CHAPTER 7

PRIVACY LAW & HIPAA

Objectives

After studying this chapter, you should be able to

1. Discuss federal privacy laws that pertain to health care.
2. Discuss the conditions that led to the passage of HIPAA.
3. Discuss the four standards of HIPAA.
4. Explain the advantages to uniform transmission standards and code sets.
5. Determine which covered entities must comply with HIPAA provisions.
6. Summarize the provisions of the Privacy Rule and how they apply to your profession.
7. Recognize and dispel some of the more prevalent myths concerning HIPAA.

Key Terms

code set
covered entities
covered transaction
designated record set
electronic data interchange (EDI)
electronic transmission
encryption
firewalls
Health Insurance Portability and Accountability Act (HIPAA)
limited data set
minimum necessary
Notice of Privacy Practices (NPP)
permissions
privacy
Protected Health Information (PHI)
rule
security
standard
state preemption
transaction
treatment, payment, and healthcare operations (TPO)
verification

VOICE OF EXPERIENCE

HIPAA and Privacy Officer Discusses Compliance

Tom is the Health Insurance Portability and Accountability Act (HIPAA) Compliance Coordinator and Privacy and Information Security Officer for a Midwestern regional hospital. Tom emphasizes that health care facilities have always been concerned with information privacy and patient confidentiality, but with the enactment of HIPAA, "the force of the law is behind privacy."

Tom has a degree in computer information systems and has added national training sessions for HIPAA privacy and security to his resume. Different providers will comply with HIPAA in different ways, Tom says. Early in the compliance process, Tom trained 4500 hospital employees. He trains all new hires, students, and volunteers in HIPAA compliance and conducts continuing departmental training as necessary. The initial training is all instructor led, but update sessions will be a combination instructor-lead and computer-based self study.

The most frequently-asked question from hospital staff members, Tom says, is "Can I talk to this person?" Before releasing information, Tom advises staff members to "refer to your policies or, if in doubt, check with compliance. There are few restrictions on sharing health care information with other health care providers, but we have to understand who is a 'health care provider.' For example, some assisted care facilities may not provide healthcare, and we can't always release information to them."

Since implementation of HIPAA, many situations require clarification before information can be released. For instance, can the person manning the hospital information desk tell a caller from the police department if a certain person is a patient in the hospital? "It depends," Tom answers. "If the police call and say a suspect fell out of a window during a robbery and may have broken his arm, and they ask if we have anyone like that who was recently in the emergency room, we can give them names and addresses, but we can't release information about medical treatment administered. Victims of a crime or witnesses to a crime are treated differently. The hospital cannot release any information regarding a victim unless the release is required by law (like gunshots) or if the victim authorizes us to make the release."

The privacy portion of HIPAA means protecting the protected healthcare information (PHI) that the facility has collected, "no matter what form or medium it is in, including paper, electronic, and verbal forms," Tom tells hospital staff. "HIPAA Security is an entirely different matter. Security relates to information technology and electronic security. It does not address things like conversations or paper charts. We have had to develop policies and goals that meet HIPAA security standards . . . Appropriate security involves items like unique passwords, anti-virus protection and firewalls at Internet service provider (ISP) levels . . ."

One of the more difficult issues to address from the security perspective is the fact that the hospital employs telecommuters and, says Tom, "They must meet the minimum standard for working from home. For example, they must have operating system updates sufficient for protection of information." This can be difficult to enforce if telecommuters are using their personal computers as opposed to hospital-provided equipment.

"Encryption [scrambling] of information is provided for in HIPAA," Tom adds. "We encrypt patient lists sent to outside contractors, such as the survey company and billing service we use. We are moving toward more encryption."

"Total HIPAA compliance is our goal," Tom states. "It's ongoing and never completely accomplished because 100 percent security is unachievable."

So far, Tom sums up, HIPAA enforcement, handled by the Office of Civil Rights, has not resulted in major penalties for health care facilities. "They are taking a 'helping hand' approach to resolving issues as opposed to a strict enforcement action."

PRIVACY AND THE UNITED STATES CONSTITUTION

privacy Freedom from unauthorized intrusion.

Contrary to popular belief, the term **"privacy"** (freedom from unauthorized intrusion) does not appear in the U.S. Constitution or the Bill of Rights. However, the U.S. Supreme Court has ruled in favor of privacy interests (and occasionally against them), deriving the right to privacy from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution. Those amendments are

First Amendment: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Third Amendment: No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Fourth Amendment: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fifth Amendment: No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Ninth Amendment: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Fourteenth Amendment: Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

The following Court Case is an example of a privacy action that was recently decided by the United States Supreme Court:

Court Case

Privacy Loses to Security

Under the Alaska Sex Offender Registration Act of 1994, any sex offender or child kidnapper incarcerated in the state must register with the Department of Corrections within 30 days before his release, providing his name, address, and other information. The person must register with local law enforcement authorities within a working day of his conviction, if he remains free, or if entering the state, if he is released from incarceration in another state. If he was convicted of an aggravated (made worse by more serious circumstances, such as deadly force, violence, or the commission of another crime) sex offense or of two or more sex offenses, he must register for life and verify the information quarterly. If he was convicted of a single, non-aggravated sex crime, the offender must provide annual verification of the specified information for 15 years.

The offender's information is forwarded to the Alaska Department of Public Safety, which maintains a central registry of sex offenders. Some of the data, such as fingerprints, anticipated change of address, and whether the offender has had medical treatment after his conviction is kept confidential. However, the following information is published on the Internet: the offender's name, aliases, address, photograph, physical description, driver's license number, motor vehicle identification numbers, place of employment, date of birth, crime, date and place of conviction, length and conditions of sentence, and a statement as to whether the offender is in compliance with the Act's update requirements or cannot be located. Both the Act's registration and notification requirements are retroactive (apply to those convicted before the Act was passed).

Two sex offenders convicted of aggravated sex offenses were released from an Alaska prison and completed rehabilitative programs for sex offenders. They were convicted before the Act's passage, and sought in court to have the Act declared void in their cases, both because they believed the Act violated privacy and because they believed it should not be retroactive.

A District Court granted the petitioners summary judgment. The state appealed, and the Ninth Circuit Court reversed the District Court's decision, holding that because the Alaska Sex Offender Registration Act is non-punitive, its retroactive application is upheld. The appeals court also held that the public safety issue was more important than the petitioners' privacy. The petitioners appealed, and the case reached the United States Supreme Court, which upheld the Ninth Circuit Court's decision. The petitioners must register as required under the Alaska Act.

Smith v. Doe, 123 S.Ct. 1140, 71 USLW 4182 (2003)

FEDERAL PRIVACY LAWS

Concern about privacy has led to the enactment of federal and state laws governing the collection, storage, transmission, and disclosure of personal data. Common points in most of these laws include

1. Information collected and stored about individuals should be limited to what is necessary to carry out the functions of the business or government agency collecting the information.
2. Once collected, access to personal information should be limited to those employees who must use the information in performing their jobs.
3. Personal information cannot be released outside the organization collecting it unless authorization is obtained from the subject.
4. When information is collected about a person, that person should know that the information is being collected and should have the opportunity to check the information for accuracy.

Here is a summary of the major U.S. government laws concerning privacy:

TABLE 7-1 Major Federal Privacy Laws

Date Enacted	Law	Purpose
1970	**Fair Credit Reporting Act**	Prohibits credit reporting agencies from releasing credit information to unauthorized people, and allows consumers to review their own credit records.
1974	**Family Educational Rights and Privacy Act**	Gives students and parents access to school records and limits disclosure of records to unauthorized parties.
1974	**Privacy Act**	Forbids federal agencies from allowing information to be used for a reason other than that for which it was collected.
1978	**Right to Financial Privacy Act**	Strictly outlines procedures federal agencies must follow when looking at customer records in banks.
1984	**Computer Fraud and Abuse Act**	Forbids unauthorized access of federal government computers.
1984	**Cable Communications Policy Act**	Regulates disclosure of cable television subscriber records.
1986	**Electronic Communications Privacy Act (ECPA)**	Provides privacy protection for new forms of electronic communications such as voice mail, e-mail, and cellular telephone.
1988	**Video Privacy Protection Act**	Forbids retailers from releasing or selling video-rental records without customer consent or a court order.
1991	**Telephone Consumer Protection Act**	Restricts activities of telemarketers.
1992	**Cable Act**	Extends the privacy provisions of the Cable Communications Policy Act of 1984 to include cellular and other wireless services.
1994	**Computer Abuse Amendments Act**	Amends the 1984 act to forbid transmission of harmful computer code such as viruses.
1996	**National Information Infrastructure Protection Act**	Penalizes theft of information across state lines, threats against networks, and computer system trespassing.
1996	**Health Insurance Portability and Accountability Act (HIPAA)**	Guarantees that workers who change jobs can obtain health insurance. Increases efficiency and effectiveness of the U.S. health care system by electronic exchange of administrative and financial data. Improves security and privacy of patient-identifiable information. Decreases U.S. health care system transaction costs.
1997	**No Electronic Theft (NET) Act**	Closed a loophole in the law that let people give away copyrighted material (such as software) on the Internet without legal repercussions.

