

The HIPAA Security Standards

3

CHAPTER OUTLINE

- HIPAA Security
 - Electronic Protected Health Information
 - Threats to Information Security
 - Security Background
- Organization of the HIPAA Security Standards
 - Administrative, Physical, and Technical Standards
 - Implementation Specifications
- Administrative Standards
 - Key Provisions
 - Implementation Specifications for Administrative Standards
- Physical Standards
 - Key Provisions
 - Implementation Specifications for Physical Standards
- Technical Standards
 - Key Provisions
 - Implementation Specifications for Technical Standards
- HIPAA Security Standards: Portable and/or Mobile Media, Faxes, and E-mail
 - Portable and/or Mobile Media Guidance
 - Sending Faxes and E-mail
- Case Discussion
 - Case 1
 - Case 2
 - Case 3

LEARNING OUTCOMES

After studying this chapter, you should be able to:

1. Define electronic protected health information (ePHI).
2. List the three goals of the HIPAA security standards.
3. Compare and contrast risk analysis and risk management.
4. Define identity theft.
5. Describe the organization of the HIPAA Security Rule.
6. Explain the purpose of implementation specifications, distinguishing between those that are required and those that are addressable.
7. Describe key administrative safeguards.
8. Discuss key physical safeguards.

9. Describe key technical safeguards.
10. Discuss the HIPAA security considerations for portable and/or mobile devices and for fax and e-mail transmissions.

KEY TERMS

addressable implementation specifications
administrative standards
antivirus software
authentication
authorization
availability
backup procedure
confidentiality
confidentiality notice
cryptography
degaussing
digital certificate
e-discovery
electronic protected health information (ePHI)
encryption
firewall
HIPAA Security Rule
identity theft

implementation specifications
integrity
malware
network security
password
physical standards
portable and/or mobile media devices
protocol
required implementation specifications
risk analysis
risk management
role-based authorization
sanction policy
security incidents
technical standards
unique user identification
workstation



Why This Chapter Is Important

The HIPAA security standards complement the HIPAA privacy regulations by describing how electronic information about patients must be kept safe. Knowledge of the security measures is essential for allied health personnel, who must know how to safeguard the electronic exchange of information on behalf of patients.

What Is Your Opinion? <<

Think about the following cases as you study the HIPAA security standards. In each case, protected health information had been improperly disclosed. In your opinion, what steps could have been taken to avoid the security violation? Decide on your answers, and compare them with the case discussion that precedes the chapter summary.

CASE 1

A medical assistant e-mailed the results of a patient's TB test to the wrong specialist's office.

CASE 2

The Department of Veterans Affairs announced that all agency computers would be upgraded with data security encryption immediately. The move came in the wake of a second theft of a VA laptop from a vendor's office. Laptops would be the first to receive the encryption programs, followed by desktop computers and portable media.

CASE 3

A thief stole backup tapes from the van of a provider's employee who had taken the tapes in order to do some work over the weekend. The provider waited for more than three weeks to tell the state department of justice and the patients about the loss of personal medical and financial information. The provider was later ordered by the state to provide twelve months of free credit monitoring to patients affected by the data breach. The provider also had to pay patient claims for any losses directly resulting from the data theft.

HIPAA Security

The **HIPAA Security Rule** was published in the *Federal Register* on February 20, 2003, with required implementation by April 20, 2005. The rule contains many security standards that have become federal law, as required under HIPAA. The security standards require appropriate administrative, physical, and technical safeguards to protect the privacy of protected health information against unintended disclosure through breach of security (see Figure 3-1 on page 62).

ELECTRONIC PROTECTED HEALTH INFORMATION

Like the HIPAA Privacy Rule, the Security Rule applies to covered entities (CEs; see Chapter 1). The Security Rule, though, focuses only on *electronic* protected health information, not on paper records. **Electronic protected health information (ePHI)** is PHI (see Chapter 2) that is stored or transmitted in electronic form. Electronic storage includes computer systems and storage devices of all types. Electronic transmission methods include Internet, computer networks within organizations, and

Figure 3-1

HIPAA Security Standard Home Page

The screenshot shows the CMS website's "Security Standard Overview" page. The page is titled "Security Standard Overview" and contains the following sections:

- Security Standard Overview**: A brief introduction to the HIPAA Security Standard, stating that the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.
- HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information**: A section providing general information on the risks and possible mitigation strategies for remote use of and access to Electronic Protected Health Information (EPHI). It states that CMS has prepared guidance to provide HIPAA covered entities with general information on the risks and possible mitigation strategies for remote use of and access to EPHI.
- HIPAA Security Educational Paper Series**: A section stating that CMS has delegated authority to enforce the non-privacy provisions of the HIPAA Regulations, to include HIPAA Security. This guidance document sets forth CMS' minimal compliance expectations for covered entities seeking to safeguard EPHI that is accessed, stored or transported offsite. Please note however that this document does not seek to provide a comprehensive list of risks and mitigation strategies but rather a general list of suggestions for organizations that require remote use of sensitive health information. To view this document, please see the link on the Download section below.
- Downloads**: A section with a link to "HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information [PDF, 330KB]".
- Related Links Inside CMS**: A section with a link to "HIPAA Security Educational Paper Series".
- Related Links Outside CMS**: A section with a link to "HIPAA - General Information".
- Page Last Modified: 12/14/2005 12:00:00 AM**: A section with a link to "Help with File Formats and Plug-Ins".
- Submit Feedback**: A link to "Submit Feedback".

At the bottom of the page, there is a footer with the following text: "Department of Health & Human Services | Medicare.gov | USA.gov Web Policies & Important Links | Privacy Policy | Freedom of Information Act | No Fear Act Centers for Medicare & Medicaid Services, 7500 Security Boulevard Baltimore, MD 21244".

HIPAA CAUTION

Paper Not Addressed by Security Standards

Information not in electronic form before the transmission, messages left on voice mail, and paper-to-paper faxes that were not electronic before being sent are not covered.

ePHI that is physically moved from one location to another using magnetic tape, disks, CDs, flash drives, or any other removable media.

