> **NOTE**
>
> Neither HIPAA nor the HITECH Act provides a **private cause of action**. This means that neither law gives people a right to sue a covered entity that wrongfully uses their PHI. An individual would have to use a different legal theory, such as negligence, to sue a covered entity that wrongfully uses his or her PHI.

Unsecured PHI includes PHI that isn't disposed of properly. PHI is considered unsecured during destruction if it's still readable or recoverable after disposal. PHI that is shredded or completely destroyed is disposed of properly.

Covered entities must provide notice to people who are affected by a breach of unsecured PHI. These are the people whose PHI was disclosed, or potentially disclosed, because of the breach. The covered entity must notify them no later than 60 days after it discovers the breach.[40] A breach is *discovered* on the first day that the covered entity knows about the breach. Individuals must be notified without "unreasonable delay." This means that a covered entity must notify individuals as soon as it can reasonably do so. A covered entity may delay notification if a law enforcement official requests it.

Any notice to an individual must include:

- A complete description of what happened
- A description of the PHI involved
- A description of what the covered entity is doing to mitigate the breach
- Steps the person should take to protect themselves from harm like identity theft
- Contact information for the covered entity[41]

The HITECH Act also specifies the method for notifying people of a breach of their unsecured PHI. The default way to provide notice is via first-class mail. There are other ways to provide notice in some circumstances. For example, a covered entity can provide notice via e-mail if the individual has agreed to receive communications by e-mail. If the breach involves more than 500 people, then the covered entity must also immediately notify HHS about the breach. It also must notify local media about the breach, so news outlets can help inform people. All covered entities must submit annual reports to the HHS about breaches involving less than 500 people.

Main Requirements of the Security Rule

HHS published the Security Rule in February 2003. It's an information security rule. It requires covered entities to use security safeguards. These safeguards must protect the confidentiality, integrity, and availability of **electronic protected health information (EPHI)**. EPHI is patient health information that is computer based. Covered entities were required to comply with the Rule by April 20, 2005.

Like the Privacy Rule, the Security Rule was the first time the U.S. government stated federal protections for EPHI. Under the Rule, covered entities must protect all EPHI that they create, receive, maintain, or transmit.[42] They must protect it from reasonably anticipated threats. They also must guard against uses or disclosures of EPHI that aren't allowed by the Privacy Rule.

Electronic Health Records and Personal Health Records

In January 2005, President Bush called for the creation of a nationwide network of electronic health records. He wanted this network to be created within 10 years. An *electronic health record (EHR)* refers to government-endorsed technologies that allow health care providers to store, retrieve, and share medical information. The goal of an EHR is to make paper medical records obsolete.

The HITECH Act allocates $19.2 billon to promote the adoption of EHRs. Beginning in 2011, health care professionals who use approved EHR technologies will be eligible for some types of incentives. These incentives are to help cover the cost of adopting EHR technologies. Health care providers that move too slowly to adopt EHR will not receive the incentives.

An EHR is different from a *personal health record (PHR)*. PHRs are health records that are compiled and maintained by a person. EHRs are compiled and maintained by health care providers. A PHR typically refers to individual-compiled health records in an electronic format. People can compile and store this information on their computers. They also can use applications and tools offered by third parties. Many health insurance companies give their members access to tools that allow them to compile PHRs. These tools and PHRs are specific to the health insurance plan.

Covered entities must create policies and procedures to comply with the Security Rule.[43] They must review their documents on a regular basis and update them as needed. They must provide training to their employees. They also must make security program documents available to employees in printed manuals or on Web sites. A covered entity also must have a sanctions policy to discipline workers who violate the Security Rule.

The Security Rule allows covered entities flexibility in creating their overall security program. The Rule doesn't require covered entities to use specific types of technology. In creating their program, covered entities may think about:

- The size and complexity of the entity
- Its technical infrastructure, hardware, and software security resources
- The costs of security measures
- The potential risks to EPHI[44]

NOTE

The Security Rule contains document retention requirements. Covered entities must maintain their Security Rule documentation for six years after it's created. They also must maintain old documents for six years after they're retired. The six-year time limit starts to run on whichever date (creation or retirement) is later.

