Chapter 9

Legal Aspects of Health Information Management

Chapter Outline
• Key Terms
• Objectives
• Introduction
• Legal and Regulatory Terms
• Maintaining the Patient Record in the Normal Course of Business
• Confidentiality of Information and HIPAA Privacy and Security Provisions
• Legislation That Impacts Health Information Management
• Release of Protected Health Information
• Internet Links
• Summary
• Study Checklist
• Chapter Review

Key Terms
administrative law
assault
battery
breach of confidentiality
burden of proof
call-back method
case law
civil law
Clinical Laboratory Improvements Amendments (CLIA)
common law
deposition
digital
disclosed
discovery
electronic protected health information (EPHI)
emancipated minor
crypt
HIPAA standards for privacy of individually identifiable health information

confidentiality
contempt of court
contracts
coroner
court order
covered entities
criminal law
decrypt
defendant
de-identification of protected health information (PHI)
Objectives
At the end of this chapter, the student should be able to:

- Define key terms
- Identify and define health information legal and regulatory terms
- Maintain the patient record in the normal course of business
- Maintain confidentiality of protected health information (PHI)
- Comply with HIPAA privacy and security provisions
- Interpret legislation that impacts health information management
- Appropriately release protected health information (PHI)

INTRODUCTION

Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets.

Oath of Hippocrates, 4th century, BC

This chapter discusses legal aspects of health information management (HIM) covered as part of an introductory course in health care academic programs such as coding and reimbursement, health information administration, health information technology, medical assistant, medical billing, medical office administration, medical secretary, medical transcription, and so on. For comprehensive coverage (e.g., taught as a separate course), refer to Delmar Cengage Learning’s Legal Aspects of Health Information Management by Dana C. McWay.

The following topics are covered in this chapter: legal and regulatory terms, Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security issues, release of information processing, reportable conditions and events, and the use of specialized health information (e.g., HIV). Additional information about HIPAA can be found in Delmar Cengage Learning’s HIPAA for Health Care Professionals, by Carole Krager and Dan Krager. The following legal aspects of HIM are discussed elsewhere in this textbook:

- Chapter 1: Ethics
- Chapter 2: Accreditation, regulation, and physician credentialing
- Chapter 4: Amending record entries, authentication of record entries, computer-based patient record (CPR), destruction of records, facility closure (e.g., handling patient records), incident reports, legibility of record entries, ownership of the patient record, patient record completion responsibilities, potentially compensable event (PCE), provider documentation requirements (e.g., amending the record, correcting errors, and so on), record retention laws, and timeliness of record entries
- Chapter 6: Advanced directives, consent forms, content of the patient record (e.g., The Joint Commission standards, Medicare conditions of participation, and so on), and informed consent

impeach
interrogatory
law
malpractice insurance
medical examiner
medical liability insurance
medical malpractice
negligence
Occupational Safety & Health Administration (OSHA)
Patient Safety Organization (PSO)
plaintiff
privacy
privacy rule
privileged communication
protected health information (PHI)
public law
qualified protective order
release of information log
res gestae
res ipsa loquitur
res judicata
respondeat superior
root cause analysis
security
security rule
sources of law
stare decisis
statute
statute of limitations
statutory law
subpoena ad testificandum
subpoena duces tecum
tort
treatment, payment, and health care operations (TPO)
LEGAL AND REGULATORY TERMS

A law (or statute) is a rule of conduct passed by a legislative body (e.g., federal congress) that is enforced by the government and results in penalties when violated.

- **Civil law** deals with the legal rights and relationships of private individuals and includes:
  - **Torts** (any wrongful acts for which a civil suit can be brought)
  - **Contracts** (binding agreements between two or more parties)
- **Public law** deals with relationships between individuals and government and includes:
  - **Criminal law** (crimes and their punishments)
  - **Regulations** (published rules that interpret laws)

The individual who initiates a civil complaint and has the burden of proof (responsibility for proving harm) is called the plaintiff. (There is no plaintiff in criminal law). The defendant is the individual against whom the complaint is brought. Usually a civil case is initiated when the plaintiff’s attorney files a complaint with the appropriate court and has a summons issued and served on the defendant. The defendant’s attorney files a response with the court.

Discovery is the legal process lawyers use to obtain information about all aspects of a case, and its goal is to find information that will help prepare a case for trial or settlement. An interrogatory is a form of discovery that includes a list of written questions that must be answered by the party served (either defendant or plaintiff); that party must swear, under oath, that the answers provided are accurate to the best of his or her knowledge. Answers to interrogatories are sometimes used during a trial to impeach a party, which means that if an answer to a trial question is different from that given to the same question in interrogatory format, the judge could doubt the party’s honesty. Because answers to interrogatories are prepared as a formal written document prepared by a lawyer, there is more control over how responses are delivered (as compared with being asked the same question during a deposition). As a result, depositions are sometimes preferred over interrogatories for discovery of certain types of information. A deposition is a form of discovery used to learn answers to certain questions, obtain a sworn statement from the deponent, observe a witness’s behavior and ability to testify, and discover weaknesses and strengths in each party’s case.