The goals of the HIPAA security standards (see Figure 3-2) are to ensure:

- The **confidentiality** of ePHI—ensuring that the information is shared only among authorized individuals or organizations
- The **integrity** of ePHI—making sure that the information is not changed in any way during storage or transmission and that it is

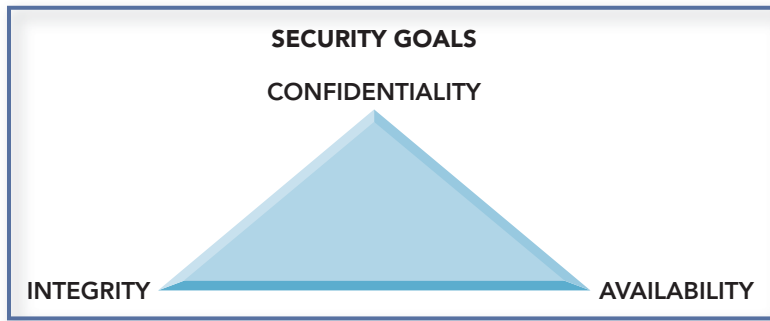


Figure 3-2
Security Goals

authentic and complete and can be relied on to be sufficiently accurate for its purpose

- › The **availability** of ePHI—ensuring that the systems responsible for delivering, storing, and processing data are accessible, when needed, by those who need them under both routine and emergency circumstances

The HIPAA security standards do not state specific actions that CEs must take. Instead, the rule recognizes that the policies and procedures must vary according to the size of a CE (the number of employees and locations) and the type of work it performs. The wording of the security standards provides goals and examples that allow a covered entity to use any security measures that allow it to meet the requirements. A CE must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.

THREATS TO INFORMATION SECURITY

The HIPAA security standards require covered entities to analyze and then manage the risk that any ePHI they possess could be accessed by anyone other than appropriate and authorized individuals. **Risk analysis** means that the CE must examine and document any potential threats to the security of its information. **Risk management** means establishing policies and procedures that reduce the risk of breaches of security. The risk analysis and management process involves planning, implementing, and verifying the protection of the CE’s electronic assets from internal and external threats.

Threats to information security come from a number of sources, including natural events as well as events resulting from intent to cause harm. Common threats include:

- › Natural disasters such as rain, fire, flood, earthquake, explosion, lightning, and building structural failure
- › Utility outages such as loss of electrical power
- › **Malware**—any program that harms information systems, which is often brought into an organization through e-mail attachments or programs that are downloaded from the Internet (see Table 3-1)
- › Identity theft
- › Subversive employees or contractors
- › Computer system changes and updates

COMPLIANCE TIP

Ongoing Tasks

Covered entities must ensure that the risk analysis and risk management process is ongoing and dynamic and can change as the environment or operations change.

FYI**Identity Theft**

Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. Identity theft of financial information is a fast-growing crime, affecting nearly 9 million Americans each year. Any purchase at a website or a similar online transaction, such as online banking, increases an individual's risk of identity theft. In some cases, identity theft occurs when someone's medical information is stolen and misused.

People's identities are stolen in a number of ways. They may be stolen from an unprotected computer, from unshredded documents, by thieves invading a mailbox, or by phishing—when thieves try to trick people into revealing personal information by imitating e-mail from legitimate institutions. The thief takes this personal information to illegally get income, such as taking money from ATMs or using credit cards for purchases.

The federal government and many states have passed laws prohibiting identity theft. The HIPAA security standards are one of a number of laws and regulations that are attempting to control identity theft. Anyone who intentionally uses the Social Security number of another person to establish a new identity or to defraud the government is breaking the law.

If a SSN theft is suspected, it should be reported to the Federal Trade Commission at www.ftc.gov/bcp/edu/microsites/idtheft

TABLE 3-1**Types of Malware**

Viruses	A virus self-replicates by inserting copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program.
Worms	A worm is a self-replicating, self-contained program that usually executes itself without user intervention.
Trojan Horses	A Trojan horse is a self-contained, nonreplicating program that, while appearing to be benign, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to systems. They often deliver other attacker tools to systems.
Malicious Mobile Code	Malicious mobile code is software with malicious intent that is transmitted from a remote system to a local system and then executed on the local system, typically without the user's explicit instruction.
Blended Attacks	A blended attack uses multiple infection or transmission methods. For example, a blended attack could combine the propagation methods of viruses and worms.
Tracking Cookies	A tracking cookie is a persistent cookie that is accessed by many websites, allowing a third party to create a profile of a user's behavior. Tracking cookies are often used in conjunction with web bugs, which are tiny graphics on websites that are referenced within the HTML content of a webpage or e-mail. The only purpose of the graphic is to collect information about the user viewing the content.
Attacker Tools	Various types of attacker tools might be delivered to a system as part of a malware infection or other system compromise. These tools allow attackers to have unauthorized access to or use of infected systems and their data, or to launch additional attacks.
Non-malware Threats	These are often associated with malware. Phishing uses computer-based means to trick users into revealing financial information and other sensitive data. Phishing attacks frequently place malware or attacker tools on systems.

It is often difficult for individuals to recognize when a computer system has suffered a security compromise. The job of detecting problems in each CE's electronic system is shared by personnel who use the ePHI in their daily work and personnel such as information technology specialists who monitor and service the computer system.

SECURITY BACKGROUND

Because of the advantages to health care organizations, most CEs use computer networks rather than providing every employee with a

stand-alone personal computer. The CE's information is accessed and stored on devices connected over this network, permitting employees to share data and programs. The network is connected to larger networks outside the organization, such as the Internet. As a result, **network security**, the practice of protecting and preserving resources and information on a network, is an important information security issue. Maintaining a secure network involves a variety of different aspects.

Network Basics

Within an organization, PCs are connected to a network so that users can exchange and share information and hardware (such as printers). The central component of the network is a server, a powerful computer that acts as an intermediary between PCs on the network and provides a large volume of disk storage for shared information, such as shared application programs. The server controls access to the data through the use of access controls that limit user access to various files and programs stored on the server.

Imagine that all of a facility's computer resources are placed in locked rooms—accounting data in one room, research in another room, and so on. Decisions need to be made about who will have access rights to the different types of data. Once access rights have been assigned, each user is given a key to the designated rooms. To initiate a session on the network, users at a PC must log into the server and provide a user ID and key (a password). They are then able to use the files to which they have been granted access rights. In addition to assigning access rights, CEs use software to create activity logs. These logs detail the activity on each system and can be reviewed for abnormalities.

Routers, Firewalls, and Proxy Servers

A router is a device that links a local network to a remote network and determines the best route for data to travel across the network. For example, a company may use a router to connect a local area network to the Internet. A network router reads every packet of data passed to it, determining whether it is intended for a destination within the router's own network or should be passed farther along the Internet.