(continued)

TABLE 7-1 *continued*

Date Enacted	Law	Purpose
1998	**Digital Millennium Copyright Act (DMCA)**	Makes it illegal to bypass antipiracy measures in commercial software, and outlaws the sale of devices that copy software illegally.
1999	**Gramm-Leach Blily Act**	Requires all financial institutions and insurance companies to clearly disclose their privacy policies regarding the sharing of non-public personal information with affiliates and third parties.
2001	**Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act**	Gives law enforcement broad leeway in monitoring people's activities including Internet, e-mail, and library habits.
First enacted in early 1970s, revised in 2002	**Code of Federal Regulations (CFR), 42 (Public Health), Part 2**	Provides for the confidentiality of medical records of patients treated for drug and alcohol dependency.

As you can see from Table 7-1, most federal privacy laws have dealt with financial and credit information or the theft or illegal disclosure of electronic information. All states have laws governing the confidentiality of medical records, but laws vary greatly from state to state. The HIPAA of 1996 was the first *federal* legislation to deal thoroughly and explicitly with the privacy of medical records. To ensure compliance, HIPAA provides for civil and criminal sanctions for violators of the law.

Check Your Progress

1. Name four common points in most federal and state privacy laws.

_____

_____

_____

_____

2. The first federal law to deal thoroughly and explicitly with the privacy of medical records is

_____.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) Federal law passed in 1996 to protect privacy and other health care rights for patients.

Circumstances that led to the 1996 passage of federal HIPAA legislation include the following:

- Health care has become a complicated business. Health care employees are faced with a quagmire of complex billing codes, a multitude of software programs in use for storing medical records and for processing billing and payment, and more time spent on administrative chores and less time on patient issues.

- Managed care adds yet another level to the many administrative duties necessary to administer patient care including case reviewers, claims and coding experts, billing personnel, committees to review every facet of service, employees trained to handle patient complaints, and so on. Nurses had assumed many of the duties associated with health care services reporting and administration, and both physicians and nurses had less time to spend on patient care.
- Patients gather information from television ads and the Internet, often expecting their physicians to prescribe medications and treatments not appropriate for their medical problems. A side effect has been that medical malpractice and risk management issues threaten to put some physicians and health care facilities out of business due to the high cost of medical malpractice insurance and the rising costs of staying in the health care business.
- Health care consumers were and are increasingly dismayed over the rising cost of medical care and health insurance to the point that millions of Americans do not seek necessary medical care for treatment their insurance plans will not cover, are underinsured, or do not have health insurance.

In the mid-1990s when groups of health care professionals, consumers and others confronted members of the U.S. Congress about solving these serious health care problems, Congress responded with passage of the Health Insurance Portability and Accountability Act of 1996, to be administered by the *U.S. Department of Health and Human Services (HHS)*. HHS has assigned enforcement activities for the Privacy Rule to the *U.S. Office for Civil Rights (OCR)*. A second agency within HHS, the *Centers for Medicare and Medicaid Services (CMS),* has enforcement authority for other HIPAA Administrative Simplification standards, including transactions, code sets, identifiers, and security.

HIPAA LANGUAGE

Covered Entities

covered entities Health care providers and clearinghouses that transmit HIPAA transactions electronically.

In HIPAA language health plans, health care clearinghouses, and all health care providers that transmit HIPAA standard transactions electronically are called **covered entities.**

Covered entities include

- hospitals, including academic medical centers.
- nursing homes.
- hospices.
- pharmacies.
- physician practices.
- dental practices.
- chiropractors.
- podiatrists.
- osteopaths.
- physical therapists.
- alternative medicine (acupuncture, massage therapists).
- laboratories.
- health plans (payers).
- health care clearinghouses.

HIPAA offers no exclusion from the covered entity determination for small-practices. If a health care practice exchanges even one of the standard transactions via electronic means with any payer, that practice is a covered entity.

The following table can help health care practitioners and facilities determine if they are covered entities. For more complete information for determining covered entities, visit www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

Covered entities are people, businesses, or agencies that must comply with the HIPAA Standards and Privacy Rule.

Covered Transactions

covered transactions Electronic exchanges of information between two covered-entity business partners using HIPAA-mandated transaction standards.

Electronic exchanges of information between two covered-entity business partners using HIPAA-mandated transaction standards (explained below) are called **covered transactions.** HIPAA Standard Transactions include, but are not limited to the following: (For a more complete description of covered transactions, visit www.wedi.org/snip/public/articles/details%7E9.htm.)

- A physician submitting an electronic claim to a health plan.
- A physician sending a referral or authorization electronically to another physician, lab, or hospital.
- A physician sending patient-identifiable information to a billing service or to another physician.
- Any health care provider employs another entity, such as a clearinghouse or billing agency, to send claims to payers or health plans.

TABLE 7-2 How to Determine Covered Entities

Question	Answer	
Do you furnish, bill, or receive payment for health care in the normal course of business?	No Not a covered entity	Yes Probably a covered entity
Does your practice conduct covered transactions?	No Not a covered entity	Yes Covered entity
Are any of the covered transactions conducted in electronic format?	No Not a covered entity	Yes Covered entity
Does the practice conduct all of the following transactions *on paper, by phone, or by FAX* (from a dedicated fax machine, as opposed to faxing from a computer)? • Submitting claims or managed care encounter information • Checking claim status inquiry and response • Checking eligibility and receiving a response • Checking referral certifications and authorizations • Enrolling and disenrolling in a health plan • Receiving health care payments and remittance advice • Providing coordination of benefits	No Covered entity if even one transaction is conducted electronically	Yes Not a covered entity (no electronic transactions)
Does the practice bill Medicare, and is it a small provider with fewer than 10 full-time equivalent employees? (Effective October 16, 2003, Medicare may not pay claims submitted on paper.)	No Covered entity	Yes Not a covered entity

(A patient sending an e-mail message to a physician that contains patient-identifiable information would not be a HIPAA standards-covered transaction because patients are not covered entities.)

Any physician, health care practitioner, or health care facility, regardless of size, that files even one electronic claim is a covered entity and must use HIPAA electronic transaction and code set standards.

Other Important HIPAA Terms

designated record set Includes records maintained by or for a covered entity.

A **designated record set** includes records maintained by or for a covered entity including medical records and billing records about individuals; a health plan's enrollment, payment, 10 claims adjudication, and case or medical management record systems; and records used by or for the covered entity to make decisions about an individual.

Notice of Privacy Practices (NPP) A written document detailing a health care provider's privacy practices.

Notice of Privacy Practices (NPP) is a written document detailing a health care provider's privacy practices. Under HIPAA's Privacy Rule, every patient visiting his or her health care provider after April 14, 2003, must have received a NPP. Patients are asked to sign the form, and it is filed with patient's medical records.

Protected Health Information (PHI) Information that contains one or more patient identifiers.

Protected Health Information (PHI) refers to information that contains one or more patient identifiers and can, therefore, be used to identify an individual. The Privacy Rule (see below) says that PHI must be protected whether it is written, spoken, or in electronic form. Health information with no identifiers is said to be **"de-identified,"** and is not considered PHI. Information that includes one or more of the following makes a patient's medical record identifiable:

- name.
- zip code.
- date of birth.
- dates of treatment.
- telephone numbers.
- fax number.
- e-mail addresses.
- Social Security number.
- medical record numbers.
- health plan beneficiary numbers.
- birth certificate and driver's license.
- vehicle identification number and license plate number.
- website address.
- finger prints and voice prints.
- photos.

state preemption If a state's privacy laws are stricter than HIPAA privacy standards, the state laws take precedence.

