CHAPTER 6

# Security and Privacy of Health Information

HEALTH INFORMATION CAN BE USED in a number of different ways. Doctors and other health care professionals use and share it to provide medical care. Insurance companies and employers share it for insurance coverage and payment. Many people worry that this type of information could be used improperly, as well as for valid uses. Insurance companies could use it to deny health care coverage. Employers could use it to decide not to hire someone. Thieves could steal medical information and use it to commit medical identity theft.

Health care providers no longer store health information just in paper files. Many providers use computer systems to create and store electronic health records. When information is stored electronically, data may be combined from a number of different sources. It's possible to create comprehensive medical records that contain a lot of data about a person. The health care industry must take steps to secure these types of records.

This chapter focuses on laws that protect the privacy and security of health information. For the most part this chapter focuses on the unique challenges presented by growing amounts of electronic health information. This chapter also discusses how federal and state laws work together to protect this information.

## Chapter 6 Topics

This chapter covers the following topics and concepts:

- What the business challenges facing the health care industry are
- Why health care information is sensitive
- What the Health Insurance Portability and Accountability Act is
- What the role of state law in protecting medical records is
- What some case studies and examples are

## Chapter 6 Goals

When you complete this chapter, you will be able to:

- Describe the business challenges facing the health care industry
- Explain why health care information is sensitive
- Explain the main parts of the Health Insurance Portability and Accountability Act
- Describe the role of state law in protecting the confidentiality of medical records

## Business Challenges Facing the Health Care Industry

The health care industry faces many of the same privacy and security challenges as other industries. The difference is the type of data that is used. The health care industry collects consumer financial and personal health information. Health care providers collect consumer financial information to make sure that consumers pay for medical goods and services. They collect health information to provide these goods and services. Many people consider health information to be very sensitive.

The health care industry often collects and stores this data in electronic form. It's collected from a number of sources. Hospital computer systems contain notes from hospital employees and primary care physicians. Health insurance companies collect and combine patient data from different providers. It's important for organizations to maintain the security of computer systems that hold health data. Patients demand that this data be protected. Unfortunately, health information often is compromised in data breaches. This can cause problems for health care consumers.

**NOTE**

In November 2009, Health Net of the Northeast, Inc. reported that 1.5 million patient records were affected when it lost an external hard drive. The hard drive also contained the personal information of physicians who participated in its network. The data was not encrypted. Health Net paid large fines to the states of Vermont and Connecticut to settle allegations that it violated federal laws that protected patient records.

Health information can be exploited and used improperly. One such crime is medical identity theft. **Medical identity theft** is a specialized type of identity theft. In medical identity theft, thieves steal a person's name and other parts of his or her medical identity. They use this information to get medical services or goods. When the thief gets health care, providers could add treatment notes about the thief on the victim's medical record. A thief can use personal information obtained from health records to steal health insurance information and make a false claim for health care services. Unpaid medical charges could end up on the victim's credit report.

**FYI**

A 2013 study by the Ponemon Institute estimated that victims of medical identity theft pay, on average, almost $19,000 in costs linked to the theft.

Medical identity thieves are not only computer hackers or members of organized crime rings. Health care providers such as doctors, dentists, and hospital employees also can be identity thieves. In 2003, an employee at a cancer center stole the identity of a center patient. The identity thief was sentenced to 16 months in prison and ordered to pay restitution.

**NOTE**

A judge orders defendants to pay restitution. It's paid to victims to compensate them for damages related to a crime.

In 2006, a desk clerk at a Florida clinic stole the health information of more than 1,000 patients. The clerk sold the data to another person. That person used the data to submit almost $2.8 million in fraudulent Medicare claims to the U.S. government. After trial, the court sentenced the person who submitted the fraudulent claims to seven years in prison. The court ordered the person to pay $2.5 million in restitution. The court sentenced the desk clerk to three years of probation for her part in the crime. She also had to pay $2.5 million in restitution.

Medical theft is very serious. It can damage a victim's finances with false insurance claims for services. Like regular identity theft, victims must spend time and money resolving payment disputes and credit issues. It also can affect a victim's future medical care. If a thief's medical information becomes a part of the victim's medical record, the victim may not qualify for medical insurance benefits.

Medical identity theft also can harm a person's physical safety. In this crime, health care providers enter diagnoses and treatment notes about the identity thief onto a victim's medical record. If doctors rely on those false notes later, they could give a victim an erroneous diagnosis. If false health information concerns life-threatening conditions, a victim could even be killed by an incorrect course of treatment.

Medical identity theft is a problem because it can be hard to correct false information in a medical record. Since health information is shared electronically for a number of purposes such as treatment and payment, it can be hard to determine all of the places where false information must be corrected.

## Why Is Health Care Information So Sensitive?

Most people consider their medical information to be among the most sensitive types of personal information. It's because this information can be full of private details that people don't want to share. People must share these details with health care providers to receive treatment. Providers include this information in medical records. These records

contain information on diagnoses, lab results, and treatment options. They also contain information about chronic conditions or mental health counseling. They also hold private details about a person's lifestyle.

Doctor/patient confidentiality is a long-held tradition. The Hippocratic Oath, which dates back to the 4th century B.C.E., recognizes this belief. The Hippocratic Oath is a pledge that many medical school students recite upon their graduation. The traditional version of the oath states: "Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."[1] The statement means that a doctor will keep the patient's health secrets.

Health records often contain intimate details about a person. People fear that they will be embarrassed if their health information isn't kept secret. Some people may even fear for their lives if particularly intimate facts, such as reasons for health counseling, are disclosed. People fear that others may discriminate against them. They fear that insurance companies or employers could reject them because of information in their health records. For instance, people who have been treated for anxiety or high blood pressure in the past might fear that their application for private life insurance will be denied. People with a known genetic predisposition for certain types of diseases might fear that they will be denied health insurance.

The U.S. government recognizes the special sensitivity of some medical records. The Drug Abuse Prevention, Treatment, and Rehabilitation Act of 1980[2] protects patient information about alcohol or drug abuse. This law applies to any federally assisted alcohol or drug abuse treatment program. It states that these programs may not disclose patient information without consent. There are very few exceptions to this rule. Patient information can be disclosed without consent only in limited situations. A treatment program may disclose patient information in a medical emergency or to report child abuse.