Depending on the configuration, the packets of data usually must pass through an open port in the firewall before continuing on to their destination. A **firewall** is a security device that examines traffic entering and leaving a network and determines (based on a set of user-defined rules) whether to forward it toward its destination. Packet filtering is a process in which a firewall examines the nature of each piece of information traveling into or out of the network. A firewall acts as a gatekeeper, deciding who has legitimate access to a network and what sorts of materials should be allowed in and out.

The purpose of a firewall is not only to prevent unauthorized entry into the network, but also to prevent unauthorized data from exiting the network. It controls what users can access on the Internet. For example, a firewall could be set up to block access to websites that are used for playing games. Firewalls are also used to log information such

Selecting Good Passwords

If you are picking your own password, these are recommendations:

- Always use a combination of at least six letters and numbers that are not real words and also are not obvious (such as a number string like 123456 or a birth date).
- Do not use a user ID (login, sign-on) as a password. Even if an ID has both numbers and letters, it is not secret.
- Select a mixture of uppercase and lowercase letters if the system permits, and include special characters such as @, \$, or & if possible.
- Change passwords periodically, but not too often. Forcing frequent changes can actually make security worse because users are more likely to write down the passwords.

HIPAA CAUTION

Protect Passwords!

Never share your password with coworkers or patients and clients.

as files that are transferred, websites that are visited, and servers that are logged into. Some firewalls even have antivirus software built in to reject known viruses.

Passwords

Passwords are another means of preventing unauthorized users from gaining access to information on a computer or network. Password utilization is a standard practice in most health care organizations. It is easy to implement, and it can keep unauthorized users from successfully logging onto a system or network. Password logging programs can track all successful and failed log-in attempts, which can be useful in detecting possible break-in attempts or unauthorized logging.

Unless they are very small organizations, most CEs use **role-based authorization**, in which access is based on the individual's title and/or job function, so that only people who need information can see it. Once access rights have been assigned, each user is given a key to the designated databases. Users must enter a user ID and a key to see files to which they have been granted access rights. For example, in a hospital admissions department, receptionists may view the names of patients being admitted that day, but they should not see those patients' medical records. However, the nurse or physician needs to view the patient records. Receptionists are given individual computer passwords that let them view the day's schedule but that deny entry to patient records. The physicians and nurses possess computer passwords that allow them to see all patient records.

Cryptography and Transmission Protocols

Cryptography is the protection of information by transforming it into an unreadable format before it is distributed. To read a message, the recipient must have a key that deciphers the information. The act of encoding the contents of the message is known as **encryption**. Cryptography also enables the recipient to determine whether the message has been intercepted and tampered with before final delivery. This allows the message to be checked for authenticity.

There are two types of encryption. In symmetric encryption, the same key is used to encrypt and decrypt the message. In asymmetric (or public-key) encryption, one key encrypts a message and another decrypts it.

Another method, based on data communication technology, uses a network communication **protocol** to ensure that the data sent are the data received. This requires a kind of check digit at the beginning and end of a message that is recognized by the receiver.

Cryptography or communication protocols are essential for the transmission of sensitive data. These methods are widely used to protect e-mail messages, credit card information, and corporate data.

3-1 Thinking It Through

The following situation was reported by the Associated Press:

AP June 12, 2007

The personal health information of more than 9,000 Concord Hospital patients was exposed on the Internet for more than a month. The hospital's president said there's no way of knowing whether any were poached by criminals.

The hospital sent letters last week notifying 9,297 patients and confirmed the breach Saturday to local media. A statement posted Sunday on its website said Concord Hospital was working to ensure no future security lapses.

Concord Hospital said Verus, Inc., its online billing contractor, disabled an electronic firewall protecting the information on April 12 to perform maintenance, then inadvertently left it off. Verus notified Concord Hospital of the breach on May 30.

1. In this situation, who is responsible for the security breach?
2. What risks do the patients face, in your opinion?
3. What steps is Concord Hospital likely to require its business associate, Verus, Inc., to take in the future to protect the security of Concord's ePHI?

Antivirus Software

Antivirus software scans a system for known viruses. After detection, the antivirus software attempts to remove the virus from the system and, in some cases, fix any problems the virus created. Antivirus tools cannot detect and eliminate all viruses. New viruses are continually being developed, and antivirus software must be regularly updated to maintain its effectiveness.

COMPLIANCE TIP

Internet Security Symbol

On the Internet, when an item is secure, a small padlock appears in the status bar at the bottom of the browser window.



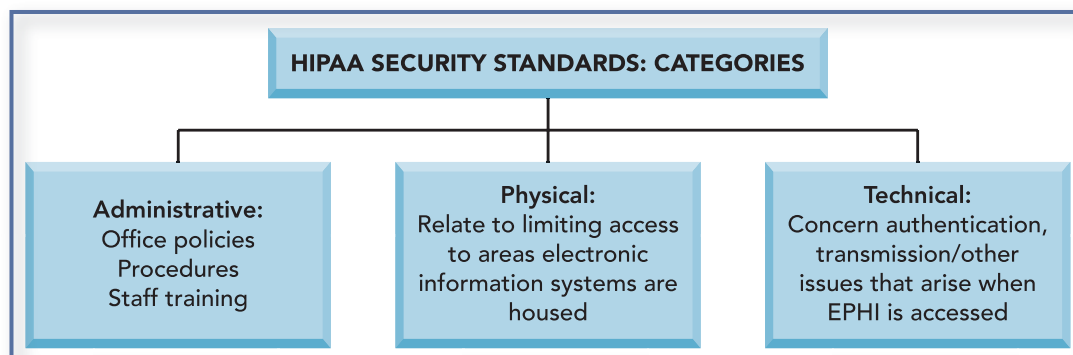
The padlock symbol shows that encryption is being used.

Organization of the HIPAA Security Standards

The HIPAA Security Rule contains specific standards that give direction on how to meet its requirements. The standards are organized into three categories, as shown in Figure 3-3.

Figure 3-3

The HIPAA Security Standards Categories



ADMINISTRATIVE, PHYSICAL, AND TECHNICAL STANDARDS

Administrative standards relate to the administrative actions that a covered entity must perform, or train staff to do, to carry out security requirements. These actions include implementing office policies and procedures for ways to prevent, detect, contain, and correct security violations. **Physical standards** require covered entities to implement policies and procedures that limit unauthorized physical access to electronic information systems such as computers as well as the facilities where the ePHI is stored. **Technical standards** require CEs to create policies and procedures that govern the technical aspects of accessing ePHI within computer systems by appropriate personnel.

COMPLIANCE TIP

Required Records

For all standards and implementation specifications, CEs must maintain a current document that explains their compliance process. This document must be retained for six years from either the date it was created or the date it last went into effect, whichever is later, and remain available to those persons responsible for implementing the procedures.