The health care industry is involved most often in civil cases and less often in criminal cases. However, because government is increasing its investigations into and prosecutions for health care fraud and refusing to treat patients based on financial status, the health care industry will be faced with more criminal cases. The types of civil legal actions that most typically affect the health care industry are torts and contracts. Many claims founded in tort and contract law are resolved without appearing in court.

Sources of Law

In addition to the Constitution of the United States and individual state constitutions, sources of law include:

- Administrative law
- Case law (or common law)
- Statutory law

Administrative law includes regulations created by administrative agencies of government. Regulations interpret how a law is to be enforced, and they are generally much more detailed than the law on which they are based. Federal regulations are issued as the Code of Federal Regulations (CFR), which is subdivided into 50 titles containing numerous chapters, parts, and sections (Figure 9-1).

EXAMPLE

The Centers for Medicare and Medicaid Services (CMS) is the federal administrative agency responsible for creating regulations to implement HIPAA legislation. Privacy regulations were published in the Federal Register, Volume 65, Number 250, Part II 45, Code of Federal Regulations (CFR), Parts 160 and 164—Standards for Privacy of Individually Identifiable Health Information. The regulation that clarifies which businesses must comply with the privacy rule is as follows:

160.102 Applicability

Applies to health plan, health plan clearinghouse, health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Case law (or common law) is based on judicial decisions and precedent rather than on statutes. Sometimes case law applies only to situations where the facts of a new case exactly match the facts of the
Chapter IV—Centers for Medicare and Medicaid Services, Department of Health and Human Services (Parts 400-499)

SUBCHAPTER A—GENERAL PROVISIONS
400 Introduction; definitions.
401 General administrative requirements.
405 Special programs and projects.

SUBCHAPTER B—MEDICARE PROGRAM
405 Federal health insurance for the aged and disabled.
406 Hospital insurance eligibility and entitlement.
407 Supplementary medical insurance (SMI) enrollment and entitlement.
408 Premiums for supplementary medical insurance.
409 Hospital insurance benefits.
410 Supplementary medical insurance (SMI) benefits.
411 Exclusions from Medicare and limitations on Medicare payment.
412 Prospective payment system for inpatient hospital services.
413 Principles of reasonable cost reimbursement; payment for ESRD services ...
414 Payment for Part B medical and other health services.
415 Services furnished by physicians in providers, supervising physicians in teaching settings ...
416 Ambulatory surgical services.
417 Health maintenance organizations, competitive medical plans, and health care prepayment plans.
418 Hospice care.
420 Program integrity: Medicare.
421 Intermediaries and carriers.
424 Conditions for Medicare payment.

SUBCHAPTER C—MEDICAL ASSISTANCE PROGRAMS
430 Grants to States for medical assistance programs.
431 State organization and general administration.
432 State personnel administration.
433 State fiscal administration.
434 Contracts.
435 Eligibility in the States, District of Columbia, the Northern Mariana Islands, and American Samoa.
436 Eligibility in Guam, Puerto Rico, and the Virgin Islands.
440 Services: General provisions.
441 Services: Requirements and limits applicable to specific services.
442 Standards for payment to nursing facilities and intermediate care facilities for the mentally retarded.
447 Payments for services.
455 Program integrity: Medicaid.
456 Utilization control.

SUBCHAPTER D—PEER REVIEW ORGANIZATIONS
462 Peer review organizations.
463 Utilization and quality control review.
475 Reconsiderations and appeals.
476 Acquisition, protection, and disclosure of peer review information.

SUBCHAPTER E—STANDARDS AND CERTIFICATION
482 Conditions of participation for hospitals.
483 Requirements for States and long-term care facilities.
484 Conditions of participation: home health agencies.
485 Conditions of participation: providers of specialized services.
486 Conditions for coverage of specialized services furnished by suppliers.
487 Survey and certification procedures.
489 Provider agreements and supplier approval.
491 Certification of certain health facilities.
493 Laboratory requirements.
494 Conditions for coverage of particular services.
495 Appeals procedures for determinations that affect participation in the Medicare program ...