People often feel as if they have little control over where their health information is shared. This is a privacy concern. Providers share health information for treatment purposes. It's also shared with government agencies if payment is made through

**FYI**

The MIB Group, Inc. is an industry group that helps protect against fraud. Members of the group are U.S. and Canadian insurance companies. Group members share information about life, health, and long-term care insurance applicants. They share this information to make sure that applicants don't conceal or hide certain types of health information. Insurance companies need some of this information to determine whether a person is insurable. This helps avoid fraudulent insurance applications and claims. MIB members share this information in a coded format to protect privacy. The MIB is subject to a number of U.S. security and privacy laws. These include the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and Canadian privacy legislation. To learn more about the MIB, visit *http://www.mib.com*.

government programs such as Medicaid or Medicare. It's also shared with insurance companies. Insurance companies sometimes ask for health insurance records to make decisions about whether a person is a suitable risk for life or health insurance. These records are shared in court cases, particularly if a plaintiff claims an injury in a lawsuit. They are used to prove that a defendant caused the plaintiff's injury and is liable for that injury.

People can do very little to mitigate an improper disclosure of their health information. They may feel a social stigma if certain facts are shared indiscriminately or exposed in a data breach. There are few ways to correct that stigma. For instance, people recovering from substance abuse might not want other people to know. They may be concerned that society will judge them unfairly for their past substance abuse. They may be concerned about being denied employment or other opportunities. They may worry that they could be prosecuted for using illegal substances. No amount of money or fines assessed against a provider who improperly discloses this information can compensate a patient for such embarrassment or fear. People can't be instructed to "forget" this type of information once they hear it.

The federal government recognizes that health information is highly sensitive. The Health Insurance Portability and Accountability Act is the best-known U.S. law protecting the security and privacy of health information.

## The Health Insurance Portability and Accountability Act

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. It created the law to help make health insurance portable. HIPAA is used to fight health insurance fraud and eliminate waste. It also simplifies how health insurance is administered.

### Purpose

> **NOTE**
> *Job lock* refers to situations where workers feel locked into their jobs. They're afraid they will lose their employer-provided benefits if they leave.

HIPAA is best known for its rules that protect the privacy and security of personally identifiable health information. These terms are part of the law's "Administrative Simplification" requirements. While these rules are the focus of this chapter, it's important that you know that HIPAA has other provisions as well. They were enacted so that health insurance could be *portable*, or carried from one employer to another. Prior to HIPAA, some workers felt that they were stuck in a job because they feared they would lose their health insurance if they changed jobs.

HIPAA protects health care coverage when workers change jobs. It protects both workers and their families. It forbids a new employer's health plan from denying coverage for some reasons. It prohibits employers from discriminating against workers based on certain conditions, such as pregnancy. It also limits employer-provided health plans from using pre-existing conditions as reasons for excluding workers from the plan.

## Other Laws Affecting Health Care in the United States

The focus of this chapter is the Health Insurance Portability and Accountability Act (HIPAA). This is the law that most comprehensively addresses the protection of health care information. However, there are a number of laws that affect health care in the United States. You hear about these laws every day. This is because health care is very important to most people. Two other laws that you may hear about are the HITECH Act and "Obamacare."

In February 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[3] The HITECH Act is part of the American Recovery and Reinvestment Act (ARRA) of 2009. ARRA is a $787 billion stimulus package. President Obama signed it into law on February 17, 2009. ARRA contains incentives that encourage the adoption of health care information technologies. It anticipates an increase in the use and exchange of electronic protected health information (EPHI). Because of this, the HITECH Act strengthens HIPAA privacy and security protections for PHI.

The Health and Human Services (HHS) rules implementing the HITECH Act took a long time to create. They were published in January 2013. The HITECH Regulations were effective March 26, 2013. Compliance was required by September 23, 2013. The HITECH Act and HHS regulations made major changes to the steps that health care providers must take to protect the privacy and security of health information. They are the most sweeping changes to HIPAA since the law was created.

The HITECH Act also created a federal breach notification law for health care information. This means that health care providers must notify people if their health information is involved in a security breach. Sometimes the HITECH Act's provisions will be highlighted in the text of this chapter because it represented such a large change to original HIPAA legislation.

The Affordable Care Act of 2010 (ACA) was enacted in 2010.[4] This act is sometimes referred to as "Obamacare." The ACA created comprehensive health care reforms in the United States. The ACA's goal was to increase access to health care and lower the cost of health care. The main requirement of the ACA is that individuals, the government, and employers have a shared responsibility to meet health care needs. Under the law, individuals must obtain health insurance. Employers have to provide health insurance to most employees. The government has to create health marketplaces where individuals can buy health insurance if they need it. The law also contains provisions and incentives to improve health care information technology in the U.S.

The ACA was quickly challenged. Opponents of the law argued that some of its provisions were unconstitutional. Specifically, they argued that requiring individuals to purchase health care was unconstitutional. In June 2012, the U.S. Supreme Court upheld that provision of the law.

HIPAA, HITECH, and the ACA all work together to address various aspects of health care, funding, and insurance in the United States. The interplay between all of these acts is very complex.

### The Difference between COBRA and HIPAA

Often the words COBRA and HIPAA are used when discussing continuing health benefits following job loss or resignation. While both laws work together to help protect employees and their health benefits, they have different functions.

COBRA is the Consolidated Omnibus Budget Reconciliation Act of 1986.[5] COBRA allows some types of employees (and their families) to continue their health coverage when they change or lose a job. COBRA is usually more expensive than health coverage under the employer's plan. It is usually less expensive than individual coverage through a private health insurance company.

COBRA covers employer-provided health plans that have 20 or more employees. It also applies to health coverage offered by federal, state, and local governments. Former employees qualify for COBRA if they leave a job voluntarily. They also are eligible for COBRA if they are terminated for any reason other than gross misconduct. To be eligible for COBRA, a former employee must have been enrolled in an employer's health plan at the time of separation from the job.