State preemption means that if a state's privacy laws are stricter than HIPAA privacy standards and/or guarantee more patients' rights, the state laws will take precedence.

treatment, payment, and healthcare operations (TPO) Treatment means that a health care provider can provide care; payment means that a provider can disclose PHI to be reimbursed; healthcare operations refers to HIPAA-approved activities and transactions.

Treatment, payment, and healthcare operations (TPO) is another important term. Within HIPAA, *treatment* means that a health care provider can provide care. *Payment* means that a provider can disclose PHI to obtain reimbursement for health care. *Healthcare operations* refers to a number of activities and transactions within and among entities including conducting quality assessments, reviewing the competence or qualifications of health care practitioners, and managing the business.

Business associates are not covered entities, but covered entities must have contracts or agreements with business associates that conduct certain activities on behalf of a covered entity. Contracts must specify that the business associate will safeguard protected health information according to HIPAA requirements. The agreement should include recourse provisions for the covered entity if the business associate accidentally or intentionally releases patient-identifying information entrusted to it.

Business associates of covered entities include, but are not limited to, services engaged in

accounting
accreditation
benefit management
billing
claims processing
consulting
data aggregation
data analysis
dictation and transcription
legal consultation
practice management
processing or administration
quality assurance
re-pricing
utilization review

Check Your Progress

3. Distinguish between *covered entities* and *covered transactions.*

4. Give two examples of a covered entity.

5. Give two examples of covered transactions.

6. Define *state preemption.*

HIPAA STANDARDS

standard A general HIPAA requirement.

rule Document that includes the standards.

HIPAA contains four sets of standards, with rules that health care facilities must implement within a designated time frame. Under HIPAA, a **standard** is a general requirement; a **rule** is a document that includes the standards. Each rule begins with a Notice of Proposed Rule-Making (NPRM) that HHS presents for

public comment and suggested revisions. HHS publishes the final rule in the *Federal Register.* Health care providers then have 24 months to comply with the rule. The four HIPAA standards are as follows:

TABLE 7-3 HIPAA Standards and Timelines

Standard Name	Purpose	Deadline for Implementation	Comments
1. Transactions and Code Sets	Primary goal is Administrative Simplification. Provides for uniformity and simplification of billing and coding for health care services, and requires the use of standard formats and data content for transmitting files electronically	10/16/2002 10/16/2003 4/16/2003	Implementation time could be extended to the latest date, but by 4/16/2003 health care providers must have started testing transactions. HHS established contingency plans that extended past the deadline to ease the transition from nonstandard to standard transactions.
2. Privacy Rule	Protecting the privacy of patient-identifying information in any form or medium. Gives certain rights to patients, as explained below.	4/14/2003	HHS continues to release guidance to clarify the Privacy Rule. The Rule allows for an update only once yearly.
3. Security Rule	Provides for the security of electronic Protected Health Information (ePHI). It does this by requiring general and specific protections for data stored and transmitted electronically. Some of the security measures listed include use of firewalls, anti-virus software, encryption, password protection, and other measures. (Terms defined below.)	4/21/2005	Security safeguards required by the Privacy Rule must be in place by 4/14/2003, even though the date for compliance with the Security Rule is 2005.
4. National Identifier Standards	To provide uniform national identifiers for the movement of electronic transactions. The 4 national identifiers are provider, health plan, employer, and individual	7/30/2004	*The final rule for a Standard Employer Identifier was published on 5/31/02. The final rule for a Standard Provider Identifier was published on January 23, 2004. The Standard Health plan identifier is under development. The Standard Individual Identifier is on Congressional hold waiting for regulatory action.

*See the following website for updates to Standard 4 www.cms.hhs.gov/hipaa/hipaa2/regulations/identifiers/default.asp

STANDARD 1. TRANSACTIONS AND CODE SETS

transaction Transmission of information between two parties for financial or administrative activities.

code sets Any set of codes used to encode health care data elements.

A **transaction** refers to the transmission of information between two parties to carry out financial or administrative activities. **Code sets** are "any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes." HIPAA provisions say that codes must now be uniform throughout the country to make filling out insurance claim forms and billing for services much easier than before.

Before HIPAA, medical facilities filing and collecting on claims used different formats, which often held up payment while codes were explained and further information was submitted. (By the mid-1990s, there were over 400 different software formats for coding and billing in medical facilities.) Now, through HIPAA, the law says, "Everyone must send or receive transactions using standard formats and data content." All health care providers must ensure that they can send and receive information using standard data formats and data content. Health care providers, not software vendors, are responsible for compliance.

Code Sets

Under HIPAA, all local code sets are eliminated. Code sets now fall under four categories:

1. Coding systems for diseases, impairments, or other health problems.
2. Causes of injury, disease, impairment, or other health problems.
3. Actions taken to prevent, diagnose, treat, or manage diseases, injuries, and impairments.
4. Substances, equipment, supplies, or other items used to perform these actions.

Health care practitioners required to use HIPAA code sets will need to consult a HIPAA compliance officer in their facilities or areas for reference to HIPAA publications on coding.

Transaction Requirements

The HIPAA Transaction Standard was finalized on August 17, 2000, giving covered entities until October 16, 2003, to comply. Extensions were possible (see Table 7-3), but covered entities that applied for the extensions were required to begin testing of electronic transactions and code set standards by April 16, 2003. The Act also specified that physicians with ten or more full-time equivalent employees were required to file electronically for Medicare reimbursement, unless "no method is available" to file electronically, and in that case, such covered entities could file on paper.

electronic transmission Sending information over electronic networks.

electronic data interchange (EDI) The use of uniform electronic network protocols to transfer business information between organizations.

Complying with HIPAA Transaction Standards means that covered entities must use the HIPAA defined standards when using *electronic data interchange (EDI)* for electronic transmissions. **Electronic transmission** refers to the sending of information from one network-connected computer to another. **Electronic data interchange (EDI)** is the use of uniform electronic network protocols (formats) to transfer business information between organizations. Banking, financial, and retail businesses first began using electronic data interchange (EDI) to transmit information in the mid-1960s, and it has been the transmission method of choice for businesses since the mid-1990s.

Under HIPAA, if a health care provider conducts one of the following general categories of covered transactions electronically, they must use the HIPAA standards:

1. Claims or encounter information.
2. Eligibility requests.
3. Referrals and authorizations.
4. Claim-status inquiries.

Health plans and clearinghouses must be able to receive the above transactions and must also be able to conduct four additional transactions electronically:

1. Premium payment.
2. Claim payment and remittance advice.
3. Enrollment and disenrollment.
4. Coordination of benefits.

Since converting electronic transmissions to HIPAA standards is highly technical, health care practitioners and facilities need to rely on information technology (IT) staff or outside IT experts to be sure they are in compliance.

Advantages to using standard EDI protocols to transmit PHI electronically include

- EDI protocols ensure that protected information travels between linked computers as intended because everyone is using a common language.
- EDI protocols are compatible with firewall and encryption features that help ensure confidentiality of PHI.

There are many advantages for health care providers and consumers in using uniform transaction formats and code sets to transmit health information:

- Uniform coding ensures consistency to the language used to identify diseases.
- Uniform coding helps HHS track disease trends for public health purposes.
- Uniform coding speeds communication between payers and health care providers and speeds the payment process.
- Uniform coding ensures that covered entities can communicate without confusion and long delays.
- Uniform coding helps track how drugs are used and evaluate quality of health care.
- Once codes are learned, employees responsible for coding will find their jobs easier.

STANDARD 2: PRIVACY RULE

As the electronic age progresses, individuals have become increasingly concerned about the privacy of their medical records. However, patient fears are not the underlying reason for the HIPAA Privacy Rule. Because Congress recognized that electronic transmission of health information is the rule in today's computerized society, legislators paid particular attention to ensuring that confidentiality of medical records will not be violated through electronic transmission or storage.

permission A reason for each use and disclosure of patient information.

Health care providers and plans can use and disclose patient information (PHI), HIPAA legislators said, but they must identify a **permission**—a reason for each use and disclosure.