Figure 9-1 Partial List of Code of Federal Regulations (CFR) Titles, Chapters, Subchapters, and Parts (Courtesy Delmar/Cengage Learning.)
case that was previously decided. In other cases, the court makes a decision on a general principle that may apply to many situations. Case law principles also include the following:

- **Res gestae.** Latin for “things done,” which means that hearsay statements made during an incident are admissible as evidence.
- **Res ipsa loquitur.** Latin for “the thing speaks for itself,” which means that something is self-evident (e.g., surgical instrument left in patient’s abdominal cavity).
- **Res judicata.** Latin for “the thing is decided,” which means that the final judgment of a competent court is conclusive; it prevents a plaintiff from suing on a claim that has already been decided, and it prevents a defendant from raising any new defense to defeat enforcement of an earlier judgment.
- **Respondeat superior.** Latin for “let the master answer,” which means that an employer is responsible for the legal consequences of an employee’s actions.
- **Stare decisis.** Latin for “to stand by things decided,” which means that it is a doctrine of precedent and courts adhere to the previous ruling.
- **Subpoena ad testificandum.** (Figure 9-2) A court order that requires an individual to appear in court to testify. A court order is a written command or direction ordered by a court or judge. Failure to obey a subpoena constitutes contempt of court, which is punishable by fine or imprisonment.
- **Subpoena duces tecum.** (Figure 9-3) A written command or direction, signed by the court of the clerk, ordering an individual to appear in court with documents (e.g., medical records).

**EXAMPLE**


This action was brought against the hospital to recover damages for allegedly negligent medical and hospital treatment which necessitated below the knee amputation of his right leg. The jury returned a verdict against the hospital in the sum of $150,000. This amount was reduced by $40,000, the amount of the settlement with the doctor. The judgment in favor of the plaintiff in the sum of $110,000 was affirmed on appeal by the Appellate Court for the Fourth District, which granted a certificate of importance.

On November 5, 1960, the plaintiff, who was 18 years old, broke his leg while playing in a college football game. He was taken to the emergency room at the defendant hospital where Dr. Alexander, who was on emergency call that day, treated him. Dr. Alexander, with the assistance of hospital personnel, applied traction and placed the leg in a plaster cast. A heat cradle was applied to dry the cast. Not long after the application of the cast plaintiff was in great pain and his toes, which protruded from the cast, became swollen and dark in color. They eventually became cold and insensitive. On the evening of November 6, Dr. Alexander “notched” the cast around the toes, and on the afternoon of the next day he cut the cast approximately three inches up from the foot. On November 8 he split the sides of the cast with a Stryker saw; in the course of cutting the cast the plaintiff’s leg was cut on both sides. Blood and other seepage were observed by the nurses and others, and there was a stench in the room, which one witness said was the worst he had smelled since World War II. The plaintiff remained in Charleston Hospital until November 19, when he was transferred to Barnes Hospital in St. Louis and placed under the care of Dr. Fred Reynolds, head of orthopedic surgery at Washington University School of Medicine and Barnes Hospital. Dr. Reynolds found that the fractured leg contained a considerable amount of dead tissue, which in his opinion resulted from interference with the circulation of blood in the limb caused by swelling or hemorrhaging of the leg against the construction of the cast. Dr. Reynolds performed several operations in a futile attempt to save the leg but ultimately it had to be amputated eight inches below the knee.

**Statutory law** is passed by a legislative body (e.g., Congress), and it can be amended, repealed, or expanded by the legislative body. A **statute of limitations** refers to the time period after which a lawsuit cannot be filed. Such statutes vary from state to state, and the statute of limitations for medical malpractice cases varies from one to three years. Medical malpractice results when a health care provider acts in an improper or negligent manner and the patient’s result is injury, damage, or loss. The **American Heritage® Dictionary of the English Language** defines **negligence** as the “failure to exercise the degree of care considered reasonable under the circumstances, resulting in an unintended injury to another party” (e.g., misdiagnosis, error in performing a surgical procedure, failure to recognize and treat complications, failure to obtain informed consent from a patient for treatment performed, and so on). Providers purchase **medical liability (or malpractice) insurance**, which pays a lawsuit’s covered damages (settlement amount) and defense costs (e.g., lawyer fees).
BEFORE THE DEPARTMENT OF HEALTH, STATE OF NEW YORK

JOHN DOE, )  SUBPOENA AD TESTIFICANDUM  
Petitioner, )

vs. )

RICHARD ROE, M.D. ) Case No.    NY-123456789
Respondent. )

TO: Richard Roe, M.D.

000 Medical Plaza

Anytown, U.S.A.  84100

RE: John Doe

Date of Birth:  8/28/55

YOU ARE COMMANDED to appear at the County Courthouse, 15 Main Street, Room 14A, Albany NY 00000 on or before (June 5th, YYYY), pertaining to the above-referenced individual who has requested the Division of Professional Licensing to conduct a prelitigation panel review of a claim of medical malpractice.

DATED this fifth day of May YYYY.

