have been given special privileges. In particular, monitor actions such as account set up and password resets to assure appropriate use of these capabilities.

Awareness and Training

- Ensure that there are organizational records or documents to demonstrate that information security awareness is conducted. Annual refresher training is required. Ensure that management is aware of individuals who have not completed their annual security awareness training.
- Link security awareness with user provisioning. Employees, temporary workers, contractors, and some vendors must complete initial security awareness training before gaining access to PHI.
- Ensure that management annually reviews and provides feedback for both the initial and the refresher security awareness training. This ensures that the content is current and that it addresses newly-discovered threats or risks.
- Require all workers (e.g., employees and nonemployees such as students, volunteers, contractors, etc.) to sign a confidentiality agreement.
- Ensure that the organization's medical staff bylaws or rules outline physician responsibilities for protecting the confidentiality of health information.
- Adequately train staff members with remote access on the use of clinical information systems and their responsibilities for protecting confidential information.
- Ensure that employees are 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

- Update business associate agreements in light of the HITECH Act to include the new HIPAA security rule requirements as well as the definition of breach [according to the final Omnibus Rule]. Details for breach notification include the following:
    - How to report

    - When to report
    - Who to report to
- Obtain satisfactory assurances of compliance in contracts or agreements from business associates and any of their agents or subcontractors.

Computer Workstations

- Implement policies and procedures that outline workers' responsibilities for securing workstations, laptops, and other portable devices.
- Ensure that users consistently logg off before leaving their work area. Active screen savers after a predetermined period of inactivity to prevent incidental disclosure of PHI.
- Maintain an accurate inventory for computer equipment (e.g., laptops, desktops, tapes, flash drives, etc.) and biomedical devices that store PHI.
- Implement general security safeguards and controls for biomedical devices storing PHI to maintain security consistency.

Contingency and Disaster Recovery Planning

- Back up information systems periodically. Maintain all back-up data in a secure offsite location. The frequency of the back-up procedure is determined by the organization's needs.
- Ensure that information needed to treat patients is available at the bedside in the event of a loss of data-processing capabilities.
- Ensure that departments have their own documented contingency plan in place in the event of planned or unplanned downtimes of critical applications and systems.
- Conduct a formal business impact analysis 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.
- Ensure that the disaster recovery plan meets the recovery point objective and recovery time objective for the organization.
- Document evidence of a recent exercise or a test of the disaster recovery plan.

Incident Reporting and Response

- Inform employees regarding how to detect and report known or suspected information incidents and privacy breaches.
- Develop an incident response team. Provide training for the team's core members particularly regarding the collection and handling of evidence during an investigation.
- Conduct a tabletop exercise periodically to test incident response capability.
- Follow breach reporting requirements as specified under the HITECH Act. Ensure that there is an objective process in place for analyzing the potential risk of harm in the event of an incident.

Media Protection and Controls

- Ensure that 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 in order to avoid breach notifications and lower enforcement penalties.

- Include voice technology that is produced digitally from or stored on an information system in policies, safeguards, and controls used to protect electronic media.
- Ensure that policies and procedures address patient requests to obtain copies of their medical information in an electronic format include appropriate media controls to reduce risks.
- Dispose of printed reports containing confidential information when those reports are no longer needed. Ensure disposal in a manner that protects confidentiality (i.e., shredding, pulping, or burning).
- Sanitize all hard disk drives. This ensures that all confidential information is erased permanently from the drive before being disposed of or reused. Maintain documentation of destruction.

Mobile and Portable Device Security

- Maintain an accurate inventory of laptops, tablets, and other portable devices that store PHI.
- Take steps 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

Human Resources Security

- Use photo identification badges to distinguish employees and workforce members from contractors, sales representatives, and visitors.
- Document procedures 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 must be appropriate to a worker's level of access to PHI and other confidential information.
- Conduct additional background checks for individuals serving in trusted positions, such as a system administrator or network engineer.
- Conduct a reinvestigation process for positions identified as high risk.

Physical and Environmental Protection

- Ensure that 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 accessing restricted access areas such as data centers
    - Policy for 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. Ensure collection of copies of related facility work orders.

- Conduct privacy and security walkthrough inspections regularly. Document findings to ensure that all PHI is secured properly when not in use. Also evaluate physical security controls and identify any issues or weaknesses in the implementation of the information security program.

Policies, Procedures, and Plans

- Review information security policies periodically and update as necessary to ensure that they are in line with accreditation standards as well as state and federal laws
- Use tools (i.e. intranet, database) to manage and distribute policies and procedures centrally and to verify that workers have reviewed the policies that pertain to them.
- Conduct periodic evaluations 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

- Ensure appropriate measures to protect systems from unauthorized remote access.
- Enable an automatic disconnect of a log-in session after a specific period of inactivity.