Safeguards and Implementation Specifications

The Security Rule requires covered entities to use information security principles to protect EPHI. They must use administrative, physical, and technical safeguards. The Rule contains instructions on each safeguard. It also includes standards that must be implemented for each safeguard. These standards include a list of items that a covered entity must put into practice. These lists are called *implementation specifications.*

There are some implementation specifications that a covered entity must implement. These are called *required* specifications. Other specifications are *addressable.* Covered entities have more discretion when considering addressable specifications. For these specifications, it must assess whether that control is reasonable and appropriate in its environment.[45] If it is, then the covered entity must use it.

If an addressable specification isn't reasonable and appropriate, the covered entity doesn't have to use it. However, it must document why the specification was not appropriate. It also must implement an equivalent control. The equivalent control should accomplish the goal of the addressable specification.

Administrative Safeguards. Half of the safeguards required by the Security Rule are administrative in nature. These safeguards are actions, policies, and procedures that a covered entity must implement in order to follow the Security Rule.[46] There are nine different administrative requirements. A covered entity must implement the following standards:

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan
- Evaluation
- Business associate contracts

> **NOTE**
> Risk analysis and risk management are standard information security concepts. HHS issued guidance on risk analysis and assessment under the Security Rule in July 2010. You can learn more at *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html.*

The *security management process* standard guides a covered entity in creating its security program. It has four required implementation specifications. To comply with this standard, a covered entity must conduct a risk analysis and engage in risk management. It must also create a sanction policy and review information system activity.

Risk analysis is used to assess the vulnerabilities, threats, and risks that could harm EPHI. Risk management is the process of implementing controls to reduce risk. Information system activity review is the process of reviewing system logs and records. Covered entities must review them to make sure that EPHI is being used properly.

Covered entities are required to name an official responsible for Security Rule compliance. The *assigned security responsibility* standard requires this. This standard is similar to the Privacy Rule provision that requires covered entities to designate a privacy official. The privacy and security officials don't have to be the same person.

Under the *workforce security* standard, covered entities must implement need-to-know policies for EPHI access. They must make sure that all employees have appropriate access to EPHI. They also must ensure that employees without proper authority aren't able to access EPHI. There are three addressable specifications in this standard. To the extent that it's appropriate for its operations, the covered entity must implement authorization and supervision procedures. They must also implement workforce clearance and termination procedures.

Each of these specifications helps to ensure proper access to EPHI. The authorization and supervision procedures are used to make sure that an individual user has the authority to use EPHI in certain ways. Under the workforce clearance specification, a covered entity must create procedures to confirm that an employee's access to EPHI is correct. The termination procedures specification requires covered components to terminate employee access to EPHI when an employee leaves a covered entity.

The *information access management* standard is closely related to the workforce security standard. It requires covered entities to create policies to access EPHI. These policies must be consistent with the Privacy Rule. The standard has one required and two addressable implementation specifications.

The *security awareness and training* standard requires covered entities to create training and awareness programs. These programs must be for all members of its workforce. This standard has four addressable specifications. Where appropriate, the covered entity must implement password management procedures. It must also create logon monitoring procedures. Other procedures must protect against malicious software. The entity also should provide security updates to its workforce.

Under the *security incident procedures* standard, covered entities must implement policies to respond to security incidents. This standard has one required implementation specification. The covered entity must identify security incidents and respond to them. It also must attempt to mitigate the harm caused by security incidents. It also must document security incidents and their outcomes. In some cases a security incident under the Security Rule leads to unauthorized use or disclosure of PHI under the Privacy Rule. In these cases, the Privacy Rule might require covered entities to notify the individuals affected by the breach.