IMPLEMENTATION SPECIFICATIONS

Along with each category of HIPAA security standards are **implementation specifications** that provide specific details on how to implement them. There are two types of implementation specifications, those that are required and those that must be addressed. **Required implementation specifications** must be in place just as described by the standard. **Addressable implementation specifications** are guidelines that must be “addressed” (covered); the CE must in some manner accomplish the goal of the specifications or document why it did not do so.

Administrative Standards

According to the HIPAA Security Rule, the administrative standards guide actions, policies, and procedures that manage the security measures to protect ePHI and also manage the conduct of the covered entity’s workforce in relation to the protection of that information. The provisions and implementation specifications are shown in Table 3-2, and the major concepts are explained below.

KEY PROVISIONS

The HIPAA administrative standards include nine key points, each guiding a particular aspect of security.

Security Management Process

The security management process requires the CE to perform a risk analysis and then to manage the risk by having policies and procedures that are designed to prevent, detect, contain, and correct HIPAA security violations.

Assigned Security Responsibility

A covered entity has to appoint a HIPAA security officer who is responsible for its security policies and procedures.

TABLE 3-2

Administrative Safeguards

STANDARDS	IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED, (A) = ADDRESSABLE	
Security Management Process	Risk analysis	(R)
	Risk management	(R)
	Sanction policy	(R)
	Information system activity review	(R)
Assigned Security Responsibility		
Workforce Security	Authorization and/or supervision	(A)
	Workforce clearance procedure	(A)
	Termination procedures	(A)
Information Access Management	Isolating health care	(R)
	Clearinghouse functions	
	Access authorization	(A)
	Access establishment and modification	(A)
Security Awareness and Training	Security reminders	(A)
	Protection from malicious software	(A)
	Log-in monitoring	(A)
	Password management	(A)
Security Incident Procedures	Response and reporting	(R)
Contingency Plan	Data backup plan	(R)
	Disaster recovery plan	(R)
	Emergency mode operation plan	(R)
	Testing and revision procedures	(A)
	Applications and data criticality analysis	(A)
Evaluation		
Business Associate Contracts and Other Arrangements	Written contract or other arrangement	(R)

Workforce Security

The workforce security standard requires a CE to have policies and procedures in place to ensure that all employees who should have access to ePHI do have access. For each workforce member, or job function, the covered entity must identify the ePHI that is needed and when it is needed, and make reasonable efforts to control access to it. This also includes identification of the computer systems and applications that provide access to the ePHI. Covered entities must provide only the minimum necessary access to ePHI that is required for a workforce member to do his or her job. Policies must also ensure that employees who should *not* access ePHI are unable to do so.

COMPLIANCE TIP

Security Officer

For a small CE, such as a small physician practice, the HIPAA security officer is often the same individual as the HIPAA privacy official. In large facilities, the security officer might be the director of the information technology or health information management department.

Information Access Management

A CE has to have procedures for authorizing employees' access to ePHI. In HIPAA security terms, **authorization** is the process of determining whether a particular user (or a computer system) has the right to carry out a certain activity, such as reading a file or running a program.

Security Awareness and Training

A CE must train its employees about the security policies and procedures. (Initial security training was required by the compliance date of the rule.) Periodic retraining should be given whenever environmental or operational changes affect the security of ePHI. Changes may include new or updated policies and procedures, new or upgraded software or hardware, new security technology, or changes that are announced in the Security Rule itself.

Security Incident Procedures

A CE also must have policies and procedures in place to address **security incidents**, defined in the law as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” The CE’s security documents must explain how to identify security incidents and to whom they should be reported.

Contingency Plan

A CE must set up policies and procedures for responding to an emergency or other occurrences that threaten the security of electronic records, such as a power outage, fire, natural disaster, or computer system failure. The goal is to ensure that CEs have ePHI available when it is needed.

Evaluation

Ongoing evaluation of a CE’s policies and procedures should be conducted to update the risk analysis and handle changing situations.

Business Associate Contracts

Covered entities must have wording in their contracts with business associates (see Chapter 1) that require them to comply with the HIPAA security standards.

IMPLEMENTATION SPECIFICATIONS FOR ADMINISTRATIVE STANDARDS

A number of implementation specifications are part of the administrative standards; the following are key points.

Sanction Policy

A key specification is the required **sanction policy** that CEs must have. It should state the consequences for violations of security policies and

procedures by employees, agents, and contractors. Violations could result in actions ranging from retraining the employee who violated the policies and procedures to terminating the individual if the violation is egregious. Sanctions must be applied equally to all individuals, and the policy should apply to any and all violations.

Workforce Clearance Procedures

An important addressable implementation specification is the need to have workforce clearance procedures, which ensure that individuals who have access to ePHI have been given appropriate clearance, such as a background check before being hired.

Data Backup Plan

Most CEs have data **backup procedures** as part of normal business activities, and this is a required implementation specification under the administrative standards. Backing up is the activity of copying files to another medium (such as tape, disk, CD, or online backup service) so that they will be preserved in case the originals are no longer available. A successful backup plan is critical in recovering from either a minor or major security incident that jeopardizes critical data. For the health care industry, a backup plan must review all the important sources of data, such as:

- › Patient accounting systems
- › Electronic medical (health) records
- › Health maintenance and case management information
- › Digital files of diagnostic images and test results

Disaster Recovery Plan

Disaster recovery has taken on new urgency in recent years. As CEs' reliance on computers has increased, so have the threats of terrorism, hackers, and computer viruses. A disaster recovery plan, as required under the administrative standards, details activities and preparations to minimize loss and ensure continuity of critical business functions in the event of a major disaster. The types of events addressed by a disaster recovery plan typically include:

- › Natural disasters (earthquake, fire, flood, storm)
- › Terrorist acts (explosion, chemical weapons, hostage-taking)
- › Power disruptions and power failures
- › Computer software or hardware failures
- › Computer shutdowns (effects of hacker, virus)
- › Labor problems (strike, slowdown, walkout)

Emergency Mode Operation Plan

To ensure availability in emergency situations, one of the three goals of the security standards, CEs must implement an emergency mode operation plan.

Which administrative standard does each of the following address?