Court Case

U.S. Attorney General Denied Medical Records

In 2000, the U.S. Supreme Court found the Nebraska version of a partial birth abortion ban unconstitutional, on grounds that this type of abortion may, in certain circumstances, be the safest means by which a medically necessary abortion can be performed, and the Nebraska law lacked such a safety clause. (The law defines "partial birth abortion" as a method of abortion in which a second or third trimester fetus partially exits the womb and is then destroyed.)

When the U.S. Supreme Court has ruled, the matter is usually settled, but in response to the Court's Nebraska decision, Congress passed the federal Partial Birth Abortion Ban Act in 2003. Congress claimed it had made new factual findings that "partial-birth abortion is never necessary to preserve the health of a woman . . ."

Immediately after President George W. Bush signed the act, a group of abortion providers challenged it in court. A federal district judge in New York City granted the group an injunction to stop enforcement of the law. In March, 2004, however, the matter was ordered to trial to see if the Supreme Court's view of the facts still prevailed.

To defend the federal partial birth abortion ban in court, United States Attorney General John Ashcroft sought the medical records of 45 patients at a Chicago hospital. He needed the records to dispute expert testimony for the plaintiffs' case, and he claimed that because he sought the records without patient identifying information, he was not violating privacy laws.

However, on March 26, 2004, the United States District Court for the Northern District of Illinois disagreed. The court held that the Justice Department is not entitled to request patients' medical records, even with names and other identifying information removed.

In his opinion for the court, Judge Richard Posner explained that anonymity and privacy are not identical. Therefore, while the Justice Department would view the women's records without identifying information, the court still deemed their production a privacy violation.

While the court case settling the abortion providers' challenge to the federal Partial Birth Abortion Ban Act had not yet gone to court in June 2004, Ashcroft's petition to obtain medical records was denied.

Note: You can follow the progress of this case by conducting a Web search for "Northwestern Memorial Hospital v. Ashcroft."

Northwestern Memorial Hospital v. Ashcroft, (Appeal from the United States District Court, for the Northern District of Illinois, Eastern Division, No. 04 C 55, Argued March 23, 2004, Decided March 26, 2004).

To *use* PHI means that you use patients' protected health information within the facility where you work in the normal course of conducting health care business. To *disclose* PHI means that patients' protected health information is sent outside of the office for legitimate business or health care reasons.

PERMISSIONS

Using and disclosing PHI must fall within the following eleven HIPAA-defined permissions:

1. Required disclosures
   HIPAA *requires* just two types of PHI disclosures. The first is that you disclose PHI to representatives from HHS that want to see your books, records, accounts, and other documents. You must permit HHS representatives to see the documents they request, but you should ask HHS representatives to show identification, and you should record the reason for the requested disclosure to HHS. The second type of PHI disclosure that HIPAA

requires is to individual patients upon request. (See number 2. below, "Disclosures to Patients.")

Written authorization to disclose PHI to HHS representatives is not required.

2. Disclosures to Patients

The second disclosure HIPAA *requires* is that PHI be disclosed to any patient who asks to see his or her own medical records. (Unless the health care provider believes that access will do harm to the patient.) This includes talking to the patient about his or her diagnosis, treatment, and medical condition, as well as allowing the patient to review his or her entire medical record. There are exceptions, however. Patients do not have the right to access

- Psychotherapy notes (See below for a definition of *psychotherapy notes*.).
- Records that are being compiled for a civil, criminal, or administrative action.
- Records that are exempt from the Clinical Laboratory Improvement Act of 1988 (CLIA). CLIA requires clinical labs to disclose test results or reports only to authorized persons—usually the person who ordered the test.

If you deny access to PHI to a patient, a review process may be instituted to determine whether or not you acted reasonably. However, under HIPAA, a patient cannot challenge a decision to deny access to his or her PHI if

- Any of the above restrictions exist.
- The patient is a prison inmate.
- PHI was obtained through clinical research that includes treatment. This applies only during the research and only if limitation of access is agreed to in advance.
- The PHI is a government record.
- The PHI was obtained under a promise of confidentiality.

Decisions to deny access to a patient's PHI may be reviewed when challenged if

- The patient will be harmed if access is withheld.
- Someone else is mentioned in the record and that person will be harmed if access is withheld.
- The person making the request is the patient's personal representative, and you believe the patient or someone else may be harmed if the personal representative is allowed access.

Written authorization to disclose PHI to patients (as when a patient asks to see his or her medical record) is recommended, and you should ask to see identification for individuals requesting disclosure.

3. Use or disclosure for treatment, payment, or health care operations (TPO)

Health care practitioners need to use PHI within the medical office, hospital, or other health care facility for coordinating care, consulting with another practitioner about the patient's condition, prescribing medications, ordering lab tests, scheduling surgery, or for other reasons necessary to conduct health care treatment or business.

PHI may also be disclosed within a facility for the purpose of obtaining information about a patient's insurance coverage, inquiring about copayments, billing, claims management, and so on.

Health care operations—those activities the provider participates in that relate to business functions—may also require disclosure of PHI. These

activities include quality assessments, case management, care coordination, contacting providers and patients with alternative treatment information, certification, accreditation, licensing or credentialing, medical reviews, legal service, auditing for fraud and abuse and for other purposes, and so on.

PHI disclosures for this purpose do not require written authorization.

4. Others' treatment, payment, operations
   If other covered entities contact you or your employer for access to PHI, such as insurance plans, attorneys, medical survey representatives, and pharmaceutical companies, you must have the patient's written authorization to release PHI.
5. Personal representatives (friends, family)
   Use professional judgment to determine if a family member, friend, or personal representative is participating in the care of a patient. For example, you saw the patient invite another person into the exam room, or you heard the patient ask that individual to pick up his or her prescription. You may share information with these individuals, in proportion to their involvement in the care of the patient. You should verify with the patient, if possible, before sharing information. If the patient objects, honor his or her wishes

   If a person claims to have the legal right to make medical decisions for a patient, including the right to review medical records, ask to see the legal document, and verify the representatives' identity. A signature authorizing disclosure is recommended. If the patient is able, you can also verify with the patient.
6. Disaster relief organizations
   Unless the patient objects, health care providers may disclose PHI to persons performing disaster relief notification activities. If the situation involves TPO, no authorization is needed.
7. Incidental disclosures
   In December 2002, HHS released guidelines for clarifying when incidental disclosures of PHI are permitted without authorization from patients. For example, permitted disclosures include
   - Nursing care center staff members can speak about patients' care if they take reasonable precautions to prevent unauthorized individuals, such as visitors in the area, from overhearing.
   - Nurses and other health care practitioners can talk to patients on the phone or discuss patients' medical treatment with other providers on the phone if they are reasonably sure that others cannot overhear.
   - Health care practitioners can discuss lab results with patients and other health care practitioners in a joint treatment area if they take reasonable precautions to ensure that others cannot overhear.
   - Health care practitioners can leave messages on answering machines or with family members, but information should be limited to the amount necessary for the purpose of the call. (For detailed messages, it may be prudent to simply ask the patient to return a call.)
   - You can ask patients to sign in, and you can call patients by name in waiting rooms, but a sign-in sheet must not ask for the reason for the visit.
   - You can announce patients by name in a waiting room or use a public address system to ask patients to come to a certain area.
   - You can use an X ray light board at a nursing station if it is not visible to unauthorized individuals in the area.
   - You can place patient charts outside exam rooms if you use reasonable precautions to protect patient identity: face the chart toward the wall or place the chart inside a cover while it is in place.