DEPARTMENT OF HEALTH

By: Petra Lyons

Petra Lyons, Regulatory & Compliance Officer
Division of Professional Licensing

Figure 9-2  Subpoena ad Testificandum (Courtesy Delmar/Cengage Learning.)
ADAM ATTORNEY
15 MAIN STREET
ALBANY NY 00000
PHONE: (518) 555-1234

BEFORE THE DEPARTMENT OF HEALTH, STATE OF NEW YORK

JOHN DOE, )                     SUBPOENA DUCES TECUM
   Petitioner, )
   )
   vs. )
   )
   RICHARD ROE, M.D. )
   Respondent. )
   )
   )
   Case No. NY-123456789

TO: Richard Roe, M.D.
   000 Medical Plaza
   Anytown, U.S.A. 84100

   RE: John Doe
   Date of Birth: 8/28/55

YOU ARE COMMANDED to produce at the County Courthouse, 15 Main Street, Room 14A, Albany NY 00000 on June 5th, YYYY at 9 A.M., a complete copy of your medical records, pertaining to the above-referenced individual who has requested the Division of Professional Licensing to conduct a prelitigation panel review of a claim of medical malpractice. Attendance is not required if records are timely forwarded to the indicated address.

DATED this fifth day of May YYYY.

DEPARTMENT OF HEALTH
By: Petra Lyons
Petra Lyons, Regulatory & Compliance Officer
Division of Professional Licensing

Figure 9-3  Subpoena Duces Tecum (Courtesy Delmar/Cengage Learning.)
EXAMPLE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law passed by Congress that amended “the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.”

Exercise 9–1 Legal and Regulatory Terms

True/False: Indicate whether each statement is True (T) or False (F).

1. Public law includes both federal regulations and criminal law.
2. The health care industry is most often involved in criminal cases.
3. Statutory law is based on precedent and judicial decisions.
4. Stare decisis is Latin for “let the master answer.”
5. The defendant is the individual who initiates a civil complaint.

MAINTAINING THE PATIENT RECORD IN THE NORMAL COURSE OF BUSINESS

The medical record is a legal business record that must be maintained according to accreditation standards (e.g., The Joint Commission), legal principles (e.g., federal and state laws), professional practice standards (e.g., AHIMA practice briefs that provide guidelines for recordkeeping issues), and regulations (e.g., Medical Conditions of Participation). While laws, regulations, and standards originally applied to the maintenance of paper records, they also apply to electronic (or computer-based) records that are usually legally acceptable as long as they are properly created and maintained in the normal course of business.

NOTE: Standards will vary depending on applicable case law, state laws, and type of health care setting.

Currently, no state has enacted a comprehensive law that systematically deals with all issues raised by the computerization of records, although some states have enacted legislation that expressly recognizes the validity of the electronic medical record (EMR). Other states have indirectly recognized the validity of EMRs by passing laws that standardize electronic authentication, recognize the right of providers to create and maintain medical records in electronic form, and require that computer systems have certain characteristics such as the capacity to prevent subsequent alterations or to protect the security of records. HIPAA legislation also does not attempt to formulate standards for electronic records, although it directs regulatory authorities to devise appropriate rules for the transmission of data.

Although medical record documentation is technically considered hearsay, the Federal Rules of Evidence 803(6) and the Uniform Business Records as Evidence Act have been adopted by most states to allow records maintained in the regular course of business as an exception to the hearsay rule. For a medical record to be considered admissible as evidence, the records must be:

- Created by a person within the business who has knowledge of the acts, conditions, diagnoses, events, or opinions documented
- Documented in the normal course of business
- Generated at or near the time of patient care
- Maintained in the regular course of business

EMRs are also admissible if they meet the four principles above and meet the following Comprehensive Guide to Electronic Health Records guidelines that demonstrate accuracy and trustworthiness:

- Type of computer used is accepted as standard and efficient equipment
- Method of operation to create electronic medical record is recorded
- Method and circumstances of preparing the record include sources of information on which the record is based, procedures for entering information into and retrieving information from the computer, controls and checks used, and tests performed to ensure the accuracy and reliability of the record
- Information documented in the EMR has not been altered in any way

Other safeguards that can help ensure the admissibility of the EMR include:

- Maintaining records at an off-site backup storage system in case the on-site system is damaged or destroyed
• Using an imaging system to copy documents that contain signatures
• Ensuring that records, once in electronic form, cannot be altered
• Safeguarding the confidentiality of records and preventing access by unauthorized persons
• Allowing authentication of record entries via electronic signature keys
• Implementing procedures for systems maintenance

Exercise 9–2 Maintaining the Patient Record in the Normal Course of Business

Fill-In-The-Blank: Enter the term that most appropriately completes the statement.

1. From a legal standpoint, medical record documentation is officially considered ________. However, most states have adopted the Federal Rules of Evidence 803(6) and the ________ as Evidence Act as an exception.

2. Laws, regulations, and standards originally applied to maintenance of records, but now also apply to ________ records.

3. HIPAA legislation directs regulatory authorities to devise appropriate rules for the ________ of data.

4. Standards that govern medical records will vary depending on application case law, type of health care setting, and ________.