When employees leave their job, they must receive a notice from their employer about COBRA eligibility. Former employees who qualify are entitled to health coverage that is the same as they had while they were employed. Under COBRA, former employees must pay their own health insurance premiums. This includes any amount a former employer might have previously paid on the employees' behalf. COBRA benefits usually last for a maximum of 18 months.

COBRA lets employees continue to get health coverage that they had through an employer for a certain period of time. HIPAA, on the other hand, makes sure that an employee is not discriminated against in new health coverage because of health history and pre-existing conditions.

A *pre-existing condition* is a health condition that existed before a person applies for a medical or other insurance policy. Insurance companies have different ways of dealing with these types of conditions. Some may provide only partial coverage for them. Others may not cover them at all. Some companies may cover the condition only after a certain period of time has passed.

HIPAA protects workers in group health plans. Employers that offer health insurance coverage typically offer these types of plans. HIPAA doesn't require that employers offer health coverage. If they do, however, HIPAA applies. Most of HIPAA's rules apply to situations when workers change jobs or move from one group health plan to another. This is the "portability" portion of the law. HIPAA doesn't apply to situations where a worker had no health coverage at all and then gets a job with health care coverage.

HIPAA's pre-existing condition rules are very important. They help prevent job lock. They also promote mobility. HIPAA limits pre-existing condition exclusions in two ways. First, it allows employer-provided health plans to look back only six months for pre-existing conditions. A condition counts as pre-existing only if a worker received treatment for it sometime over the six months prior to enrolling in a health plan. If a worker didn't receive treatment for the condition in those six months, then the condition isn't pre-existing.

The second limitation applies to conditions that are determined to be pre-existing. HIPAA limits the amount of time that employer-provided health plans can force a worker to "sit out" of coverage because of these conditions. Prior to HIPAA, health plans could force workers with pre-existing conditions to do without coverage for those conditions for a very long time. In most instances, HIPAA limits this waiting period to 12 months. That period can be shortened in many situations.

HIPAA also provides some protection against discrimination based upon genetic testing results. HIPAA states that the results of these types of tests alone can't be considered a pre-existing condition. There must be an illness diagnosis to trigger a pre-existing condition. This rule is very important as more people become aware of their genetic histories. Genetic testing is used to determine if a person is more likely to have some illnesses or diseases. This information is very sensitive. Under HIPAA, a woman who has been genetically tested and has the breast cancer gene can't be denied coverage in an employer-provided health plan if she hasn't been diagnosed with breast cancer. Just having the gene can't be considered a pre-existing condition.

Other HIPAA provisions were aimed at improving U.S. health care. These provisions are called the "Administrative Simplification" provisions. They were designed to encourage "the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[6] As part of these provisions, HIPAA required the Department of Health and Human Services (HHS) to make rules regarding the privacy of individually identifiable health information. HHS was also required to create security standards to protect this information. This chapter addresses the Privacy and Security rules.

**FYI**

The Genetic Information Nondiscrimination Act of 2008[7] protects against some types of genetic testing discrimination. It states that health insurance companies can't use genetic testing results to make eligibility decisions about a healthy person. They also can't use that information to determine the cost of premiums. The law also states that employers can't use genetic information when making hiring, firing, or other job decisions. It bars employers or health insurance plans from requiring genetic testing.

**NOTE**

PHI includes notes that your doctor puts in your medical record. It also includes any conversations your doctor has with anyone else about your health care. Billing information for health care goods and services provided to you is PHI. Information that your health insurance company has about your health care may also be PHI.

## Scope

HIPAA's Privacy and Security Rules apply to covered entities. The rules tell covered entities how they may use protected health information. Under HIPAA, **protected health information (PHI)** is any individually identifiable information about the health of a person. This includes mental and physical health data. PHI includes past, present, or future information.[8] It also includes information about paying for health care. PHI can be in any form. It's commonly considered to be all information that is put in a person's medical record.[9] The one exception to PHI is that it does not include information about individuals who have been dead for more than 50 years.

HIPAA requires covered entities to handle PHI in certain ways. The law defines covered entities. They include health plans, health care clearinghouses, and any health care provider that transmits certain types of health information in electronic form.[10]

A *health plan* is an individual or group plan that pays for medical care. It includes group health plans of more than 50 people, a health insurance issuer, and health maintenance organizations (HMOs). The government's Medicare and Medicaid programs are health plans. Military health care programs are also health plans. All health plans must follow HIPAA.

Many workers receive health insurance through their employers. These plans help provide medical care for workers and their families through insurance or reimbursement. These are group plans. The workers and their families are the "group" that is being insured.

A *health care clearinghouse* is an organization that processes health information that is in a nonstandard format. HIPAA requires that some health care electronic transactions be conducted in electronic format. HHS specifies these formats. Some health care providers may not conduct these transactions electronically. If they don't, they might enter into contracts with other organizations called clearinghouses. Clearinghouses handle the electronic transactions on the provider's behalf. They include billing services or repricing companies. They facilitate business operations between health care providers and insurers. A clearinghouse is covered by HIPAA because it conducts electronic health care transactions.

A *health care provider* is a covered entity under HIPAA. A **covered entity** is any health plan, health care clearinghouse, or health care provider that transmits certain types of health information in electronic form. The HIPAA Security and Privacy Rules "cover" them. An entity is covered if it provides health care and if it shares certain types of information electronically. This is a two-part test. A health care provider is a person or organization that provides health care services. This includes preventive and diagnostic physical care. It also includes mental health counseling and services. In short, a provider performs all activities traditionally associated with health care. Providers include doctors and clinics, dental practices, and pharmacies.

**FYI**

The Department of Health and Human Services provides tools to help entities determine whether they are covered by HIPAA. Those tools are available at *http://www.hhs.gov/ocr/privacy/*.

Even if an entity provides health care, it may not be a covered entity. A health care provider is only a covered entity under HIPAA if it shares certain types of information electronically. HHS calls the information that is shared a *standard transaction*. A standard transaction is an electronic exchange of information for health care activities that falls within defined categories. If a health care provider electronically shares information that falls within a category, then it must share it in a particular way.