8. Public purpose
   Health care practitioners and facilities may be asked to disclose PHI "for the public good." If a state law does not prohibit releasing specific PHI, HIPAA allows this type of disclosure without patient authorization. Such disclosures include
   - When disclosure is required by law. You should limit the PHI disclosed to the requirements of the law. Verify identification of representatives asking for PHI.
   - Public health authority. Public health representatives are authorized by law to collect information to prevent or control disease, injury, birth, death, and for other public health investigations.
   - Child abuse or neglect. You may release this information to public health authorities that are authorized to receive reports of child abuse or neglect.
   - Victims of abuse, neglect, or domestic violence. If a health care practitioner has reason to believe a patient is a victim of abuse, neglect, or domestic violence, he or she may disclose PHI if
     - The disclosure is required by law.
     - The individual agrees to disclosure.
     - The disclosure is necessary to prevent serious harm, or the individual is physically or mentally unable to consent to disclosure. If disclosed in this situation, health care practitioners must notify the patient that they made the disclosure.
   - Food and Drug Administration (FDA). Health care practitioners may disclose PHI to the FDA for safety, quality, or effectiveness such as reporting adverse events, product defects, product recalls, or monitoring patient response to a drug.
   - Communicable diseases. If authorized by law to notify persons who may have been exposed to a communicable disease or are at risk of spreading a disease, health care practitioners may disclose PHI.
   - Employee workplace medical surveillance. Health care practitioners may disclose PHI to a patient's employer under certain conditions. Consult the privacy officer for those conditions.
   - Health oversight activities. These activities include audits, investigations, inspections, licensure, and disciplinary actions. You cannot disclose PHI about the person who is the subject of an investigation.
   - Judicial and administrative proceedings. HIPAA adds special criteria that must be included in most subpoenas. Court orders generally have no additional criteria added by HIPAA. Consult your privacy official or your legal department if you receive a subpoena or court order to release PHI.
   - Law enforcement. There are eight circumstances that apply concerning the disclosure of PHI to law enforcement officials:
     - required by law, such as gunshot wounds, child abuse or neglect, or domestic violence.
     - warrant or process.
     - government agency request.
     - identifying a suspect or material witness.
     - victims of a crime.
     - suspicious death.
     - crime on the premises.
     - medical emergency.

Consult your privacy official or legal department if law enforcement representatives ask for PHI.

- Coroners and funeral directors. You may disclose PHI to a coroner or medical examiner to identify a deceased person and to funeral directors to help them carry out their duties.
- Organ, eye, or tissue donation. You can disclose PHI to appropriate agencies to facilitate organ and tissue donations.
- Research. Consult your privacy officer for special conditions that apply.
- Avert a serious and imminent threat to health or safety. You can disclose PHI if you believe a serious and imminent threat to health or safety exists.
- Special government functions. Special circumstances apply to individuals in the military, veterans, and prison inmates. Consult your privacy officer to determine the appropriate response.
- Workers' compensation. You can disclose PHI to comply with state workers' compensation laws.

9. Authorization
   A valid patient authorization allows you to disclose PHI. Use or disclose PHI as limited by the authorization. When in doubt, check with the privacy officer, and always document use or disclosure and those instances when access to PHI is denied.
10. De-identification
    You can disclose certain types of patient information when identifying information has been removed, because once the identifiers have been removed, the data is no longer considered protected by the HIPAA regulation. Check with your privacy officer for circumstances that require de-identification.

Check Your Progress

7. Briefly summarize the four HIPAA standards.

8. Which of the four standards is most concerned with confidentiality of medical records?

9. What are the two required disclosures of health care information that HIPAA mandates?

10. What information must be included in health care facility privacy notices?

limited data set Protected health information from which certain patient identifiers have been removed.

11. Limited data set
A **limited data set** is protected health information from which certain specified, direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into an agreement promising specified safeguards for the protected health information within the limited data set.

SPECIAL REQUIREMENTS FOR DISCLOSING PROTECTED HEALTH INFORMATION

As discussed above, each use and disclosure of PHI must fall within one of the eleven permissions. However, before using or disclosing PHI you must also review any special restrictions that were agreed to and requirements for disclosing information for certain purposes, such as marketing or fund-raising. These special requirements are

verification Verify the identification of anyone requesting patient information.

1. **Verification**
Ask any person who requests access to PHI to show identification if the request is made in person. If a person asks over the telephone for you to fax PHI and you don't know that person, use common sense. If a patient is making the request, ask for information that you can verify by checking the medical record. If an outside company representative, such as an insurance employee is making the request, say you will return the call, and call the insurance office's business telephone number (not a number the caller gave you) to verify that the employee works there. Once you have verified that a patient has made the request, or that the request is legitimate, call the receiving office to say you are faxing PHI. Fax only the information the patient has requested from the medical record. After you send the fax, request confirmation that it was received. Note the request in the patient's record.

minimum necessary The limited amount of patient information to be disclosed, depending on circumstances.

2. **Minimum Necessary**
This refers to the limited amount of patient data that may be disclosed as required by circumstances. For example, within a medical office a receptionist may only need to know that a patient's insurance information is up to date. An insurance clerk may only need to know a patient's insurance coverage. A billing clerk may only need to know the patient's co-pay and related contact information. The insurance company only needs to access those portions of the medical record that concern the reason for a patient's visit. (The company does not need the entire medical record, for instance, to pay for a child's immunization visit.)

When responding to requests to provide PHI, remember to provide only the information the patient has requested and to provide only the information necessary for workplace duties to be fulfilled. Everyone requesting information does not need to see a patient's entire medical record. If a patient has requested, in writing, that certain individuals not be allowed access to his or her PHI, you must honor the request. Therefore, before disclosing PHI, check the patient's record for special requirements. Always use the "minimum necessary" standard when disclosing PHI.

3. Marketing
Pharmaceutical and survey companies and other organizations may request patient information in order to target marketing efforts toward certain

patient groups or to communicate general health information. These disclosures are not generally allowed without a patient authorization.

Communications such as mammogram reminder mailings, newsletters about childhood vaccinations, or news about health fairs and classes are not considered marketing and may be conducted without a patient authorization, although if they request that you stop such communications, you should honor their request. If you have the patient's authorization to send additional marketing materials, you may do so. These authorizations are commonly granted at the time of treatment, but you may not make treatment dependent upon signing the authorization. Consult your privacy officer before using patient lists for nontreatment, payment, or healthcare operations communications.

4. Psychotherapy Notes
HIPAA defines *psychotherapy notes* as those notes that are
   1. Recorded by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session.
   2. Maintained separately from the medical record.

   Protected psychotherapy notes do *not* include
   a. Medication prescription and monitoring.
   b. Counseling session start and stop times.
   c. The modalities and frequencies of treatment furnished.
   d. Results of clinical tests.
   e. Any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

   Health care providers may *not* use or disclose psychotherapy notes for any purpose, including most treatment, payment, or health care operations, without written authorization from the patient. Exceptions include
   - The person who originated the notes wants to review them.
   - Counseling training programs want to use PHI to help trainees improve their skills.
   - Using the notes as a defense in a legal action or other proceedings brought by the patient.
   - The Secretary of HHS wants to see them.
   - Use or disclosure is required by law.
   - A health care practitioner needs to report a serious threat to health or safety, under specific conditions.

   Consult your privacy officer for guidance if you are asked to disclose psychotherapy notes.

5. Policies and Procedures Consistent with Notice of Privacy Practices
HIPAA requires health care providers to have in place written policies and procedures on how to handle privacy. These internal policies and procedures must be consistent with the written privacy notification provided to every patient. If you work in a dentist's office, for example, and you will send appointment reminders to patient's, the practice's privacy notification must state that the reminders will be sent. HIPAA compliance officers and privacy officers can provide advice on how to implement consistent privacy policies and notifications.

6. State Laws
All HIPAA compliance policies and procedures must be consistent with both state and federal laws. If state and federal laws conflict, you must follow the law that offers either the greater privacy protection or that which offers more patient rights. If state laws are more stringent or offer more

patient rights than federal laws, the state law must be followed. Conversely, if HIPAA conflicts with state laws, and HIPAA is more limiting or grants more patient rights, follow the HIPAA regulations. Consult HIPAA compliance officers, privacy officers, and attorneys to develop consent forms compatible with laws in your state.

The following Court Case was adjudicated after HIPAA was passed in 1996 but before it was fully implemented by health care practitioners nationwide:

Court Case

EMT Liable for Violating Patient's Privacy

An EMT employed by a volunteer fire department provided emergency treatment to a female patient for a drug overdose or possible overdose. The unresponsive patient was transported to a hospital. The EMT returned home and later spoke to a friend, telling her that she had assisted in taking a specific patient to the hospital emergency room for a possible overdose.

Prior to the emergency the EMT had never met the patient. However, about two weeks prior to the incident, the EMT heard about the patient and her medical problems at a social event. The woman who spoke about the patient was apparently a friend, and it was this person that the EMT telephoned after the patient's overdose.

The patient sued the EMT and her insurance company, alleging that she had defamed her and violated her privacy by publicizing information concerning her medical condition and making untrue statements indicating that she had attempted suicide. The patient claimed that she had been and was continuing to undergo medical care due to illness and that the apparent overdoes she suffered was a "reaction to medication."