5. A safeguard that can help ensure the admissibility of the EMR in court is ________.

CONFIDENTIALITY OF INFORMATION AND HIPAA PRIVACY AND SECURITY PROVISIONS

Any information communicated by a patient to a health care provider is considered privileged communication, which means it is private. Patients have the right to confidentiality, which is the process of keeping privileged communication secret and means that information cannot be disclosed without the patient’s authorization. (Exceptions include information released via subpoena duces tecum and according to statutory reporting requirements, discussed later in this chapter.) A breach of confidentiality occurs when patient information is disclosed (or released) to other(s) who do not have a right to access the information. In this situation, the disclosing provider failed to obtain patient authorization to release privileged communication; this results in violation of federal law (HIPAA). According to HIPAA privacy and security provisions:

• Patients have the right to an expectation of privacy regarding their privileged communication, which means information cannot be disclosed without their authorization.
• Security safeguards must be implemented to ensure that facilities, equipment, and patient information are safe from damage, loss, tampering, theft, or unauthorized access.

NOTE: If security policies and procedures are not established and enforced, concerns might be raised about the security of patient information during legal proceedings. This could result in questioning the integrity of the medical record.

Health Insurance Portability and Accountability Act of 1996

EXAMPLE 1

A patient entered the health information department and requested a copy of the results of a brain scan that she had undergone in the emergency department the night before. The patient signed the release of information authorization form, and when the record was retrieved the health information technician (HIT) noticed that the results revealed a serious abnormality. Instead of releasing a copy of the report to the patient, the HIT explained to the patient that she should discuss the results of the brain scan with her primary care physician. The patient became very nervous and scared and could not be convinced to discuss the results with her primary care physician. The HIT then decided to escort the patient to the emergency department and explain the situation to the emergency physician, who agreed to review the results with the patient. That physician also contacted the patient’s primary care physician to let him know about the situation.

EXAMPLE 2

A health information department clerk responded to a request to hand carry patient records to a nursing floor. One of the patients was an employee of the health information department, and during transport the clerk read the record and asked the employee why she was on a particular medication. The employee reported the incident to the health information manager, who contacted Human Resources. The incident was investigated, and the clerk was terminated.

As stated previously, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
amended the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical savings accounts; to improve access to long-term care services and coverage; to simplify the administration of health insurance; and for other purposes (e.g., privacy of health information). HIPAA is the first federal law that governs the privacy of health information nationwide.

HIPAA legislation was organized according to five titles:

- **Title I**—Health Care Access, Portability, and Renewability
- **Title II**—Preventing Health Care Fraud and Abuse, Administrative Simplification, and Medical Liability Reform
- **Title III**—Tax-Related Health Provisions
- **Title IV**—Application and Enforcement of Group Health Plan Requirements
- **Title V**—Revenue Offsets

**NOTE:** Only HIPAA Title II content is discussed in this chapter because the remaining content covers health care reimbursement issues, which is discussed in Chapter 10. Title II legal aspects include medical liability, privacy, and security, discussed below.

### HIPAA Made Simple

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) resulted from Clinton administration and congressional efforts to reform health care by enabling workers of all professions to change jobs even if they (or family members) have pre-existing medical conditions, by reducing health care fraud and abuse, by reducing paperwork associated with health claims processing, and by guaranteeing the security and privacy of health information. The “portability” aspect of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. The “accountability” aspect protects health data integrity, availability, and confidentiality and has the greatest impact on health care organizations.

### Medical Liability

The threat of excessive awards in medical liability cases has increased providers’ liability insurance premiums and resulted in increases in health care costs. As a result, some providers stop practicing medicine in areas of the country where liability insurance costs are highest, and the direct impact on individuals and communities across the country is reduced access to quality medical care. Although medical liability reform was included in HIPAA legislation, no final rule was published. While individual states, such as Ohio, have passed medical liability reform, the United States Congress is also formulating separate federal medical liability reform legislation. In 2003, the House of Representatives (HR) passed HR 5 for medical liability reform. In addition, the Senate (S) introduced S 607, the HEALTH Act, which is a medical liability reform bill that includes a hard cap of $250,000 on noneconomic damages.

**NOTE:** Related to HR 5 and S 607 is passage by the House of Representatives on March 12, 2003, of HR 663, the Patient Safety and Quality Improvement Act, which allows providers to report health care errors on a voluntary and confidential basis. Patient Safety Organizations (PSOs) would be established to analyze the problems, identify solutions, and provide feedback to avoid future errors. A database would also be created to track national trends and reoccurring problems. The bill advanced to the Senate (as bill number S 720) where it was passed out of the Senate Committee on Health, Education, Labor, and Pensions on July 23, 2003.