> **NOTE**
>
> Under the Security Rule, a security incident is unauthorized access or use of information. It can be successful unauthorized access or just attempted unauthorized access. Incidents also include interference with the operation of information systems.[47]

The *contingency plan* standard requires covered entities to develop policies to recover access to EPHI in the event of an outage or disaster. This standard contains three required and two addressable specifications. It requires covered entities to prepare data backup, disaster recovery, and emergency operation plans. Together the plans

state how an organization backs up and restores its EPHI. The emergency operations plan requires covered entities to protect EPHI when it's operating in emergency mode. Where reasonable, the covered entity must also create procedures to test and review its contingency plans.

The *evaluation* standard requires the covered entity to review its security safeguards program. It must regularly review changes to its information systems and practices. It must make sure that its safeguards still protect EPHI. The covered entity can perform this evaluation on its own. It also can hire external organizations to conduct this review.

> **TIP**
>
> Remember that under the Security Rule, a covered entity must apply an addressable implementation specification if it's reasonable. It must also be appropriate. A covered entity must document why it doesn't implement one of these types of specifications. It must then implement an equivalent control if possible.

The *business associate contracts* standard requires covered entities make sure that their business associates protect EPHI. Covered entities must enter into written contracts with any organizations that use EPHI on their behalf. These are called business associates agreements. Business associates agreements are required under both the Privacy and Security Rules. A covered entity must identify all of its business associates. It also must make sure that it has contracts will all of them.

Table 6-2 summarizes the administrative safeguards required by the Security Rule. It also includes a summary of required and addressable implementation specifications.

Physical Safeguards. Physical safeguards are controls put in place to protect a covered entity's physical resources. These measures protect information systems, equipment, and buildings from environmental threats. The Security Rule contains four physical security standards. A covered entity must put into practice the following standards:

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

Under the *facility access controls* standard, covered entities must implement policies that limit physical access to their computer systems. They must limit access to the buildings where these systems are located. Only authorized individuals should be allowed to access these systems and facilities. This standard has four addressable implementation specifications.

Where appropriate, the covered entity must create access contingency plans. These plans allow access to facilities and systems during emergencies. A covered entity also must create a facility security plan. This plan is designed to protect systems and buildings from unauthorized access, tampering, and theft. When it seems appropriate, covered entities must create access control and validation procedures. They should include measures to manage visitor access. They also should document repairs and modifications to a facility.

TABLE 6-2 Administrative safeguards.

SAFEGUARD	REQUIRED SPECIFICATIONS	ADDRESSABLE SPECIFICATIONS
Security Management Process	Risk Analysis Risk Management Sanction Policy Information System Activity Review	
Assigned Security Responsibility	Required	
Workforce Security		Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures
Information Access Management	Isolating Health Care Clearinghouse Function	Access Authorization Access Establishment and Modification
Security Awareness and Training		Security Reminders Protection from Malicious Software Logon Monitoring Password Management
Security Incident Procedures	Response and Reporting	
Contingency Plan	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan	Testing and Revision Procedure Applications and Data Criticality Analysis
Evaluation	Required	
Business Associate Contracts and Other Arrangements	Required	

> **NOTE**
> Under the Security Rule, a workstation is a computing device and any electronic media used by or around the device. Examples include a laptop or desktop computer or any similar device.[48]

The Security Rule contains two standards related to workstation security. Both standards are required. Neither standard has implementation specifications. In the *workstation use* standard, a covered entity must make sure that employees use workstations properly. This means that it should review the applications used on work-stations. It must review whether those applications introduce security risks that could harm EPHI. For example, a covered entity might decide that it's too risky to allow workstations used to access EPHI to connect to the Internet. The covered entity must look at workstation use for both on-site and off-site locations.

According to the *workstation security standard* covered entities must implement physical safeguards for workstations that access EPHI. The covered entity must make sure that access to the workstation is restricted to authorized users. A covered entity might protect workstations by keeping them in areas that only authorized employees are allowed to access.

Under the *device and media controls* standard, a covered entity must track information systems containing EPHI. They must track these systems in and out of a facility. They also must track system movement within a facility. This standard has two required and two addressable implementation specifications.