The insurance company claimed the EMT's actions were within the scope of her employment. The EMT argued that she had not acted recklessly or unreasonably in contacting the patient's friend regarding her care.

The EMT offered to settle for $5,000, but the plaintiff refused, and the matter went to a jury trial. The jury found that the EMT had violated the plaintiff's right of privacy, as alleged. The jury also awarded the plaintiff/patient $37,909.86 in compensatory damages and attorney fees.

The EMT and her insurance company appealed. An appeals court upheld the judgment of the lower court.

Pachowitz v. Ledoux, 2003 WL 21221823 (Wis.App., May 28, 2003).

PATIENT RIGHTS

HIPAA has also put in writing six important patient rights that must be explained in health care provider privacy notifications, and health care providers may not ask patients to waive their rights. These rights are found in Table 7-4.

TABLE 7-4 Patients' Rights Under the HIPAA Privacy Rule

Patient Right	Comments	Documentation Required	Documentation Recommended
Access to medical records and the right to copy them.	Access to records is guaranteed under HIPAA, but there are some limitations, as mentioned above.	No.	Yes.
Request for amendment to designated record set.	A patient has the right to request amendments to his or her PHI or other personal information. Unless a provider has grounds to deny the request, amendments must be made.	Yes.	
Request for an accounting of disclosures of PHI.	You are required to account for certain disclosures. Check with your privacy officer for a list. You have up to 60 days to provide the disclosure list.	Yes. Always keep a record of the appropriate disclosures, and make a copy of the disclosure report for the patient's file.	
Request to be contacted at an alternate location.	Patients can request to have you contact them at places other than work or home. You can deny the request if you cannot reasonably comply.	Yes. Obtain a request from the patient in writing. Note in the patient's electronic medical record and in a paper communication for staff members who do not have access to the patient's electronic medical record. Document reasons for denying the request if it is denied.	
Requests for further restrictions on who has access to PHI.	A patient can request that certain persons or entities do not have access to his or her medical record. You may deny the request if you cannot reasonably comply.	Yes. Ask the patient to complete an opt-out form that is then filed with electronic and paper records. Document reasons for denying the request if it is denied.	
Right to file a complaint.	Enforcement of the Privacy Rule is complaint-driven. Patients should be encouraged to work first with the provider. Retaliation is prohibited.	Yes. Refer the complaint to the Privacy Officer. Document the complaint in a privacy complaint log. Evaluate the complaint and determine how best to solve it.	

STANDARD 3: SECURITY RULE

security Policies and procedures used to protect electronic information from unauthorized access.

Privacy refers to those policies and procedures health care providers and their business associates put in place to ensure confidentiality of electronic, written, and oral protected health information. **Security** refers to those policies and procedures health care providers and their business associates use to protect electronically transmitted and stored PHI from unauthorized access. The Security Rule was finalized on February 20, 2003. The compliance date for covered

entities was listed as April 20, 2005. For small health plans, the compliance date was April 20, 2006.

Maintaining security of electronic data is complex, and specific technical knowledge and experience is required to implement the requirements of this rule. The Security Rule is flexible, allowing small health care providers to use different security procedures than larger providers. All health care providers must conduct security risk assessment surveys to determine their specific vulnerabilities, and to determine the appropriate response. Security aspects that must be considered include

- Has a security officer for the practice been appointed?
- Are passwords that allow access to electronic information protected?
- Risk assessment should include evaluating how each person protects the password.
- Passwords should not be posted for all to see.
- Passwords should not be unnecessarily divulged to others.
- Are appropriate security measures, such as firewalls, encryption, and antivirus software in place, and are they checked and updated regularly?

For example, some covered entities and their business associates use private networks that are not subject to traffic and security problems common with Internet use. Telecommunications networks that transmit electronic data from business to business are often direct links between senders and receivers, called *value-added networks (VANs)*. VANs operate over dedicated, secure communication lines leased from the telephone company especially for this purpose.

firewalls Hardware or software designed to prevent unauthorized access to electronic information.

encryption Coded information that cannot be read until it is decoded.

Other entities and associates use the Internet, but they use **firewalls** (hardware or software designed to keep out unauthorized users) and encryption software to keep information private. **Encryption** software translates information into a code that can be decoded by the recipient but cannot be read by unauthorized viewers.

- Are security measures "reasonable and appropriate" for the health care practice and are they periodically reviewed?
- Have security breaches occurred in the past? If so, what caused the breaches, and have causes been remedied?
- Are security measures in place for business associates that have access to PHI?
- Have staff members been trained in maintaining security of electronic information?
- Are internal sanctions in place for security breaches, and have staff members been informed of such sanctions?

As stated earlier, the implementation of the HIPAA security rule can be a technically daunting task. It is best to involve the appropriate technical person or department as early as possible in the process to ensure the appropriate security level has been achieved and documented.

STANDARD 4: NATIONAL IDENTIFIER STANDARDS

The purpose of the National Identifier Standards is to provide unique identifiers (addresses) for electronic transmissions. Just as websites you visit on the Internet have unique "addresses," called Uniform Resource Locators (URLs), when this standard is fully implemented, certain health care-related entities will have standard identifying numerical or alphanumerical addresses.

These identifiers will be kept in a central databank and will include unique "addresses" for employers, providers, and health plans. See Table 7-3, "HIPAA Standards and Timelines," for implementation dates and details.

FREQUENTLY ASKED QUESTIONS ABOUT HIPAA

For fear of government prosecution, HIPAA compliance overkill has been a problem in some cases. Myths and misinterpretations must often be dispelled as health care providers implement HIPAA standards and rules. For example, it is not true in all cases that health care providers cannot issue the names of hospital patients and patient condition updates to family members. Nor is it true that health care providers cannot correspond about a patient's care or that police 911 dispatchers cannot give EMTs a patient's name. Here are a few frequently asked questions about HIPAA provisions that can help dispel myths:

Q: May one physician's office send a patient's medical records to another physician's office without the patient's consent?

A: Yes

Q: Does the HIPAA Privacy Rule prohibit or discourage doctor/patient e-mails?

A: Health care practitioners can continue to correspond with patients via e-mail, but appropriate electronic safeguards must be in place.

Q: May a patient be listed in a hospital's directory without the patient's consent, and may the directory be shared with the public?

A: The HIPAA Privacy Rule allows hospitals to continue providing directory information to the public, unless the patient has specifically chosen not to be included. Hospital directories can include the patient's name, location in the facility (such as hospital floor and room number), and condition in general terms. The information can also be disclosed to callers who ask for the patient by name, but the patient must be informed in advance of this use and disclosure and must have the opportunity to opt out.

Q: May clergy members learn whether members of their congregation or religious affiliation are hospitalized?

A: Hospitals may continue disclosing directory information to members of the clergy, unless the patient has objected to such disclosure.

Q: Is a hospital allowed to share patient information with the patient's family without the patient's express consent?

A: HIPAA provides that a health care provider may "disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual," medical information directly relevant to such person's involvement with the patient's care or payment related to the patient's care.

Q: May a patient's family member pick up prescriptions for the patient?

A: The Privacy Rule allows family members or others to "pick up filled prescriptions, medical supplies, X rays, or other similar forms of protected health information."

Q: Does the Privacy Rule mandate many new disclosures of PHI?

A: HIPAA *requires* just two disclosures of PHI: One to HHS representatives who ask to review provider information and the second to patients who ask to review their own medical records. Disclosure is permitted, but not mandated in other situations, as discussed above.

Q: Is the HIPAA Privacy Rule prohibitively expensive to implement?

A: A 2002 White House report estimated the costs of implementing privacy over ten years at about $18 billion. Savings incurred through implementation were estimated at about $29.9 billion over ten years. However, some sources disagree with these figures, estimating it could cost around $43 billion over ten years for health care providers to comply with HIPAA.

Q: Can patients sue health care providers who do not comply with the HIPAA Privacy Rule?

A: The HIPAA Privacy Rule does not give patients the express right to sue. Instead, the person must file a written complaint with the Secretary of Health and Human Services through the Office for Civil Rights. The HHS Secretary then decides whether or not to investigate the complaint. Patients may have other legal standings to sue, under state privacy laws.

Q: Are there legal penalties for health care providers who violate the HIPAA Privacy Rule?