### Privacy Rule

The **HIPAA standards for privacy of individually identifiable health information** (or privacy rule) include provisions that protect the security and confidentiality of health information. Because the use and disclosure of health information is inconsistently protected by state laws, patients’ privacy and confidentiality is also inconsistently protected. The HIPAA privacy rule establishes standards to protect the confidentiality of individually identifiable health information maintained or transmitted electronically in connection with certain administrative and financial transactions (e.g., electronic transfer of health insurance claims). The rule provides new rights for individuals with respect to protected health information (PHI) about them and mandates compliance by covered entities, which are private and public sector organizations that must follow HIPAA provisions. For the privacy rule, covered entities include health care providers that conduct
certain transactions in electronic form, health plans, and health care clearinghouses.

**NOTE:** The compliance date was April 14, 2003, for large health plans and April 14, 2004, for small health plans.

**Protected health information (PHI)** is information that is identifiable to an individual (or individual identifiers) such as name, address, telephone numbers, date of birth, Medicaid ID number and other medical record numbers, social security number (SSN), and name of employer. In most instances, covered entities are required to obtain an individual’s authorization prior to disclosing their health information, and HIPAA has established specific requirements for an authorization form.

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, paper-based, or verbally, are covered by the privacy rule. The provisions of the privacy rule are extensive, and they are summarized below.

Patients have the following specific rights:

- **Patient education on privacy protections.** Covered entities are required to provide patients with a clear written explanation (Figure 9-4) of how the covered entity may use and disclose their health information. (However, an inmate has no right to such a notice, and a correctional facility has no obligation to provide such a notice. Special rules and exceptions also apply to group health plans.) Patients must also be provided with an opportunity to object to disclosure of PHI.

  **NOTE:** An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that (1) the covered entity has taken action in reliance thereon (e.g., facility has already released PHI based on previously executed authorization; or (2) if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

- **Redisclosure of PHI.** The patient authorization to release PHI should include a general statement that the health information may no longer be protected by the privacy rule once it is disclosed by the covered entity. (Covered entities should inform recipients of PHI of their obligation to not redisclose PHI unless authorized to do so.)

- **Patient access to their records.** Patients will be allowed to obtain copies of their records and to request that amendments be made to documentation. In addition, non-routine disclosure must be communicated to patients.

  **NOTE:** HIPAA mandates a time limit of 60 days for covered entities to respond to requests for amendments and release of information requests.

- **Disclosures to business associates.** A covered entity may disclose PHI to a business associate (e.g., third-party payer) and may allow a business associate to create or receive PHI on its behalf if the entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

- **Patient care and notification.** A covered entity may disclose PHI to a family member (or other personal representative) PHI directly related to that person’s involvement with the patient’s care or payment related to care. A covered entity may also disclose PHI to notify a family member (or other personal representative) of a patient’s location, general condition, or death.

- **Disclosures about deceased patients.** A covered entity must protect the PHI of a deceased patient for two years following the patient’s death. (Disclosures for research purposes are exempt from this standard.)

- **Limited uses and disclosures when the patient is not available.** The covered entity may exercise professional judgment to determine whether disclosure of PHI is in the best interest of the patient and disclose only that PHI directly related to the person’s involvement with the patient’s health care. For example, a person could act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, and so on.

- **Disclosures by whistleblowers and workforce member crime victims.** A covered entity is not considered to have violated this standard if a member of its workforce or a business associate discloses PHI as the result of good faith judgment that the covered entity (1) has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or (2) that the care, services, or conditions provided by the covered entity potentially endanger one or more patients, workers, or the public; and (3) the disclosure is to a health oversight agency, attorney, or law enforcement official involving a victim of a crime.