Under this standard, a covered entity is required to create media disposal and media reuse policies. Covered entities must make sure that EPHI is destroyed or made unusable before the covered entity disposes of electronic media. The process for accomplishing this is described in a media disposal policy. A covered entity must also create media reuse policies. These policies state that EPHI must be removed from electronic media that is going to be made available for reuse. These policies must take into account media reuse within a covered entity. They also should address media reuse outside of a covered entity.

Table 6-3 summarizes the physical safeguards required by the Security Rule. It also includes a summary of required and addressable implementation specifications.

Technical Safeguards. Technical safeguards are applied in the hardware and software of an information system. The Security Rule contains five technical security standards. It doesn't require that any specific type of technology be used to follow the rule. A covered entity must implement the following standards:

- Access controls
- Audit controls
- Integrity controls
- Person or entity authentication
- Transmission security

TABLE 6-3 Physical safeguards.

SAFEGUARD	REQUIRED SPECIFICATIONS	ADDRESSABLE SPECIFICATIONS
Facility Access Controls		Contingency Operations Facility Security Plan Access Control and Validation Procedures Maintenance Records
Workstation Use	Required	
Workstation Security	Required	
Device and Media Controls	Disposal Media Reuse	Accountability Data Backup and Storage

The *access control* standard requires covered entities to use access control rules to limit authorized access to systems that store EPHI. The implementation specifications require covered entities to assign unique user names to anyone who uses its systems. They also must create procedures to access EPHI in an emergency. Addressable specifications include using automatic logoff processes. These processes end an electronic session after a period of inactivity. A covered entity also should encrypt EPHI. Together these controls limit access to EPHI.

The *audit controls* standard requires covered entities to review activity in information systems that store or use EPHI. The entity must decide what audit controls it needs to implement to protect its EPHI. Audit controls are used to look for unauthorized access.

The *integrity controls* standard requires covered entities to create policies to protect EPHI from improper modification or destruction. This is an important control to protect EPHI. Health care providers rely on EPHI to treat patients. EPHI that has been improperly modified can put a patient in danger. This standard has one addressable specification. When it's appropriate, covered entities must authenticate EPHI. These are electronic mechanisms that are used to make sure that EPHI hasn't been improperly changed or destroyed.

Covered entities are required to create procedures to verify that a person or entity trying to access EPHI is who they claim to be. This is the *person or entity authentication* standard. People and entities must prove their identities. Authentication credentials are used to ensure that a person is who they claim to be. These credentials include passwords, tokens, smart cards, and biometric credentials.

TABLE 6-4 Technical safeguards.

SAFEGUARD	REQUIRED SPECIFICATIONS	ADDRESSABLE SPECIFICATIONS
Access Control	Unique User Identification Emergency Access Procedure	Automatic Logoff Encryption and Decryption
Audit Controls	Required	
Integrity		Mechanism to Authenticate Electronic Protected Health Information
Person or Entity Authentication	Required	
Transmission Security		Integrity Controls Encryption

The *transmission security* standard requires covered entities to guard against unauthorized access to EPHI during transmission. A covered entity must review how it transmits EPHI. It must determine if there is a risk of unauthorized access. This standard includes two addressable specifications. Where appropriate, the covered entity must implement security measures that protect EPHI from being modified during transmission. It also must encrypt EPHI during transmission if appropriate.

Table 6-4 summarizes the technical safeguards required by the Security Rule. It also includes a summary of required and addressable implementation specifications.

The Security Rule and safeguards requirements are designed to protect all sorts of EPHI. HHS recognizes that sometimes covered entities might need more guidance as technology quickly evolves. For example, HHS has issued guidance to help covered entities secure mobile devices. It has also issued guidance to help covered entities securely access remote EPHI.