A: HHS may impose civil penalties ranging from $100 to $25,000 per offense. The U.S. Department of Justice may enforce criminal sanctions ranging from $50,000 to $250,000 for each offense with corresponding prison terms.

Q: If a patient refuses to sign an acknowledgment stating that he or she received the health care provider's notice of privacy practices, must the health care provider refuse to provide services?

A: The Privacy Rule gives the patient a "right to notice" of privacy practices for protecting identifiable health information. It requires that providers make a "good faith effort" to have patients acknowledge receipt of the notice, but the law does not give health care practitioners the right to refuse treatment to people who do not sign the acknowledgement.

Q: May the media still access public information from hospitals about accident or crime victims?

A: HIPAA lets hospitals continue to make public certain patient directory information as specified above in the question about hospital directories. If the patient specifically opts out of having such information made public, then the hospital must respect his or her wishes.

Q: If I need emergency assistance from the police or fire department, is the 911 dispatcher prohibited from giving my name to rescue units or EMTs?

A: No. Names and addresses should be given to rescue or EMT staff for help in locating patients and treating their medical problems as quickly as possible.

Q: As a patient, how can I protect the privacy of my health care information?

A: Privacy experts recommend that you

- Read notices of privacy practices carefully to become aware of the uses and disclosures of your information that may be made.
- Tell your health care provider your confidentiality concerns.
- Ask how large health care organizations share your information.
- Read authorization forms carefully before you sign; edit them to limit the sharing of information if you wish. Initial and date your revisions.
- Register your objection to disclosures you consider inappropriate. You can file a complaint with the provider, plan, or Department of Health and Human Services.
- Request a copy of your medical record, and review it carefully to be sure the information is correct. You can request amendments or corrections.

- Be cautious when visiting websites. If you participate in surveys or health screenings on medical information websites, look for and read privacy policies. Don't participate if you don't know how the information will be used and who will have access to it.
- Request a copy of your file from the Medical Information Bureau (MIB). MIB is an organization of insurance companies. MIB compiles reports on individuals with serious medical conditions or other factors that could affect longevity, such as participating in dangerous sports. If MIB has a file on someone, that person has a right to see and correct misinformation in the file. To obtain a copy of your file, if one exists, contact MIB Inc., P. O. Box 105, Essex Station, Boston MA 02112; (617) 426-3660; www.mib.com.
- Educate yourself about medical privacy issues.

Providers' HIPAA compliance and privacy officers are best qualified to answer specific questions about HIPAA and medical privacy. Other sources include

Websites

- www.hhs.gov/ocr/hipaa
- www.hhs.gov/ocr/privacysummary.pdf
- www.hhs.gov/news/facts/privacy.html
- www.healthprivacy.org
- www.ama-assn.org/ama/pub/category/4234.html (Or at www.ama-assn.org, do a search for HIPAA to reach the current page.)

Publications

Kevin Beaver, Rebecca Herold, *Practical Guide to HIPAA Privacy and Security Compliance,* (CRC Press, 2003).

Carolyn P. Hartley, MLA, CHP, & Edward D. Jones III, *HIPAA Plain & Simple: A Compliance Guide for Health Care Professionals* (AMA Press, 2004).

Carolyn Hartley, David C. Kibbe, Jan Root, Michael Hubbard, *Field Guide to HIPAA Implementation, Revised Edition,* (AMA Press, 2003).

Uday Ali Pabrai, *Getting Started With HIPAA,* (Premier Press, 2003).

Ethics Guide

Privacy Law and HIPAA

Confidentiality

Information patients disclose to physicians and other health care practitioners during the course of the relationship between physician and patient is confidential to the greatest possible degree. Patients should feel free to make full disclosures of information so that effective care can be provided.

The obligation to safeguard patient confidences is subject to certain exceptions which are ethically and legally justified because of overriding social considerations including

- When a patient threatens to inflict serious bodily harm to another, and there is a reasonable probability that he or she may carry out the threat.
- Communicable diseases and gunshot and knife wounds should be reported as required by applicable statutes or ordinances.

Confidentiality of Medical Information Postmortem

All medically related confidences disclosed by a patient to health care practitioners and information contained within a deceased patient's medical record, including information entered postmortem, should be kept confidential to the greatest possible degree. Ethical and legal exceptions include

- Imminence of harm to identifiable individuals or the public health.
- Potential benefit to at-risk individuals or the public health (as in communicable or inherited disease prevention or treatment.
- Any statement or directive made by the patient regarding postmortem disclosure.
- The impact disclosure may have on the reputation of the deceased patient.
- Personal gain for the physician or other health care provider that may unduly influence professional obligations of confidentiality.

When a family member or other authorized representative has given consent to an autopsy, physicians may disclose the results of the autopsy to the individual who granted consent to the procedure.

Confidentiality of HIV Status on Autopsy Reports

HIV status on autopsy reports should be held confidential to the greatest extent possible.

Physicians who perform autopsies or who have access to autopsy information regarding a patient's HIV status should be familiar with state law governing

1. The reporting of HIV and AIDS to public health authorities.
2. Obligations to inform third parties who may be at risk for HIV infection through contact with an HIV-infected decedent.
3. Other parties to whom reporting may be required (i.e., funeral directors, health care personnel involved in the care of the patient).
4. The extent of confidentiality of autopsy records.

HIV status which appears on autopsy records is part of the decedent's medical record and should be held confidential. In the case of suspicious, accidental, or unexplained death HIV status which appears on autopsy records should be kept confidential where autopsy records are not accessible to the public. In cases where state law mandates that the autopsy information be accessible to the public, then physicians should comply with state law. However, in these instances, HIV status should only be recorded when the HIV status of the decedent would be relevant to determining the patient's cause of death. Although a patient's HIV status may be learned from public records in some jurisdictions, it is still unethical for a physician to make a public disclosure of an individual patient's HIV status independent of the legal requirements governing the filing or processing of autopsy records. The physician should comply with state laws regarding disclosure to public health authorities and at-risk third parties. Where such laws are absent, the physician should fulfill ethical obligations to notify endangered third parties (i.e., sexual and needle-sharing partners). This includes reporting to organ or tissue procurement agencies if any parts of the decedent's body were taken for use in transplantation.

Health Care Fraud and Abuse

The following guidelines encourage physicians to play a key role in identifying and preventing fraud:

1. Physicians must renew their commitment to Principle II of the American Medical Association's Principles of Medical Ethics which states that

"a physician shall deal honestly with patients and colleagues, and strive to expose those physicians deficient in character, competence, or who engage in fraud or deception."

2. Physicians should make no intentional misrepresentations to increase the level of payment they receive or to secure non-covered health benefits for their patients.

Confidentiality: Insurance Company Representative

History, diagnosis, prognosis, and other information acquired during the physician-patient relationship may be disclosed to an insurance company representative only if the patient or a lawful representative has consented to the disclosure. A physician's responsibilities to patients are not limited to the actual practice of medicine. They also include the performance of some services ancillary to the practice of medicine, including certification that the patient was under the physician's care and commenting on the diagnosis and therapy administered in a particular case.

Discussion Question

1. With the implementation of HIPAA, an extensive federal law mandating certain privacy and security precautions, is privacy for protected health information now guaranteed? Explain your answer.

2. You are the medical office employee responsible for giving patients your employer's privacy notice. Even though you have explained why an elderly patient has been given the privacy notice, he complains about yet another "health care form" and refuses to read it. How will you respond?

3. A young man who died in a car accident is infected with HIV. His driver's license certifies him as an organ donor and his parents, unaware of his HIV status, give permission for his organs to be donated. As the person who must speak with the decedent's parents, how will you handle this situation?

4. The health care practitioners listed below have followed the letter of HIPAA law. Have they also acted ethically? Explain why or why not.

   A patient asks to see her medical records and a medical office records assistant complies but slams the records down in front of the patient and mutters about being "too busy" for this service.

A physician does not refuse to see a patient who has refused to complete his notification preference form, but his abrupt manner discourages the patient from continuing to see the physician.

A patient asks for a list of disclosures his physician has made of his health information within the past six years, and he is asked to submit his request in writing.

The person responsible for faxing a patient's protected health information from one physician's office to another sends the information to the wrong fax number.

Review & Case Studies

Applying Knowledge

Answer the following questions in the spaces provided.