HHS has defined some standard transactions. It also determines the format requirements for each standard. These formats provide efficiency in processing health care data. Some HHS standard transactions include information related to:

- Billing and claims payment
- Health plan eligibility
- Enrollment and disenrollment in a health plan
- Health plan premium payments

HIPAA also applies to the **business associates** of covered entities. A business associate is an organization that performs a health care activity for a covered entity. Covered entities may outsource some health care functions to other organizations. If these functions include using PHI, then they are business associate functions. Common business associate functions include claims and billing processing. They also can include quality assurance review if it involves the use of PHI. Legal services can even be business associate activities when those services require the use of PHI.

Business associates didn't have to follow HIPAA when the law was first passed. HHS couldn't require them to follow the HIPAA Privacy and Security Rules. This changed when Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009. Under the HITECH Act, business associates must specifically follow the HIPAA Privacy and Security Rules.[11] HHS may now directly require business associates to comply with HIPAA. It can also audit business associates to make sure that they are complying with the law. It can directly impose penalties on noncompliant business associates. Today business associates are held to the same standard as covered entities.

Covered entities that use PHI must follow the HIPAA Privacy and Security Rules. The Privacy Rule dictates how covered entities must protect the privacy of PHI. The Security Rule states how they must protect the confidentiality, integrity, and availability of electronic PHI.

## Main Requirements of the Privacy Rule

HHS published the final Privacy Rule in December 2000. It was first modified in August 2002. In January 2013, HHS published regulations implementing the HITECH Act that made changes to many portions of the Privacy Rule. Initial compliance with the Privacy Rule was required in April 2003. The Privacy Rule is the first time the U.S. government has specified federal privacy protections for PHI. The HHS said that the Privacy Rule had three main purposes:

- To allow consumers to control the use of their health information. This includes providing consumers with a way to access their health information.
- To improve health care in the U.S. by restoring consumer trust in the health care system.
- To create a national framework for health privacy protection.[12]

Under the Privacy Rule, covered entities may not use or disclose people's PHI without their permission. The Rule specifies situations where use or disclosure is allowed. The term **use** refers to how a covered entity shares or handles PHI within its organization. Use refers to how employees of a covered entity might handle PHI to provide health care. **Disclosure** refers to how a covered entity shares PHI with other organizations that may not be affiliated with it. A person must specifically consent to a use or disclosure that isn't permitted by the Privacy Rule.

The Rule also requires covered entities to put safeguards in place to protect a person's PHI. Covered entities must limit how their employees use and access PHI. They also must create training programs for their employees on how to protect PHI.

### Required Disclosures

Under the Privacy Rule, there are only two situations in which a covered entity must disclose PHI. The first is when a person requests access to his or her PHI. Under the Privacy Rule, people have the right to access, review, and get a copy of their PHI. They also have the right to request that their PHI be sent directly to a third party. This right to access PHI extends to records held by a covered entity that are used to make decisions about that person. It includes PHI held in medical records, billing information, and insurance claim information.

The Privacy Rule recognizes that people may not be able to request their own PHI for some reason. The rule allows people who are legally authorized to act for another to request PHI on that person's behalf. For instance, parents can request the PHI of their minor children. A *minor* child is one who is under the age of legal adulthood. The age of legal adulthood is determined on a state-by-state basis. For most situations in the U.S., a minor is a person under the age of 18.

Covered entities must respond to a person's request to access PHI within a specific period. The rule requires covered entities to respond in 30 days. This period can be extended to another 30 days with written notice to the requestor.[13] Additional extensions of time are allowed in some instances. A covered entity may charge a reasonable fee for copying the records and sending them to the requestor. If the records are maintained in an electronic format, then requestors have the right to receive their records in that electronic format.

There are some types of PHI that a covered entity doesn't have to provide. They don't have to provide it even if a person specifically requests it. If a covered entity chooses to deny access to PHI, then it must specify in writing why it's denying access. It should explain the reason for the denial and how to appeal the denial.

**NOTE**

A covered entity may not charge people requesting access to their PHI a storage retrieval fee. The Privacy Rule specifically doesn't allow these fees. However, a covered entity may charge for labor and supplies needed for copying the records. It also may charge for postage and any electronic media needed to provide the records.

Some types of PHI access denials are not appealable. People can't challenge a covered entity's decision to deny access to PHI in some of the following situations:

- Information that is compiled in anticipation of a lawsuit
- Psychotherapy notes
- Any information release that would be denied under the Privacy Act of 1974
- Any information that prisons compile on inmates. The covered entity must conduct a risk assessment about the risks of providing access prior to issuing a denial.

A covered entity may choose to deny a person access to his or her PHI. It may do this if it believes that the PHI requested is reasonably likely to endanger the life or physical safety of the person requesting the PHI. They may also deny access if they believe that the access could cause substantial harm to another person. A person may appeal this decision. A licensed health care professional who didn't participate in the original decision to deny access will review the appeal.[14]

The second type of situation where a covered entity must disclose PHI is when HHS is investigating the covered entity.[15] HHS investigates covered entities to make sure that they are following the Privacy Rule. A person may file a complaint with HHS if they believe that a covered entity isn't properly handling PHI. HHS is allowed to access PHI if it's necessary to review compliance with the Privacy Rule.

**FYI**

HHS provides a Health Information Privacy Complaint for consumer use. The complaint is available at *http://www.hhs.gov/ocr/privacy/hipaa/complaints/*.

### Permitted Uses and Disclosures

A covered entity is permitted to use and disclose a person's PHI, without written consent, in a number of situations. A use or disclosure that doesn't fall within the situations described by the rule isn't permitted unless a person specifically allows it.[16] HHS allows the following uses and disclosures of PHI without consent:

- Made to a person about his or her own PHI
- Made for treatment, payment, and health care operations
- Made after giving a person an opportunity to opt out of the use
- Made for public health and safety activities
- Limited data sets of PHI used or disclosed for specified activities

**Uses and Disclosures Made to a Person about His or Her Own PHI.** A covered entity may always disclose a person's PHI to him or her without written consent. This makes sense because health care providers must communicate with people about their own care. It would not facilitate efficient health care if people had to specifically authorize covered entities to discuss their health care with them. Providing a person's PHI to them when they ask for it also is a required disclosure under the Privacy Rule.