1. If an employee inadvertently leaves ePHI visible on a computer screen, retraining on security procedures is provided.
2. A CE includes the HIPAA administrative standards requirements in its contract with a medical transcription service.
3. A new computer system is installed, and a new risk assessment process is performed.
4. The CE has a policy requiring all employees to report breaches of security procedures by other employees.
5. The HIPAA privacy official is appointed to the role of security official.
6. All employees of the CE have to have passwords to access information.
7. The CE has weekly security training classes for new employees.
8. The CE is covered by a plan for handling a fire in the computer storage area.
9. In a very small provider office, the policy is to allow all staff members to access all ePHI in their information system, since they may perform multiple functions.

Physical Standards

Physical security means the protection of building sites and equipment from theft, vandalism, natural disasters, and accidental damage. It includes controlling the environment in which the electronic systems operate and handling electrical power (noise, brownout, humidity, and static), fire detection and suppression, heating, ventilation, and air conditioning. Physical security also includes ways to control access such as locks, guards, surveillance monitors, intrusion detectors, and alarms. It includes maintaining appropriate controls of files that are retained, stored, or scheduled for destruction. The physical safeguards and implementation specifications are presented in Table 3-3; major provisions are explained below.

KEY PROVISIONS

The HIPAA physical standards are as follows:

- *Facility access controls:* Mechanisms must be in place to ensure that only authorized staff members can enter the premises and remove systems or media containing ePHI. An example of a mechanism is a log for a physician practice that identifies all employees who have security codes for entering the facility and also for locking up the premises at the end of the work day.
- *Workstation use:* A **workstation** is an electronic computing device such as a laptop or desktop computer and electronic media stored in its immediate area. CEs must have policies and procedures that describe appropriate functions for a specific workstation or classes of workstations that are used to access ePHI. An example of this

COMPLIANCE TIP

Home or Office

All safeguards for office workstations must also be applied to workstations located off-site.

TABLE 3-3

Physical Safeguards

STANDARDS	IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED, (A) = ADDRESSABLE	
Facility Access Controls	Contingency	(A)
	Facility security plan	(A)
	Access control and validation procedures	(A)
	Maintenance records	(A)
Workstation Use		
Workstation Security		
Device and Media Controls	Disposal	(R)
	Media reuse	(R)
	Accountability	(A)
	Data backup and storage	(A)

standard is restricting the ePHI available on a reception area computer to only the ePHI needed to schedule or change appointments.

- › *Workstation security:* Mechanisms must be in place to ensure that computer workstations and all other devices are secure and are used appropriately. For example, physically attaching a computer to a desk so that it cannot be removed by a thief meets this standard.
- › *Device and media controls:* A CE must have policies and procedures that ensure security when moving computers and/or other electronic media (for example, backup tapes and flash drives) that contain ePHI within and outside the facility. An example of a policy that meets is this standard is to remove all sensitive information from the computer before transferring it to another user.

IMPLEMENTATION SPECIFICATIONS FOR PHYSICAL STANDARDS

Two implementation specifications are required for the HIPAA physical standards. The disposal implementation specification requires CEs to address the final disposition of ePHI. When disposed of, the media must be made unusable or inaccessible. Simply deleting files or formatting drives is not sufficient. One effective method of disposal is **degaussing**, in which a strong magnetic field is applied to fully erase the data. Another method is to physically break, burn, or destroy the media beyond repair.

CEs may reuse media instead of destroying it. In this case, the media reuse implementation specification requires a CE to ensure that all storage media containing ePHI (such as CDs and DVDs) are carefully cleansed of all data and images before being reused. This cleansing is usually done by running a software program designed to completely remove the data.

COMPLIANCE TIP

Retention

According to the American Health Information Management Association (AHIMA), record retention requirements are at least ten years for transactional/billing records and for law enforcement purposes. Medical histories should be retained indefinitely.

3-3

Thinking It Through

Which physical standard is addressed in each of the following examples?

1. The screens on computers are turned so they cannot be seen by casual observers.
2. The computer is located in a locked office and can be accessed by authorized employees only.
3. The medical biller who works from her home is required to follow the CE's policies regarding ePHI.
4. The hospital policy is to degauss all storage media.

HIPAA CAUTION

E-Discovery

Under rule changes effective December 1, 2006, from the Federal Rules of Civil Procedure, organizations may be required to provide electronic documents in civil law cases. **E-discovery**, the process of gathering information from digital sources, is a growing part of legal proceedings, and covered entities' retention policies will be altered in the future to meet the new requirements.

Technical Standards

The technical safeguards are defined as “the technology and the policy and procedures for its use that protect ePHI and control access to it.” Many different technology solutions are available for security, and the HIPAA security standards do not specify particular choices. Technical safeguards and implementation specifications are presented in Table 3-4, and key points are explained below.

KEY PROVISIONS

The key provisions of the technical (technology) safeguards include:

- **Access controls:** In the HIPAA security standards, access means the ability to read, write, modify, or communicate data and information. CEs must have policies and procedures to ensure appropriate

TABLE 3-4

Technical Safeguards

STANDARDS	IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED, (A) = ADDRESSABLE	
Access Control	Unique user	(R)
	Emergency access procedure	(R)
	Automatic logoff	(A)
	Encryption and decryption	(A)
Audit Controls		
Integrity	Mechanism to authenticate electronic protected health information	(A)
Person or Entity Authentication		
Transmission Security	Integrity controls	(A)
	Encryption	(A)

access to ePHI by authorized individuals only. Passwords are required for authorized individuals.

- › *Audit controls:* CEs must use hardware, software, and/or procedural mechanisms that monitor ePHI for security breaches.
- › *Integrity:* CEs must protect ePHI from improper alteration or destruction.
- › *Person or entity authentication:* **Authentication** is the process of ensuring that a person is in fact who he or she claims to be before allowing the person to access ePHI. CEs must implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. A covered entity may handle authentication in one of three ways:
 - › Require the person to enter something known only to that individual, such as a password.
 - › Require something a person possesses, such as a smart card, token, or key.
 - › Require something unique to the individual, such as a *biometric* like fingerprints, voice patterns, facial patterns, or iris patterns.

Authentication of remote users in Internet or other networks often relies on a technique called a **digital certificate**. This is an electronic authorization that is issued to remote users by a covered entity. Digital certificates are digital files that certify the identity of an individual or institution seeking access to computer-based information. In enabling such access, they serve the same purpose as a driver's license or library card. The digital certificate links the identifier of an individual or institution to a digital *public key*. Digital certificates are part of the Secure Socket Layer (SSL) protocol, which enables secure electronic transactions on the Internet.

- › *Transmission security:* CEs must have technical security measures to guard against access to ePHI that is being transmitted over an electronic communications network (for example, using secure transmission systems or encryption when e-mailing or transmitting patient data).