- **Obtaining patient authorization before information is disclosed.** Except for circumstances requiring patient authorization (e.g., psychotherapy notes), providers are not required to obtain patient
<table>
<thead>
<tr>
<th>Global Insurance Plan</th>
<th>PRIVACY NOTICE</th>
<th>Effective April 14, 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THIS NOTICE DESCRIBES HOW PERSONAL AND MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Understanding the Type of Information We Have.</strong> We get information about you when you enroll in a health plan. It includes your date of birth, sex, ID number and other personal information. We also get bills, reports from your doctor and other data about your medical care.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Our Privacy Commitment To You.</strong> We care about your privacy. The information we collect about you is private. We are required to give you a notice of our privacy practices. Only people who have both the need and the legal right may see your information. Unless you give us permission in writing, we will only disclose your information for purposes of treatment, payment, business operations (TPO) or when we are required by law to do so.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Treatment.</strong> We may disclose medical information about you to coordinate your health care. For example, we may notify your doctor about care you get in an emergency room.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Payment.</strong> We may use and disclose information so the care you get can be properly billed and paid for. For example, we may ask an emergency room for details before we pay the bill for your care.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Business Operations.</strong> We may need to use and disclose information for our business operations. For example, we may use information to review the quality of care you get.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Exceptions.</strong> For certain kinds of records, your permission may be needed even for release for treatment, payment and business operations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>As Required By Law.</strong> We will release information when we are required by law to do so. Examples of such releases would be for law enforcement or national security purposes, subpoenas or other court orders, communicable disease reporting, disaster relief, review of our activities by government agencies, to avert a serious threat to health or safety or in other kinds of emergencies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>With Your Permission.</strong> If you give us permission in writing, we may use and disclose your personal information. If you give us permission, you have the right to change your mind and revoke it. This must be in writing, too. We cannot take back any uses or disclosures already made with your permission.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Your Privacy Rights.</strong> You have the following rights regarding the health information that we have about you. Your requests must be made in writing to the Department of Health at the address below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Your Right to Inspect and Copy.</strong> In most cases, you have the right to look at or get copies of your records. You may be charged a fee for the cost of copying your records.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Your Right to Amend.</strong> You may ask us to change your records if you feel that there is a mistake. We can deny your request for certain reasons, but we must give you a written reason for our denial.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Your Right to a List of Disclosures.</strong> You have the right to ask for a list of disclosures made after April 14, 2003. This list will not include the times that information was disclosed for treatment, payment, or health care operations. The list will not include information provided directly to you or your family, or information that was sent with your authorization.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Your Right to Request Restrictions on Our Use or Disclosure of Information.</strong> You have the right to ask for limits on how your information is used or disclosed. We are not required to agree to such requests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Your Right to Request Confidential Communications.</strong> You have the right to ask that we share information with you in a certain way or in a certain place. For example, you may ask us to send information to your work address instead of your home address. You do not have to explain the basis for your request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Changes to this Notice.</strong> We reserve the right to revise this notice. A revised notice will be effective for medical information we already have about you as well as any information we may receive in the future. We are required by law to comply with whatever notice is currently in effect. Any changes to our notice will be published on our Web site. Go to <a href="http://www.medicaid.gov">www.medicaid.gov</a>, click on Health Care Coverage, and look under Spotlight. If the changes are material, a new notice will be mailed to you before it takes effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>How to Use Your Rights Under This Notice.</strong> If you want to use your rights under this notice, you may call us or write to us. If your request to us must be in writing, we will help you prepare your written request, if you wish.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Complaints to the Federal Government.</strong> If you believe that your privacy rights have been violated, you have the right to file a complaint with the federal government. You may write to: Office of Civil Rights, Dept. of Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C. 20201, Phone: 866-627-7748, TTY: 866-788-4989, Email: <a href="mailto:ocrprivacy@hhs.gov">ocrprivacy@hhs.gov</a>. You will not be penalized for filing a complaint with the federal government.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Complaints and Communications to Us.</strong> If you want to exercise your rights under this notice or if you wish to communicate with us about privacy issues or if you wish to file a complaint, you can write to: Privacy Officer, Global Insurance Plan, 100 Main Street, Anywhere US 12345, (101) 555-1234, TDD: (101) 555-1111. You will not be penalized for filing a complaint.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Copies of this Notice.</strong> You have the right to receive an additional copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. Please call or write to us to request a copy. This notice is available in other languages and alternate formats that meet the guidelines for the Americans with Disabilities Act (ADA). Esta notificació n est disponibile en otras lenguas y formatos diferentes que satisfacen las normas del Acta de Americans con Discapacidades (ADA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For Further Information.</strong> Global Health Insurance Beneficiary Helpline, 1-800-555-1234, TTY: Relay Center - 555.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Global Health Insurance is an Equal Opportunity Employer, Services and Program Provider.
authorization prior to disclosing information for treatment, payment, and health care operations (TPO). A covered entity must comply with the minimum necessary privacy standard by making reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish a task. **Treatment, payment, and health care operations** (TPO) activities are defined as follows:

- **Treatment** generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
- **Payment** encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.
- **Health care operations** are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

**NOTE:** Many providers opt to obtain authorization to disclose PHI for TPO purposes (Figure 9-5). Separate patient authorization must be obtained for non-routine disclosures and non-health care purposes (Figure 9-6), and patients have the right to request restrictions as to use and disclosure of their protected health information (PHI). Do not confuse patient consent to TPO with patient authorization to disclose PHI. According to HIPAA, patients “consent to use and disclose information,” which means they provide written permission to providers so that health information related to treatment, payment, or health care operations (TPO) can be used or disclosed.

**EXAMPLE 1**

**Disclosure of PHI for TPO purposes**

Patients routinely sign the consent form on the reverse of an inpatient face sheet, which allows the facility to communicate final diagnoses and procedures to third-party payers so that the facility can be reimbursed for care provided to the patient. In addition, patients routinely consent to medical treatment when they are admitted as a hospital inpatient. This consent form is usually located on the reverse of the face sheet. (HIPAA no longer requires covered entities to obtain consent to treatment, payment, and operations (TPO); however, most covered entities continue to obtain consent from patients.)

**EXAMPLE 2**

**Disclosure of PHI for other than TPO purposes**

Patients “authorize the use or disclosure of information” when they provide written permission to providers so that PHI can be released for purposes other than TPO. For example, when third-party payers request a copy of the patient’s entire medical record to determine whether to reimburse the facility for services provided, the patient must sign a special authorization to release PHI.