**Treatment, Payment, and Health Care Operations.** A covered entity may use a person's PHI for its own treatment, payment, or health care operations.[17] These are the most common covered entity activities. The Privacy Rule defines each of these terms. A covered entity is engaging in *treatment activities* when it's giving health care or services to a person.[18] These activities include managing a patient's health care among several providers. They also include referring a patient to another provider. A covered entity also can disclose PHI for the treatment activities of another covered entity. For example, a dentist can send a copy of a patient's dental records to an orthodontist who needs that information to treat the patient.

> **NOTE**
> Covered entities may disclose PHI to other health care providers for treatment and payment purposes. These providers don't have to be covered by the Privacy Rule.

*Payment activities* are actions to get payment for health care goods and services.[19] A covered entity may disclose PHI without consent for these activities. They include billing and collection functions. They also include submitting claims for services to health insurance companies. Covered entities also may disclose PHI to another covered entity for the payment activities of the other entity. For instance, a doctor can share a person's health insurance coverage with a laboratory that it uses to process patient blood work. The lab needs the information in order to bill the patient for the services that it provides to the doctor.

*Health care operations* are actions that support the covered entity's business. A covered entity may use a person's PHI for these activities without consent. These activities are the administrative and financial functions needed to run the business. They include review processes to make sure that a covered entity is compliant with the laws that it must follow. Health care operations include quality assessment and improvement actions. A covered entity may not usually share any PHI used for these purposes with another covered entity. The only time it's allowed is when both entities have a relationship with the person.

Covered entities may choose to get a person's consent to use PHI for treatment, payment, and health care operations. However, it isn't required under the Privacy Rule.[20] Even when a covered entity gets consent to share PHI for these purposes, it should always make sure that it uses and discloses PHI in a way that is consistent with its notice of privacy practices. These notices are discussed in this chapter.

**Uses and Disclosures Made After an Opportunity to Opt Out.** There are some situations where a covered entity may use or disclose a person's PHI only after they've had an opportunity to opt out of the use or disclosure.[21] An *opt-out* is a more informal type of consent. It applies only in limited situations. A written consent isn't needed so long as a person was advised of the right to opt out. These situations include publishing a patient's name and condition in a facility directory, and sharing PHI with a person's family and friends.

Some covered entities, like hospitals, maintain a directory of patient information. Nursing homes do this too. They use this directory to list the person's name, facility room number, and general condition. The directory contains a limited amount of PHI. A common example of a facility directory is a list of people who are patients at a hospital. The covered entity must ask patients if they want their data included in the directory. Many covered entities ask patients this question when they enter the facility for treatment. It's part of a pre-admission checklist.

Covered entities also may disclose a person's PHI to their family, friends, and caregivers without written consent. The person must be given an opportunity to opt out of the disclosure. So long as a person doesn't object, a covered entity can share PHI with friends, family, and caregivers. Covered entities can share information for treatment or payment purposes.

A person may place limits on these types of disclosures. They may specify that some, but not all, family members can receive PHI from a covered entity. For instance, a doctor may not discuss a patient's health information with his or her mother if the patient says not to.

A covered entity must use professional judgment in sharing PHI in this manner if a patient isn't present or unable to object to a disclosure. A patient can't object to a disclosure if unconscious. In these cases, the covered entity must decide that sharing the PHI is in the patient's best interest. For instance, an emergency room doctor may share information about a person's condition with his or her family and friends if the person is in surgery.

Just because a covered entity is allowed to share PHI under the rule doesn't mean that it has to do so. It isn't required to share PHI if the patient isn't present or unable to object to the disclosure. It can choose not to disclose any PHI until someone can talk to the patient.

**FYI**

HHS has created guidance for patients to help them understand when health care providers may share their PHI. That guidance is available at *https://www.hhs.gov/ohrp/regulations-and-policy/guidance/*.

**Uses and Disclosures Made for Public Health and Safety Activities.** HHS recognized that there are some situations where a covered entity should disclose a person's PHI. Sometimes it's necessary for the good of society.[22] A covered entity doesn't need a person's consent to disclose PHI in these situations. Generally, these situations involve public safety and welfare. HHS felt that requiring a person's consent to disclose PHI in these situations could negatively affect society. In general, a covered entity may disclose PHI to certain governmental entities without consent for the following purposes:

- To provide vital statistics
- To control communicable diseases
- To report abuse and neglect
- When required by other laws
- For law enforcement purposes

> **NOTE**
> Public health is the branch of medicine that is concerned with the health of a community of people. A public health authority is a state or federal agency that is responsible for public health matters. A state or local health department is a public health authority. The federal Centers for Disease Control and Prevention (CDC) is a public health authority.

*Vital Statistics and Communicable Diseases.* A covered entity may disclose a person's PHI without consent to report births, deaths, and other vital statistics. It must report these events to public health authorities. It may also disclose PHI to these authorities to prevent or control disease, injury, or disability. These types of disclosures of PHI don't require consent. For instance, New York health care providers must report certain diseases to their local health departments. They must report highly contagious diseases. They also must immediately report diseases that might indicate bioterrorism. Diseases that must be reported immediately include smallpox, anthrax, botulism, and typhoid. These diseases are serious public health threats.

The HITECH Act added regulations that allow covered entities to provide proof of immunization to schools if required for admittance. This is because schools play an important role in making sure children are vaccinated. In these cases, covered entities have to document that an individual agreed to the disclosure of the records.[23]

*Abuse and Neglect.* A covered entity may disclose PHI about victims of child abuse or neglect without consent. The covered entity may disclose the PHI only to government agencies that have the legal authority to receive these reports. Child welfare and social services agencies are allowed by state law to receive reports about child abuse and neglect. Law enforcement agencies also are allowed to receive these types of reports.

All U.S. states have laws that require health care providers to report evidence of child abuse and neglect. Other professionals that work with children, such as teachers, have similar requirements. They must report information either to state social services agencies or to local law enforcement. States make these laws because it's important to the public welfare to protect children.

**FYI**

Attorneys are allowed to issue subpoenas for information as part of lawsuits. These are often issued as part of the discovery process. **Discovery** is the legal process used to gather evidence in a lawsuit. A discovery request is a request for information from one party in a lawsuit to the other party. These requests also can be made to witnesses. Subpoenas issued by attorneys as part of the discovery process don't require court approval. When a subpoena issued as part of discovery requests PHI, the individual involved must be notified.