IMPLEMENTATION SPECIFICATIONS FOR TECHNICAL STANDARDS

For this category, there are seven implementation specifications, two of which are required.

Unique User Identification (Required)

A **unique user identification** is a required implementation specification. This means that every individual in the workplace must have his or her own unique name and/or number for access to the computer system. Sharing user identifications is not permitted.

Emergency Access Procedure Required

The technical safeguards also require a procedure to be in place for accessing ePHI if there is an emergency.

COMPLIANCE TIP

Emergency Procedures

Many CEs include the emergency access procedure as part of their general emergency procedures.

Which technology safeguard is represented by each of the following policies?

1. E-mail sent from the provider to the clearinghouse is encrypted.
2. The hospital IT system automatically creates a log that shows who accessed a particular computer and when.
3. Each individual authorized to work with patient records has a unique password.
4. A health plan installs an antivirus program on all its computers and keeps it up to date.
5. Access to the hospital's record storage area requires swiping a hospital-provided smart card.

HIPAA Security Standards: Portable and/or Mobile Media, Faxes, and E-mail

Two activities, using portable media devices and sending fax transmissions and e-mail, can put ePHI at special risk. CEs must understand the special factors that are involved with them.

PORTABLE AND/OR MOBILE MEDIA GUIDANCE

Since the HIPAA security standards went into effect, many new technologies have been introduced that have changed the way medical personnel work with ePHI. No longer is it typical to work with patients' medical information in an office setting only. In many situations, portable equipment that has improved record-keeping efficiency is used:

- › A health plan employee takes backup plan subscriber data to an off-site storage facility.
- › A physician accesses an e-prescribing program while out of the office and responds to patients' requests for refills.
- › A home health nurse collects patient data while visiting patients and enters the information into a laptop computer.

While these technologies provide administrative benefits, security incidents related to their use have increased. The main concern is protecting ePHI when CEs allow remote access to data through portable devices or on external systems or hardware that they do not own or manage. Widely used **portable and/or mobile media devices** include:

- › USB flash drives and memory cards
- › Laptop computers
- › Personal digital assistants (PDAs) and smart phones
- › Home computers

- › Hotel, library, or other public workstations and wireless access points (WAPs)
- › Backup media
- › Remote access devices (including security hardware)

Because of the concern by the federal government, the *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information* has been published. It emphasizes that CEs should be extremely cautious about allowing the off-site use of ePHI.

Security incidents can occur during access, storage, or transmission. Basic guidelines are as follows:

- › Strictly limit remote access to ePHI to authorized users based on their roles within the organization and their need for access to ePHI.
- › Back up all ePHI entered into remote systems.
- › Employ encryption on all portable or remote devices that store PHI.
- › Install virus protection software on portable devices.

Special security incident procedures should cover the steps that should be taken if there is loss of ePHI through the use of portable media. Employees may need to save evidence of criminal activities, manage the harmful effects of improper use or disclosure, and notify affected parties. A sanction policy must explain the consequences of failing to comply with the security policies and procedures related to off-site use of, or access to, ePHI.

SENDING FAXES AND E-MAIL

Likewise, if a covered entity sends faxes and e-mail, HIPAA requires taking reasonable steps to protect PHI, as well as limiting the information to the minimum necessary to meet the purpose of the request. There is a danger that the fax or e-mail will be sent to an unauthorized receiver, threatening the confidentiality of the information. The following administrative procedures are recommended:

- › Double-check the recipient's fax number or e-mail address before transmittal and confirm delivery via telephone or review of the appropriate confirmation.
- › Include a **confidentiality notice** (see Figure 3-4) on all fax cover sheets and on e-mail. The statement should instruct the receiver to destroy the materials and contact the sender immediately in the event that the transmission has reached him or her in error.

Physical safeguards are also recommended:

- › Place fax machines in areas that require security keys, badges, or similar mechanisms for access.
- › Periodically remind regular fax or e-mail recipients to provide notification in the event that their fax numbers or e-mail addresses change.

INTERNET RESOURCE

HIPAA Security Guidance



www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf

COMPLIANCE TIP

Employment Prerequisite Possible

HIPAA security guidance states that a covered entity should consider requiring employees to sign a statement of adherence to security policies.

Figure 3-4

Confidentiality Notice for
Faxes and E-mail

CONFIDENTIALITY NOTICE: This transmission, including any attachments to it, may contain confidential information or protected health information subject to privacy regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This transmission is intended only for the use of the recipient(s) named above. If you are not the intended recipient or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of any of the information contained in this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify me by reply e-mail, and destroy the original transmission in its entirety without saving it in any manner.

HIPAA CAUTION

Confidentiality Notices

Although they are not required, confidentiality notices provide added legal protection. They do not, however, absolve the sender of liability if the information reaches the wrong party.

A technical security service in the case of faxes involves making certain that audit controls, like fax transmittal summaries and confirmation sheets, are stored and reviewed periodically for unauthorized access or use. Preprogram and test destination numbers in order to minimize the potential for human error.

Case Discussion

At the beginning of the chapter, three cases were presented. These are reviewed below, with discussion of how the HIPAA security standards could have been applied to block the breach.

CASE 1

A medical assistant faxed the results of a patient's TB test to the wrong specialist's office.

Discussion: This wrongful disclosure could have been avoided if the receiver's fax number had been verified before transmission. To mitigate problems, a preprinted confidentiality statement on the fax cover sheet should instruct the receiver to destroy the faxed materials and contact the sender immediately in the event that the transmission reached him or her in error.

CASE 2

The Department of Veterans Affairs announced that all agency computers would be upgraded with data security encryption immediately. The move came in the wake of a second theft of a VA laptop from a vendor's office. Laptops would be the first to receive the encryption programs, followed by desktop computers and portable media.

Discussion: From an administrative viewpoint, the physical security of laptops at all sites should be secured, and the vendor, as a business associate of the agency, should have its physical safety guidelines in place. Encrypting data on laptops and other computers will effectively halt access to the ePHI.

CASE 3

A thief stole backup tapes from the van of a provider's employee who had taken the tapes in order to do some work over the weekend. The provider waited for more than three weeks to tell the state department of justice and the patients about the loss of personal medical and financial information. The provider was later ordered by the state to provide twelve months of free credit monitoring to patients affected by the data breach. The provider also had to pay patient claims for any losses directly resulting from the data theft.

Discussion: The provider's security incident procedures should provide for quick notification of the unlawful disclosure of electronic protected health information. Likewise, employees should not take patient data home unless specifically authorized to do so.