- Use two-factor authentication may for remote connectivity—especially for anyone with system administrator privileges.

Risk Analysis and Management

- Document a well-defined risk analysis process. The process is followed to identify threats and vulnerabilities and to present the results in a formal risk analysis report.
- Conduct periodic risk analysis on systems and applications that store, process, or transmit PHI. Risk analysis is an ongoing process to evaluate whether security controls are appropriate. Perform such analysis whenever there is a significant change in the computing environment. The U.S. Department of Health and Human Services released "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" in the summer of 2010. This guidance, "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]
- Ensure that management reviews and signs risk analysis reports. These reports include the findings and recommended corrective actions that must occur as a result of conducting a risk analysis.
- Ensure that the latest network vulnerability scanning and penetration test results are available for review. Ensure that the risks associated with the discovered vulnerabilities are managed appropriately.

Transmission Security

- Ensure that PHI and other confidential information being transmitted outside of the organization (via the Internet) is encrypted using a method that meets Federal Information Processing Standards 140-2.
    - **Note**: Although encryption is an addressable HIPAA Security Rule standard and not required, it is highly recommended to minimize the probability of a data breach and reduce the likelihood of compliance enforcement penalties.
- Ensure that outbound e-mail is scanned. Emails detected as containing sensitive and confidential information must be encrypted automatically to protect them from unauthorized access, alteration, and disclosure.
- Ensure that 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 should be replaced with stronger encryption standards when those are developed.

Information Asset Management

- Nominate an owner for all information assets and ensure that the individual is held accountable for the overall security of that information.
- Identify owners for all information assets. Also identify the responsibility for the maintenance of appropriate controls.
- Ensure that the owner delegates the implementation of specific controls while also remaining responsible for the proper protection of the assets.

Vulnerability Management

- Perform periodic technical vulnerability scans as well as nontechnical administrative reviews and gap analyses.
- Ensure all information assets and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches.
- Protect all information assets against malware, and regularly update anti-virus software or programs.

Note

1. U.S. 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 and Acknowledgement (2013)

William M. Miaoulis, CISA, CISM

Appendix Prepared by (2010)

Tom Walsh, CISSP

Appendix Acknowledgments (2010)

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

Appendix B: Topic Areas to Address in Organization/Department Policies and Procedures

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

HIPAA Security Rule Standards and Implementation Specifications

- Security Management
    - Risk analysis
    - Risk management
    - Sanctions
    - Information system activity review
- Security Responsibility
- Workforce Security
    - Authorization and/or monitoring
    - Workforce clearance procedures
    - Termination procedures
- Information Access Management
    - Isolating healthcare clearinghouse functions

- Security Awareness and Training
    - Security reminders
    - Protection from malicious code
    - Log-in monitoring
    - Password management
- Security Incident Procedures
    - Response and reporting
- Contingency Planning
    - Data backup plan
    - Disaster recovery plan
    - Emergency mode of operation plan
    - Testing and revision procedure
    - Application and data criticality analysis
- HIPAA Evaluation
- Facility Access Control
    - Contingency operations
    - Facility security plan
    - Access control and validation procedures
    - Maintenance records
- Workstation Use / Workstation Security
- Device and Media Controls (including disks, hard drives, computers, copies, printers, bio-medical and printed reports)
    - Disposal
    - Media reuse
    - Accountability (inventories)
    - Backup and storage
- Access Controls
    - Unique user identification
    - Emergency access procedure
    - Automatic logoff
    - Encryption and decryption
- Audit Controls
    - Trails and system logs
- Integrity
    - Mechanism to authenticate electronic protected health information
- Person or Entity Authentication
- Transmission Security
    - Integrity
    - Encryption
- Documentation: Security Activity
    - Retention time limit
    - Availability

- Updates

HITECH Breach Notification

Other Topic Areas a Security Policy Must Address:

- Acquisition of Hardware
- Acquisition of Software
- Audit procedures to avoid discrimination
- Audit trail retention
- Bringing in software, discs, or other media (i.e. flash drives) from outside the organization
- Business associates
- Change management (approved, tested, risk-identified)
- Configuration management
- Dictation and transcription systems
- Electronic data interchange
- Email archiving and e-discovery
- Internet access
- Laptops, smartphones, tablets and other mobile devices
- Malicious code
- Privacy rights (including the rights of patients, families, caregivers, employees, and researchers)
- Protection of confidential and proprietary information
- Remote access to information systems/network (telecommuting)
- Retention, archiving, and destruction of electronic and paper-based information
- Workforce responsibility for data accuracy and integrity
- 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
- Vulnerability management

Article citation:
AHIMA Practice Brief. "Information Security—An Overview (2014 update)" (Updated January 2014)