The Privacy Rule contains slightly different provisions for adult victims of abuse, neglect, or domestic violence. A covered entity may disclose PHI about adult victims of these crimes if the disclosure is required by law and if the patient allows it. They may still disclose PHI if a patient doesn't allow the disclosure, or can't agree to the disclosure. In that case, the covered entity must use their professional judgment to determine that the disclosure is necessary. A disclosure is necessary if it must be made to prevent serious harm to the person.

A covered entity must promptly notify a person or their personal representative if they make a disclosure of PHI in these cases. There are some exceptions to this general rule. The covered entity doesn't have to notify an adult victim if they believe that informing them would place them at risk of harm. They also don't have to notify the individual's personal representative if they believe that the representative is responsible for the victim's injuries.

*Required by Law and Law Enforcement.* A covered entity may use or disclose PHI to the extent that it's required by law.[24] In these situations, the covered entity is usually disclosing the PHI to some sort of governmental entity. For example, it may disclose PHI in response to a court order or court-ordered warrant. It may also disclose PHI in response to a subpoena issued by a grand jury. If the covered entity is providing PHI in response to a discovery request generated as part of a lawsuit, then it must notify the person who is the subject of the PHI. That person must have a chance to object to the discovery request.

Covered entities may also disclose PHI without consent for some law enforcement activities. They may provide some types of PHI to help identify or locate a suspect, witness, or missing person. Information that a covered entity can provide in these situations is limited to identifying information. This includes name and address. It also includes distinguishing physical characteristics that could be used to identify the person that the police are looking for.

Covered entities may also provide PHI without consent if it's requested by law enforcement and it's about a victim of crime. They can also disclose PHI as needed to identify or apprehend a violent criminal. Covered entities may alert law enforcement about a person's death if they believe that the death was caused by criminal activity. They also may disclose PHI to law enforcement or government officials if they believe there's a serious threat to health or safety.

**Limited Data Sets Used or Disclosed for Specified Activities.** A *limited data set* is PHI that doesn't contain any data that identifies a person. It is PHI that is stripped of certain identifiers. These identifiers must be redacted from the PHI. Information is redacted when it is removed or obscured in a document before sharing that document with other individuals or groups.

A covered entity may share limited data sets for research, health care operations, and public health activities. It doesn't need a person's permission to share them. Identifiers that must be removed from PHI in order to create a limited data set are:[25]

- Name
- Street address (except that some geographical information may remain if certain conditions are met)
- Telephone and fax numbers
- E-mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any similar images
- Any other unique identifying number, characteristic, or code that identifies a person or their PHI

A limited data set is still PHI. A covered entity must enter into a data use agreement with the organization that receives it. The data use agreement specifies how the PHI in the limited data set will be protected.

### Uses and Disclosures That Require Authorization

> **NOTE**
>
> *De-identified data* is data that has been stripped of all information that could identify an individual. De-identified data is not PHI. The HHS has issued guidance about how to de-identify data.

A covered entity must get people's written consent in order to use or disclose their PHI in ways that are not expressly allowed under the Privacy Rule.[26] Under the Rule, written consent is called an **authorization**. These are very specific documents that allow PHI to be shared. A written authorization is required for many purposes. They are required to disclose psychotherapy notes and to use PHI in marketing materials.

A covered entity must get an authorization before it discloses PHI if a permitted use or disclosure doesn't apply. This comes into play in many ways. A covered entity needs an authorization to

**FYI**

HIPAA uses the term authorization to distinguish between consent to use or disclose PHI and other types of consent that are used in the health care industry. For example, *informed consent* is a basic rule in health care. This is written consent from a patient to undergo a medical treatment. These types of consent explain the risks and benefits of treatment. When patients sign these informed consent documents, they are agreeing to undergo the treatments specified. These forms are very different from a Privacy Rule authorization that allows PHI to be shared. When people must consent to sharing their PHI, they show their consent by signing an authorization. This eliminates confusion among different types of documents used in the health care industry.

share a person's PHI with an employer for employment purposes. Even if a person asks the covered entity to provide this information to an employer, he or she must sign an authorization. A parent will need to sign an authorization on behalf of his or her minor child to have the covered entity disclose PHI to the child's school. This might be required to allow children to participate in some school activities like sporting events.

The Privacy Rule forbids a covered entity from requiring a person to sign an authorization in order to receive health care treatment. They can't condition benefit eligibility on signing an authorization. This is so that covered entities can't force people to sign authorizations under pressure by withholding needed care.

The Privacy Rule requires authorizations to contain specific terms. It also states situations in which an authorization is defective. A defective authorization isn't valid. Authorizations are defective if the expiration date stated in the authorization has passed. They're also invalid if they aren't filled out completely. They're also invalid if a person has revoked them.

An authorization must be in plain language. This means that it should not contain any legal terms or other terms that are hard for a person to understand. A valid authorization must contain the following elements:[27]

- A specific and meaningful description of the PHI that will be used or disclosed
- Identification of the people who are allowed to make the requested use or disclosure
- Identification of the people who will receive the use or disclosure
- A clear description of the reason for the requested use or disclosure
- The date that the authorization will expire
- The signature of the person and the date

The Privacy Rule requires that covered entities provide people with a copy of any authorizations that they sign.

### Minimum Necessary Rule

A covered entity is permitted to use and disclose some types of PHI without an authorization. These situations were described earlier in this chapter. This doesn't mean that it should always disclose the entire allowable PHI. Any time a covered entity discloses PHI, it must follow the **minimum necessary rule.**[28] It may disclose only the amount of PHI

absolutely necessary. The amount disclosed must be able to satisfy the reason why the information is being used or disclosed, but no more. Covered entities must create internal processes and procedures to make sure that employees access only the amount of PHI needed to do their jobs.

> **NOTE**
> The Privacy Rule minimum necessary rule is similar to the general information security principle of need to know. Only the information needed to carry out a function or activity should be disclosed.

A covered entity must use professional judgment and make reasonable efforts to limit its use or disclosure of PHI. For instance, a health care provider shouldn't disclose a person's entire medical record if only a portion of it is responsive to a request.