FYI

Covered entities have great incentive to encrypt EPHI. This incentive exists even though many Security Rule implementation specifications do not require encryption. The incentive exists because the breach notification requirement of the Privacy Rule does not apply to the unauthorized use or disclosure of encrypted EPHI. A covered entity thus saves itself from this requirement if it encrypts its EPHI.

FYI

Since 2003, the OCR has received over 87,000 Privacy Rule complaints. As of November 30, 2013, it had received 759 Security Rule complaints.

A flowchart of the OCR complaint process is available at *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process*.

Oversight

HHS oversees compliance with the HIPAA Privacy and Security Rules. It delegated this function to the Office for Civil Rights (OCR). The OCR enforces both rules. It's also responsible for protecting people from discrimination in social services programs.

OCR has enforced the Privacy Rule since the 2003 compliance date. It began enforcing the Security Rule in July 2009. Before that, the Centers for Medicare and Medicaid Services (CMS) enforced the Security Rule. CMS is also a part of HHS.

The HITECH Act changed many of the oversight and enforcement functions for HIPAA. It required HHS to improve how it enforced the Privacy and Security Rules. To do this, Secretary of Health and Human Services delegated Security Rule enforcement to the OCR. This change eliminated duplicate rule enforcement. HHS hopes to be more efficient by having one office enforce both rules.

The OCR can fine covered entities that don't comply with the Privacy and Security Rules. The maximum fine for a Security or Privacy Rule violation is $1.5 million per year. Minimum fines range from $100 to $50,000 per violation. The penalty amount is determined by reviewing the nature of the violation. OCR also will weigh how the covered entity responded to the violation when it determines a fine.

NOTE

HHS must bring an enforcement action against a noncompliant covered entity within six years of the date of the violation.[49]

A person may be subject to criminal liability if he or she obtains or discloses PHI in violation of HIPAA. The HITECH Act clarifies that any person who wrongfully obtains or discloses PHI can be held criminally responsible. This includes a covered entity, its employees, or any other person. A person must know that their conduct is wrongful under HIPAA. The U.S. Department of Justice handles HIPAA criminal violations.

The HITECH Act allows states to enforce HIPAA compliance. States did not have this authority before. State attorneys general can stop covered entities from engaging in

FYI

HHS maintains statistics on HIPAA enforcement actions. You can learn more about the enforcement process, see statistics, and read about enforcement cases at *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/*.

practices that harm state residents and compromise their PHI. They also can recover damages on behalf of state residents who are harmed by a covered entity's conduct. The first state to use this new enforcement power was Connecticut.

The Role of State Laws Protecting Medical Records

HIPAA sets the floor for PHI security and privacy protections. This means that states are free to create laws and rules that provide more protections than HIPAA. Covered entities have to comply with both laws. Generally speaking, the controlling law is whichever law is stricter, or provides greater patient rights.

Any state law that is contrary to HIPAA isn't allowed. A state law is contrary if it's impossible for the covered entity to comply with both the state law and HIPAA. In these situations, the state laws are preempted by HIPAA. They are not allowed.

States enact many laws that may affect personal health information. These laws can provide more rights than allowed by HIPAA. For instance, in 2008 California enacted some of the strictest patient privacy protections in the country. California's laws specify harsh penalties for providers caught snooping in patient medical records. California health care providers must report privacy breaches more quickly than is specified in HIPAA. The California law requires health care providers to notify people within five days of a breach of a patient's medical information.[50] It also gives people the right to sue their health care providers for violations of the law.

It's important to review both state law and federal law when reviewing questions about the security and privacy of personal health information. You must review both types of laws to make sure that covered entities are appropriately protecting this information.

Case Studies and Examples

The following case studies show how the laws discussed in this chapter are used. These case studies are real-world examples of how regulatory agencies apply laws and rules to protect personal health information.

OCR Enforcement Information

The OCR posts HIPAA Privacy and Security Rule enforcement news on its Web page. It posts summaries of enforcement activities. It also posts monthly statistics about its activities. It also posts case examples and resolution agreements for HIPAA violations.

The OCR enforcement activities Web page can be found at *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/*.