»» CHAPTER REVIEW

CHAPTER SUMMARY

1. Electronic protected health information (ePHI) is PHI that is stored or transmitted in electronic form. Electronic storage includes computer systems and storage devices of all types. Electronic transmission methods include Internet, computer networks within organizations, and ePHI that is physically moved from one location to another using magnetic tape, disks, CDs, flash drives, or any other removable medium.
2. The three goals of the HIPAA security standards apply to ePHI. The goals are to ensure its (a) confidentiality, (b) integrity, and (c) availability.
3. The HIPAA security standards require covered entities to analyze and then manage the risk that any ePHI they possess could be accessed by anyone other than appropriate and authorized individuals. Risk analysis means that the CE must examine and document any potential threats to the security of their information. Risk management means establishing policies and procedures that reduce the risk of security breaches.
4. Identity theft occurs when a criminal uses another person's personal information to take on that person's identity for financial gain.
5. The HIPAA Security Rule is organized into three categories: (a) administrative standards, covering office policies and procedures for ways to prevent, detect, contain, and correct security violations; (b) physical standards, requiring policies and procedures that limit unauthorized physical access to electronic information systems such as computers as well as storage facilities; and (c) technical standards, requiring policies and procedures that govern the technical aspects of accessing ePHI within computer systems by appropriate personnel.
6. Implementation specifications are to be used as guidelines for covered entities in following the administrative, physical, and technical standards. Required implementation specifications must be performed as described in the standard, while addressable implementation specifications serve as guidelines that must be considered.
7. The nine administrative safeguards are:
 - *Security management process*, requiring risk analysis and management through policies and procedures that are designed to prevent, detect, contain, and correct HIPAA security violations

- › *Assigned security responsibility*, requiring appointment of a HIPAA security officer
 - › *Workforce security*, requiring policies and procedures to ensure that all employees who should have access to ePHI do have access and that employees who should *not* access ePHI are unable to do so
 - › *Information access management*, requiring procedures for authorizing employees' access to ePHI
 - › *Security awareness and training*, requiring employee training about the security policies and procedures
 - › *Security incident procedures*, requiring policies and procedures to address security incidents
 - › *Contingency plan*, requiring policies and procedures for responding to an emergency or other occurrences that threaten the security of electronic records
 - › *Evaluation*, requiring keeping policies and procedures updated
 - › *Business associate contracts*, requiring BAs to comply with the HIPAA security standards
8. The physical safeguards are:
- › *Facility access controls*, requiring mechanisms to ensure that only authorized staff members can enter the premises and remove systems or media containing ePHI
 - › *Workstation use*, requiring policies and procedures that describe appropriate functions for a specific workstation or class of workstations that are used to access ePHI
 - › *Workstation security*, requiring policies and procedures to ensure that computer workstations and all other devices are secure and are used appropriately
 - › *Device and media controls*, requiring policies and procedures that ensure security when moving computers and/or other electronic media that contain ePHI within and outside the facility
9. The technical safeguards are:
- › *Access controls*, requiring policies and procedures to ensure only appropriate access to ePHI by authorized individuals
 - › *Audit controls*, requiring the use of hardware, software, and/or procedural mechanisms that monitor ePHI for security breaches
 - › *Integrity*, requiring protection of ePHI from improper alteration or destruction

- › *Person or entity authentication*, requiring procedures to verify that a person or entity seeking access to ePHI is the one claimed
- › *Transmission security*, requiring technical security measures to guard against access to ePHI that is being transmitted over an electronic communications network

10. The HIPAA security considerations for portable and/or mobile devices advise covered entities to be extremely cautious about allowing off-site use of ePHI and, when off-site use does make business sense, to limit access, back up ePHI entered into a remote system, and use encryption and antivirus protection software. Faxes and e-mail are permitted, but the covered entity must take reasonable steps to protect the ePHI and limit the release to the minimum necessary. A confidentiality notice is considered extra protection.

MATCHING QUESTIONS

Match the key terms with their definitions.

- | | |
|--|--|
| _____ 1. confidentiality | a. Process of ensuring that a person is in fact who he or she claims to be before allowing the person to access ePHI. |
| _____ 2. integrity | b. Ensuring that the information is shared only among authorized individuals or organizations. |
| _____ 3. availability | c. Program that harms information systems. |
| _____ 4. implementation specifications | d. Allowing access according to job title and/or function. |
| _____ 5. administrative standards | e. Making sure the information is not changed in any way during storage or transmission. |
| _____ 6. technical standards | f. Required and addressable guidelines for implementing various HIPAA security standards. |
| _____ 7. physical standards | g. Policies and procedures that limit unauthorized physical access to electronic information systems. |
| _____ 8. malware | h. Policies and procedures that govern the technical aspects of accessing ePHI within computer systems by appropriate personnel. |
| _____ 9. authentication | |
| _____ 10. role-based authorization | |

- i. Office policies and procedures for ways to prevent, detect, contain, and correct security violations.
- j. Ensuring that the systems responsible for delivering, storing, and processing data are accessible, when needed, by those who need them under both routine and emergency circumstances.

TRUE/FALSE QUESTIONS


Decide whether each statement is true or false.

- ___ 1. The category of ePHI includes all protected health information, including digital and paper records.
- ___ 2. The three goals of the HIPAA security standards are the confidentiality, integrity, and availability of ePHI.
- ___ 3. Risk analysis is the process of creating policies and procedures to protect ePHI.
- ___ 4. The HIPAA Security Rule has four parts: administrative, personnel, technical, and physical.
- ___ 5. Identity theft can result in loss of money.
- ___ 6. Required implementation standards must be put into place by covered entities.
- ___ 7. Passwords can be safely shared with coworkers.
- ___ 8. Protecting a building from theft, vandalism, natural disasters, and accidental damage is covered under the administrative safeguards.
- ___ 9. The reuse of storage media is prohibited under HIPAA.
- ___ 10. Laptop computers are considered portable and/or mobile media devices.

MULTIPLE CHOICE QUESTIONS

Select the letter that best completes the statement or answers the question.