There are some exceptions to this rule. Uses or disclosures of PHI made by a health care provider for treatment purposes are not subject to the minimum necessary rule. It also doesn't apply to disclosures made to people about their own PHI. The rule also doesn't apply to uses or disclosures made when a person specifically authorizes the use or disclosure. It also doesn't apply to uses or disclosures required by law or made to HHS for its complaint investigation function.

### Other Individual Rights under the Privacy Rule

The Privacy Rule gives people additional rights regarding their PHI. These rights help people make sure that their PHI is used properly.

**Amendments of PHI.** A person has the right to ask that a covered entity amend the person's PHI.[29] A covered entity doesn't have to correct data in the record. Instead, it can include the amendment in the record. That way the integrity of the record is maintained. Other entities that might rely on the unamended PHI to the person's detriment must be notified of the amendment. The covered entity that makes this amendment also must notify the other entities. The covered entity also must notify anyone else the individual specifies.

A covered entity must respond to a request to amend PHI within 60 days.[30] That time can be extended for 30 days if the covered entity notifies the requestor in writing. A covered entity may choose not to amend PHI for some reason. A covered entity doesn't have to amend PHI if it didn't create the PHI that is in question. It also doesn't have to amend PHI if it determines that the PHI in the record is accurate and complete.

If an entity chooses to deny a request to amend PHI, then it must issue a written denial notice to the person who requested the amendment. The denial notice must contain the basis for the denial. It also must contain a statement of the person's right to disagree with the denial. A person may submit a statement of disagreement to the covered entity. The covered entity may prepare a rebuttal to the person's statement of disagreement. If a request for amendment is denied, the covered entity must include the following in the person's record:

- Identification of the PHI that is under dispute
- A copy of the person's request to amend the PHI
- A copy of the covered entity's denial of the request
- A copy of the person's statement of disagreement
- A copy of the covered entity's rebuttal statement

All of this information must be included in future uses or disclosures of the PHI that is under dispute.

**Accounting of Disclosures.** Covered entities must keep records of how they disclose a person's PHI. Under the Privacy Rule, a person has the right to receive an accounting of how the covered entity has used or disclosed the person's PHI.[31] People have the right to get an accounting of disclosures of PHI made in the six years prior to the date of their request. They also can request accountings for shorter periods.

A covered entity doesn't have to account for every PHI disclosure that it makes. The Privacy Rule states that some kinds of disclosures don't have to be included in an accounting. Any disclosure not specifically excluded must be included and tracked. Table 6-1 compares different types of disclosures.

**TABLE 6-1** Different types of disclosures.

| DISCLOSURES THAT ARE NOT TRACKED | DISCLOSURES THAT MUST BE TRACKED |
|---|---|
| Disclosures made to carry out treatment, payment, and health care activities* | Disclosures to HHS for its compliance functions |
| Disclosures to individuals | Disclosures required by law |
| Disclosures made after an authorization is received | Disclosures required for public health activities |
| Incidental disclosures | Disclosures made to report abuse |
| Disclosures where the person had the opportunity to opt out | Disclosures for judicial and administrative proceedings (in response to subpoenas and court orders) |
| Disclosures for national security or intelligence purposes | Disclosures for law enforcement purposes |
| Disclosures to correctional institutions or to law enforcement officials having custody of an inmate | Disclosures for research purposes (unless authorized or made via a limited data set) |
| Disclosures that are part of a limited data set | Disclosures to the public health agencies |
| Disclosures made more than six years before the date of the person's request for an accounting | Disclosures to avert a threat of serious injury |
| | Disclosures made by mistake (inadvertent disclosures) |
| | Any other disclosures not specifically excluded by the Privacy Rule |

*The HITECH Act has different tracking requirements for disclosures made from an electronic health record (EHR).

A covered entity must provide a person a first accounting in a 12-month period at no charge. If he or she requests more than one accounting in that period, then the covered entity can charge a reasonable fee for each subsequent request. The covered entity must inform the person that it intends to charge a fee for an extra accounting. It must give the person a chance to withdraw or change the request in order to avoid the fee.

A covered entity must respond to a request for an accounting in writing. It must respond within 60 days. This period can be extended 30 days with notice to the person who has requested the accounting. When it responds, the covered entity must include the following information:

- Date of disclosure
- Name of recipient
- Description of the PHI disclosed
- Reason for the disclosure, or a copy of the request for the disclosure

### Incidental and Inadvertent Disclosures

The difference between incidental and inadvertent disclosures of PHI is important to understand. Even though they sound similar, they are very different.

*Incidental disclosures* are permitted disclosures under the Privacy Rule. Covered entities don't have to track these types of disclosures. An incidental disclosure can result from any use or disclosure that is allowed under the Privacy Rule. They are allowed so long as a covered entity implements safeguards to limit the amount of PHI exposed though an incidental disclosure.

Examples of incidental disclosures include:

- A customer at a pharmacy hears the pharmacist quietly discussing a medication with another customer. This is an incidental disclosure because it's made as a result of an activity that is allowed under the Privacy Rule. The permitted activity is the covered entity's treatment activities.
- A patient going to a hospital to pay a bill briefly views another patient's payment information on the billing clerk's computer monitor. The first patient can see this information only briefly before the clerk accesses the patient's own record. This is an incidental disclosure because it's a result of the covered entity's permitted payment activities.

Covered entities must take steps to limit incidental disclosures. This includes speaking quietly when discussing conditions with patients and their families. It also includes shielding monitors from view as much as possible.

Inadvertent disclosures are different. *Inadvertent disclosures* are not permitted under the Privacy Rule. Covered entities must track inadvertent disclosures. They also must provide an accounting of these types of disclosures if a person requests it. These disclosures happen by mistake. An example would be if a covered entity discloses PHI without a valid authorization when one was needed. Under the HITECH Act, some types of inadvertent disclosures could even be considered an impermissible data breach that requires further action.

The HITECH Act made changes to the accounting of disclosures requirement for electronic PHI (EPHI). These changes apply to cases where a covered entity maintains an electronic health record (EHR) for a person. An EHR is an electronic record or health care information created by a covered entity. If a covered entity keeps an EHR, then it must provide a person with an accounting of the treatment, payment, and health care operation disclosures made from that EHR.[32] This expanded requirement applies only to disclosures from an electronic health record. In cases involving an EHR, a person has a right to get an accounting only for the three years prior to the date of the request. The HHS has proposed additional regulations that address how disclosures from an EHR should be accounted for. At the time of this writing, these regulations had not been finalized.