HIPAA and Federal Trade Communications Act

Sometimes an act can touch several compliance laws. In 2006, an Indianapolis, Indiana, television news station conducted an investigative report on prescription privacy. As part of its report, the news station looked at the contents of pharmacy dumpsters.

It was checking to see if pharmacies properly disposed of patient information. It checked the contents of unsecured dumpsters. These dumpsters were unlocked. There was nothing stopping the public from sifting through these dumpsters.

The news station reported that CVS pharmacies were throwing sensitive personal information in the trash. CVS is one of the largest pharmacy retailers in the United States. It has more than 6,000 stores. The investigation found that CVS was throwing away unredacted pill bottles. Information on the bottles included patient names, addresses, physician names, and the names of medication. CVS also threw away medication instruction sheets containing personal information. It threw away pharmacy receipts with credit card and health insurance account numbers. All of this information was PHI. All of it was unredacted. Other media outlets reported that CVS stores across the United States also were improperly disposing of PHI.

Information about the "Prescription Privacy" investigative report can be found at *http://www.wthr.com/global/Category.asp?c=83157.*

At the time, CVS's privacy policy stated: "CVS/pharmacy wants you to know that nothing is more central to our operations than maintaining the privacy of your health information ('Protected Health Information' or 'PHI'). PHI is information about you, including basic information that may identify you and relates to your past, present, or future health or condition and the dispensing of pharmaceutical products to you. We take this responsibility very seriously."

CVS disposal practices were investigated by the HHS and the Federal Trade Commission. It was the first time that HHS and the FTC worked together on an investigation. HHS, through the OCR, investigated CVS for violations of the HIPAA Privacy Rule. It found that CVS violated the Privacy Rule in a number of ways. Its review indicated that CVS didn't properly safeguard PHI during the media disposal process. It also found that CVS didn't properly train its employees on how to dispose of PHI. CVS also didn't have a sanctions policy.

The FTC investigated CVS for violations of the FTC Act. It alleged that CVS made false and deceptive statements about its privacy policies. It alleged that CVS promised customers that it would protect unauthorized access to personal information. It also alleged that CVS didn't actually do this. These misleading types of statements are illegal under the FTC Act.

CVS responded that there was no verification of the media reports. However, it settled charges with the FTC and HHS to resolve the cases. The FTC consent agreement requires CVS to create a comprehensive information security program. This program must protect the personal information that CVS collects from consumers and employees. The order also requires CVS to get an independent audit of its security program every two years. It must do this until 2029. CVS may not make any misrepresentations about the company's security practices.

The FTC complaint and consent agreement can be found at *http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2009/06/matter-cvs-caremark-corporation-corporation.* (Look for the February 18, 2009, entries.)

NOTE

An HHS resolution agreement is similar to an FTC consent order. Both are settlement agreements.

Under the HHS resolution agreement, CVS agreed to pay $2.25 million to settle all claims. It also agreed to follow a corrective action plan. That plan requires it to create policies to comply with the HIPAA Privacy Rule. It must create policies and procedures to safeguard PHI during disposal. It also must establish an employee training program. CVS also must create an employee sanctions policy to discipline employees who fail to follow the Privacy Rule.

The HHS resolution agreement also requires independent review of CVS compliance. CVS must be reviewed each year. The agreement requires three years of monitoring.

The HHS resolution agreement and corrective action plan can be found at *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html*.

CHAPTER SUMMARY

Personal health information is one of the most sensitive types of confidential information. Personal health information is no longer limited to paper files. This type of information is often stored in electronic form. No matter what its form, this information must be protected.

Health care providers must take steps to ensure its privacy and security. They are required to do so by both federal and state laws. They face fines and other penalties for failing to protect this information.

KEY CONCEPTS AND TERMS

Authorization
Business associates
Covered entity
Disclosure
Discovery
Electronic protected health information (EPHI)
Medical identity theft
Minimum necessary rule
Private cause of action
Protected health information (PHI)
Use