- 1. What is included in electronic protected health information under HIPAA?
 - a. digital files
 - b. printed test results

- 
- c. forms completed by patients and filed in storage cabinets
 - d. all of the above
 2. Examples of malware include
 - a. viruses
 - b. Trojan horses
 - c. worms
 - d. all of the above
 3. Appointing a security official for a newly opened clinic is an example of satisfying
 - a. an administrative security standard
 - b. a technical security standard
 - c. a physical security standard
 - d. an implementation specification
 4. Requiring employees to enter a password to authenticate their access to ePHI is an example of satisfying
 - a. an administrative security standard
 - b. a technical security standard
 - c. a physical security standard
 - d. both an administrative and a technical standard
 5. Locking the premises is an example of satisfying
 - a. an administrative security standard
 - b. a technical security standard
 - c. a physical security standard
 - d. an implementation specification
 6. Having backup procedures is an example of satisfying
 - a. an administrative security standard
 - b. a technical security standard
 - c. a physical security standard
 - d. an implementation specification
 7. Security incidents include
 - a. attempted unauthorized use of ePHI
 - b. successful unauthorized use of ePHI
 - c. neither A nor B
 - d. both A and B
 8. A sanction policy
 - a. establishes the dates of HIPAA compliance
 - b. states the consequences of violations of security policies and procedures

- c. defines physical access procedures
 - d. sets up rewards for excellence on the part of employees and business associates
9. Cryptography is
- a. used to scan computer systems for known viruses
 - b. used to prevent unauthorized users from gaining access to ePHI
 - c. protecting information by transforming it into an unreadable format before it is shared
 - d. role-based authorization
10. A firewall
- a. examines traffic entering and leaving a network
 - b. protects information by transforming it into an unreadable format before it is shared
 - c. scans computer systems for known viruses
 - d. contributes to identity theft

SHORT ANSWER QUESTIONS

Answer the following questions.

1. List the three goals for ePHI under the HIPAA Security Rule.
 - a. _____
 - b. _____
 - c. _____
2. List the three categories of the HIPAA security standards.
 - a. _____
 - b. _____
 - c. _____

APPLYING YOUR KNOWLEDGE

HIPAA Cases

1. In each of these cases of release of PHI, was the HIPAA Security Rule followed?
 - a. A laboratory faxes a patient's medical test results to a physician after verifying the fax number and including a confidentiality notice on the fax cover sheet.
 - b. A physician serves as the security officer for her solo practice.
 - c. Because of a flood in the office, all records are destroyed.
 - d. A hospital requires its personnel to wear ID badges; visitors must sign in at the front desk.

- e. A business associate turns off its antivirus program while upgrading its computer system and forgets to turn it on again, with the result that a worm enters its computers and destroys thousands of medical billing records.
- f. An employee notices that someone has been tampering with her computer, but she does not report the incident.
- g. A hospital uses an encrypted system to e-mail an organ donor's medical information to another hospital that is treating the organ recipient.
- h. All the hospital's complete patient medical records for the last ten years are accessible to the medical insurance specialist.

HIPAA Communications

1. ABC Hospital has the Policy #9 document in its Policy and Procedures manual. Study the document below and answer these questions.
 - a. What is the purpose of the policy regarding HIPAA security standards?
 - b. Name two documents that employees must sign.
 - c. What verification checks *could* be made before a person is hired by ABC Hospital? Are other verification checks possible?
 - d. Which hospital personnel are responsible for identifying the security responsibilities and supervision for the position?
 - e. Does this policy mention sanctions?

WORKFORCE CLEARANCE PROCEDURE

ADMINISTRATIVE MANUAL POLICY #9

HIPAA Security Rule Language: "Implement procedures to determine that the access of a workforce member to ePHI is appropriate."

Policy Summary

The background of all ABC Hospital workforce members must be adequately reviewed during the hiring process. When defining an organizational position, the ABC Hospital human resources department and the hiring manager must identify and define both the security responsibilities of and level of supervision required for the position. All ABC Hospital workforce members who access ABC Hospital information systems containing ePHI must sign a confidentiality agreement. All ABC Hospital employees must also sign a "conditions of employment" document that states their commitment to and understanding of their responsibility for the protection of the confidentiality, integrity, and availability of ABC Hospital's ePHI.

Purpose

This policy reflects ABC Hospital's commitment to ensure that all workforce members have appropriate authorization to access ABC Hospital information systems containing ePHI.

Policy

1. The background of all ABC Hospital workforce members must be adequately reviewed during the hiring process. Verification checks must be made, as appropriate. Verification checks include, but are not limited to:
 - Character references
 - Confirmation of claimed academic and professional qualifications
 - Professional license validation
 - Credit check
 - Criminal background check
 - Office of the Inspector General (OIG) database check
2. The type and number of verification checks conducted must be based on the employee's probable access to ABC Hospital information systems containing ePHI and their expected ability to modify or change such ePHI.
3. The extent and type of screening must be based on ABC Hospital's risk analysis process.
4. When defining a position, the ABC Hospital human resources department manager and the hiring manager must identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of ABC Hospital information systems or processes.
5. When job candidates are provided via an agency, ABC Hospital's contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds.
6. It is the responsibility of each ABC Hospital department that retains the services of a third party to ensure that the party or person(s) adheres to all appropriate ABC Hospital policies.
7. All ABC Hospital workforce members who access ABC Hospital information systems containing ePHI must sign a confidentiality agreement in which they agree not to provide ePHI to or to discuss confidential information to which they have access with unauthorized persons. Confidentiality agreements must be reviewed and signed annually by ABC Hospital workforce members who access ABC Hospital information systems containing ePHI.
8. All ABC Hospital employees must sign a "conditions of employment" document that affirms their responsibility for the protection of the confidentiality, integrity, or availability of ABC Hospital information systems and processes. The document must include the sanctions that may be applied if employees do not meet their responsibilities.

Scope/Applicability: This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information.

2. The question and response below have been circulated in an e-mail message to personnel who need to have this information. In your own words, summarize the meaning of the answer, addressing these points:
 - a. Is encryption mandatory under the HIPAA Security Rule? Why?
 - b. What kind of guidance is under discussion?

QUESTION

Is mandatory encryption in the HIPAA Security Rule?

RESPONSE

No. The final HIPAA Security Rule made the use of encryption an addressable implementation specification. See 45 CFR §§ 164.312(a)(2)(iv) and 164.312(e)(2)(ii). Covered entities use open networks such as the Internet and e-mail systems differently, and no single interoperable encryption solution for communicating over open networks exists. Setting a single encryption standard could have placed an unfair financial and technical burden on some covered entities. The encryption implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate, or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure.

RESEARCHING THE INTERNET

1. Using a web browser such as Google or Yahoo, search for and report on current information about the Federal Identity Theft Task Force. Specifically review suggestions for improved authentication procedures.
2. The National Institute for Standards and Technology (NIST) offers advice on security log management. Visit the NIST home page and locate the Computer Security Division (CSD) of NIST's Information Technology Laboratory. What is stated as the CSD's mission statement?