### Privacy Notices

Covered entities must inform people about their privacy practices.[33] The Privacy Rule requires covered entities to let people know how they use and disclose their PHI. It does this in a privacy policy. A covered entity must use and disclose PHI only in the ways described by their privacy policy.

A covered entity must use plain language to draft its notice. An average person must be able to understand the notice. The Privacy Rule requires the notice to include specific parts:

- A title that reads: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY." The covered entity must display this header in prominent type.
- A description of how the covered entity may use and disclose a person's PHI. It should include examples of disclosures that the entity makes for treatment, payment, and health care operations. This description should state when the covered entity is allowed to use or disclose PHI without a person's consent, and when the covered entity must have consent.
- A description of the person's rights with respect to his or her PHI. This section should also include information on how a person can exercise these rights. The covered entity must include information about its complaint processes. It must also include information about the person's right to complain to HHS.
- A statement that the covered entity is required by law to maintain the privacy of PHI. This statement must include the entity's legal duties with respect to PHI.
- The contact information of a person the individual can contact to ask additional questions about the covered entity's privacy notice.

**NOTE**

Many of the elements that are required in the Notice of Privacy Practices contain portions of the fair information practices principles.

**NOTE**

A *material change* is a change in an organization's operating practices that's significant. Material changes can affect how people understand their rights or interact with an organization.

A covered entity's privacy policy must contain an effective date. The covered entity must revise and redistribute its notice any time it makes a material change to the notice. Covered entities must make the notice available to anyone who asks for it. It also must make the notice available on any Web site that it maintains.

Different types of covered entities have additional rules to follow when giving their privacy notices to individuals.[34] Health plans must distribute their privacy notices to people when they enroll in the health plan. They also must make sure that plan participants receive a copy of the notice at least once every three years.

In some cases, the Privacy Rule doesn't require health care clearinghouses to develop a notice of privacy practices. They are not required to develop a notice if the only PHI that they create or receive is as a business associate of another covered entity.

Health care providers have additional rules to follow for distributing their notices to individuals. Providers must give the notice to a person no later than when they first provide services to that person. They also must make a good-faith effort to get the person's written acknowledgement of receipt of the notice. A provider must document a person's receipt of the notice if it can't gain a receipt from the person.

In emergencies, the health care provider must provide its notice of privacy practices to a patient as soon as it's reasonable. A health care provider must also post its notice in a clear and prominent location where patients can read the notice. Covered entities must retain copies of privacy notices that they distribute. They must also retain written acknowledgments.

### Administrative Requirements

A covered entity has administrative duties under the Privacy Rule.[35] It must designate a privacy official. This official is responsible for developing the covered entity's privacy policies and procedures. HHS allows a covered entity to scope its privacy policies and programs to its size and structure. This allows covered entities some discretion when they create their programs. Covered entities that are large with complex structures must develop policies appropriate for that structure. Smaller entities are not held to the same standard. They must develop their own policies.

The covered entity must also designate a person to receive consumer privacy complaints. This person handles complaints about the entity's own privacy policies. They also handle consumer complaints about the Privacy Rule. This person also answers questions about the entity's privacy notice. The privacy official often serves as this contact person.

Covered entities must create policies and procedures to protect the privacy of all PHI.[36] Policies that protect the privacy of PHI include destroying it properly. They can also include requirements that paper medical charts be secured in locked file cabinets. This requirement is similar to the HIPAA Security Rule. However, the Security Rule applies only to electronic protected health information.

Covered entities must train their employees on the Privacy Rule and its privacy policies and procedures. It must train all employees—even part-time employees, volunteers, and interns. A covered entity also must have a discipline policy for workers who violate the Privacy Rule. This is called a sanctions policy.

**FYI**

HHS relies on National Institute of Standards and Technology (NIST) guidelines to specify how PHI should be secured during storage and transmission. PHI is considered secured if a covered entity encrypts it according to these guidelines. The HHS guidance can be found at *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule.*

## Breach Notification Provisions

The Privacy Rule requires covered entities, including business associates, to mitigate an unauthorized use or disclosure of PHI.[37] Prior to the HITECH Act, a covered entity didn't have to notify individuals that their PHI was used or disclosed in an unauthorized manner. The HITECH Act now requires them to do so. It creates notification requirements that covered entities must follow in the event of a breach of unsecured PHI.[38] Both covered entities and business associates must follow these rules.

A *breach* is any impermissible use or disclosure of unsecured PHI that compromises the security or privacy of the PHI. Any unauthorized use or disclosure is presumed to be a breach under the law. In some cases a covered entity might be able to show that there is a low probability that PHI was compromised. If it can do that, then the breach notification requirements do not apply.

To show that there is a low probability that PHI has been compromised, a covered entity must engage in a risk assessment. To conduct the risk assessment, a covered entity must review:

- **The PHI that was involved in the breach**—Is the PHI involved very sensitive? Is it more likely to lead to identify theft?
- **Who used or received the PHI**—Does the entity know who used the PHI? Was it an impermissible use or disclosure?
- **Was the PHI actually acquired?**—Was the PHI involved actually viewed? Was is downloaded by the unauthorized individual?
- **Have risks been mitigated?**—If the entity knows who used the PHI, can it get assurances that they will not disclose or use the data further? Can the entity ensure that PHI has been destroyed?

The covered entity must weigh all these factors. It also must conduct this risk assessment in good faith. As noted earlier, if the risk assessment demonstrates that there is a low probability that the PHI has been compromised, then the breach notification requirements do not apply.[39]

The HITECH breach notification provisions apply to unsecured PHI. Unsecured PHI is PHI that isn't protected by a technology that renders it unusable or unreadable. Unsecured PHI is PHI that isn't encrypted or properly destroyed. PHI must be encrypted through a process that is approved by HHS to be considered secure. In April 2009, HHS issued guidance on what technologies were acceptable to encrypt PHI. It will update this guidance yearly.