1. HIPAA stands for _____.
2. The department of the federal government responsible for supervising HIPAA compliance and implementation is _____.
3. Patient complaints about privacy must be directed to which government agency?

   _____

4. Which federal government agency deals with compliance and implementation of the National Identifier Standard?

   _____

5. What is the determining factor in deciding whether or not health care providers are considered *covered entities* under HIPAA?

   _____

   _____

   _____

6. What is an *electronic transmission,* and how and why does HIPAA address it?

   _____

   _____

7. What is the primary objective of Administrative Simplification?

   _____

   _____

8. Which of the four HIPAA Standards addresses Administrative Simplification?

   _____

   _____

9. A document that informs patients on how a health care provider intends to use and disclose patient information and also informs patients of their rights is called

   _____

   _____.

10. Protected health information (PHI) refers to

    _____

    _____.

11. If a state law and HIPAA's federal law disagree, which law should you follow?

_____

12. The primary reason for the Security Rule is

_____.

Circle the correct answer for each of the following multiple choice questions.

13. A *business associate* is

- **a.** A person, group, or organization outside the medical practice that has a HIPAA-approved reason to see protected health information.
- **b.** A health care practitioner's financial advisor.
- **c.** Anyone who sells products related to health care.
- **d.** None of the above

14. You could unintentionally expose content on your personal computer or your employer's system network by

- **a.** Shopping on the Internet while you are at work.
- **b.** Downloading games from the Internet.
- **c.** Sending and receiving unsecured e-mails to and from friends.
- **d.** All of the above

15. If a patient complains that his privacy was breached, what should you ask that he or she do?

- **a.** Call a lawyer.
- **b.** Speak to your privacy officer to try to handle the complaint in the office.
- **c.** Immediately file a complaint with the Office for Civil Rights.
- **d.** Discuss the problem with someone else in the office.

16. Which of the following are the Privacy Officer's responsibilities?

- **a.** Researching the Privacy Rule.
- **b.** Helping to develop the Notice of Privacy Practices.
- **c.** Training staff on privacy policies and procedures.
- **d.** All of the above

17. Which of the following are *not* covered by HIPAA's Security Rule?

- **a.** The content of all documents pertaining to patient privacy.
- **b.** Maintaining electronic security for networked computers.
- **c.** Using HIPAA standards for electronic transmission of protected health information.
- **d.** None of the above

18. Which of the following is *not* considered marketing under HIPAA provisions?

- **a.** A pharmaceutical company wants to send special mailings to a provider's diabetic patients to announce a new blood-sugar testing device.
- **b.** A reminder to female patients when mammograms should be scheduled.
- **c.** Cholesterol screening results sent to patients through the mail.
- **d.** None of the above are considered marketing under HIPAA.

19. Which of the following is *not* a violation of HIPAA's Privacy Rule?

- **a.** You call across a crowded waiting room to tell a patient he has forgotten his prescription for dilantin, a drug used to control seizures.
- **b.** You are a medical assistant for a physician's private practice, and you tell a friend, who is a bank teller, that a mutual friend has seen your employer and is pregnant.
- **c.** A telephone caller identifies himself as an insurance plan representative and requests PHI. You do not know the caller, but you comply.
- **d.** All of the above are violations of HIPAA's Privacy Rule.

20. An unauthorized person (a computer hacker) manages to access the computers in the hospital where you work and downloads information. Who is the most likely person to handle the disaster?

- **a.** The Privacy Officer.
- **b.** The hospital administrator.
- **c.** The Security Officer.
- **d.** The medical records supervisor.

Match each description that follows with the correct answer by writing the appropriate letter in the space provided.

_____ **21.** The HIPAA-mandated standard for electronic transmissions.

_____ **22.** A valid reason to disclose protected health information.

_____ **23.** This person evaluates, manages, and reports on the security of a health provider's electronic data.

_____ **24.** Networks closed to the Internet that are provided by the telephone company.

_____ **25.** Covered entities.

_____ **26.** Covered transactions.

_____ **27.** Refers to providing only as much patient information as needed for a request or to conduct health care business.

_____ **28.** One of two types of PHI access mandated by HIPAA.

_____ **29.** One of a patient's six rights mandated by HIPAA.

_____ **30.** To remove patient-identifying information from PHI.

- **a.** File a complaint
- **b.** value-added networks
- **c.** physicians and pharmacists
- **d.** minimum necessary
- **e.** de-identify
- **f.** billing patients and filing insurance claims
- **g.** HIPAA representatives ask to see PHI
- **h.** Security Officer
- **i.** Privacy Officer
- **j.** permission
- **k.** Electronic Data Interchange (EDI)

Answer the following questions by placing "T" for True and "F" for False in the blank spaces.

_____ **31.** Under HIPAA, each patient will receive just one privacy notice, no matter how many health providers he or she has seen after April 14, 2003.

_____ **32.** Patients may have copies of a provider's privacy notice to file in his or her private records.

_____ **33.** HIPAA states in plain English that patients have *no* rights to sue health care practitioners.

_____ **34.** HIPAA requires every health care provider to become 100% compliant.

_____ **35.** HIPAA provides civil and criminal sanctions for those who violate the Privacy Rule.

_____ **36.** Health care providers should establish internal sanctions for privacy and security violations.

_____ **37.** The Privacy Rule protects PHI only in electronic form.

_____ **38.** If a patient requests you amend a medical record, you are required to do so.

_____ **39.** If a patient requests that you provide an accounting of disclosures, you do not have to account for disclosures for treatment, payment, and health care operations.

_____ **40.** You should feel comfortable sharing your password with others in the medical office, especially if the physician gives you his password.

Case Study

Use your critical-thinking skills to answer the questions that follow each of the case studies.

Mona frequently travels for her job, and even when she is in town, she's usually reached most easily on her mobile phone. She has three teenagers at home and doesn't want them to pick up her health care messages. She also wants her medical bills sent to her work address.

41. What should Mona's health care provider do to accommodate her requests?

_____

_____

Lewis received a basketball scholarship to attend college, and he signed a form giving the university health service permission to access his health care records. Lewis now wants to know what is included in his health care records.

42. What should Lewis's health care provider do?

_____

Shirley, an EMT, is off duty and is driving her private vehicle on the interstate in a snow storm. The car ahead of Shirley hits an icy patch and skids off the road, overturning as it hits the ditch. Shirley stops to help and dials 911 on her mobile phone. The lone woman in the wrecked car has scratches and bruises and an obviously broken arm. While Shirley is helping the woman, a news van stops and a television reporter films the wreck for the evening news. The injured driver refuses to answer questions, so the reporter turns to the EMT who knows the injured driver's name.

43. May the EMT tell the television reporter the injured woman's name without violating federal law? Why or why not?_____

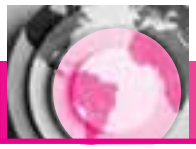
44. Rescue services arrive while the television reporter is there. Can the ambulance attendants, also EMTs, tell the television reporter the apparent extent of the woman's injuries? Why or why not?

_____

45. You are a nurse and a teenaged patient's mother tells you she wants access to her daughter's medical records. What will you do?

_____

_____



INTERNET ACTIVITIES

Complete the activities and answer the questions that follow:

46. Rush Limbaugh, a conservative radio talk-show host based in Florida, made national headlines when his hearing was restored via a cochlear transplant. Then in 2002, Limbaugh came under investigation for possible violations of Florida's "doctor shopping" law, which makes it illegal to secretly obtain overlapping prescriptions from different doctors. Limbaugh had admitted publicly in October 2003 to a painkiller addiction as the result of chronic back pain.

Although Limbaugh was not charged with a crime, prosecutors seized his sealed medical records with search warrants and won a judge's permission to review them. Limbaugh sued for invasion of privacy, maintaining that prosecutors seized his entire medical records and had no use, for example, for records pertaining to his ear examination.

In June 2004, the case had not been settled. For updates, check www.sun-sentinel.com for articles regarding the lawsuit, or do a Web search for "Rush Limbaugh" AND "medical records."

What is the current status of the case?

_____

In your opinion, based on what you have read in the articles you found about Florida's laws regarding privacy of medical records, did Limbaugh have a good case for violation of privacy? Why or why not?

_____

_____

47. Visit www.hhs.gov/news/facts/privacy.html. Access "Frequently Asked Questions" and prepare a list of ten questions and answers you believe would be most helpful in an information sheet prepared for patients.