**Recourse if privacy protections are violated.** Patients have the right to file a formal complaint with a covered entity, or with HHS, when violations of privacy protections occur. For example, releasing information to an employer, without the patient’s authorization, so that personnel decisions can be made is a violation.

Covered entities have the flexibility to establish their own policies and procedures to meet privacy rule standards, and they should:

- **Create written privacy policies and procedures,** which clarify who has the right to access protected information, how protected information will be used within the covered entity, and when protected information may be disclosed. Covered entities must ensure that their business associates also protect the privacy of health information (e.g., add HIPAA clause to business agreements).
- **Train employees** regarding HIPAA privacy policies and procedures.
- **Designate a privacy officer** who is responsible for ensuring that procedures are followed (e.g., health information manager).

Covered entities are required to take reasonable steps to limit the use or disclosure of, and requests for, protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do not apply to the following:

- Disclosures to or requests by a provider for treatment purposes
- Disclosures to the individual who is subject of the information
I hereby give my consent for Alfred State Medical Center to use and disclose protected health information (PHI) about me to carry out treatment, payment, and health care operations (TPO). (The Privacy Notice provided by Alfred State Medical Center describes such uses and disclosures more completely.)

I have the right to review the Privacy Notice prior to signing this consent. Alfred State Medical Center reserves the right to revise its Privacy Notice at any time. A revised Privacy Notice may be obtained by forwarding a written request to Privacy Officer, Alfred State Medical Center, 100 Main Street, Anywhere NY 00000.

With this consent, Alfred State Medical Center may call my home or other alternative location and leave a message on voice mail or in person in reference to any items that assist the practice in carrying out TPO, such as appointment reminders, insurance items, and any calls pertaining to my clinical care, including laboratory test results, among others.

With this consent, Alfred State Medical Center may mail to my home or other alternative location any items that assist the practice in carrying out TPO, such as appointment reminder cards and patient statements as long as they are marked Personal and Confidential.

With this consent, Alfred State Medical Center may email to my home or other alternative location any items that assist the practice in carrying out TPO, such as appointment reminder cards and patient statements. I have the right to request that Alfred State Medical Center restrict how it uses or discloses my PHI to carry out TPO. The practice is not required to agree to my requested restrictions, but if it does, it is bound by this agreement.

By signing this form, I am consenting to allow Alfred State Medical Center to use and disclose my PHI to carry out TPO.

I may revoke my consent in writing except to the extent that the practice has already made disclosures in reliance upon my prior consent. If I do not sign this consent, or later revoke it, Alfred State Medical Center may decline to provide treatment to me.

Signature of Patient or Legal Guardian

Print Patient's Name

Date

Print Name of Patient or Legal Guardian, if applicable

Be signed by the individual and dated.

Figure 9-5  TPO Consent Form with HIPAA Content Requirements (Courtesy Delmar/Cengage Learning.)
## Authorization Form for Disclosure of Protected Health Information (PHI)

1. **I hereby authorize Alfred State Medical Center to disclose/obtain information from the health records of:**
   - **Patient Name**
   - **Date of Birth (mm/dd/yyyy)**
   - **Telephone (w/ area code)**
   - **Patient Address**
   - **Medical Record Number**

2. **Covering the period(s) of healthcare:**
   - From (mm/dd/yyyy) to (mm/dd/yyyy)
   - From (mm/dd/yyyy) to (mm/dd/yyyy)

3. **I authorize the following information to be released by Alfred State Medical Center (check applicable reports):**
   - [ ] Face Sheet
   - [ ] Progress Notes
   - [ ] Pathology Report
   - [ ] Drug Abuse Care
   - [ ] Discharge Summary
   - [ ] Lab Results
   - [ ] Pathology Report
   - [ ] Other:
   - [ ] History & Physical Exam
   - [ ] X-ray Reports
   - [ ] HIV Testing Results
   - [ ] Consultation
   - [ ] Scan Results
   - [ ] Mental Health Care
   - [ ] Doctors Orders
   - [ ] Operative Report
   - [ ] Alcohol Abuse Care
   - [ ] Other:

   - [ ] History & Physical Exam
   - [ ] X-ray Reports
   - [ ] HIV Testing Results
   - [ ] Consultation
   - [ ] Scan Results
   - [ ] Mental Health Care
   - [ ] Doctors Orders
   - [ ] Operative Report
   - [ ] Alcohol Abuse Care

   This information is to be disclosed to or obtained from:
   - **Name of Organization**
   - **Address of Organization**
   - **Telephone Number**

   for the purpose of:

4. **I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization I must do so in writing and present my written revocation to the Health Information Management Department. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. Unless otherwise revoked, this authorization will expire on the following date, event, or condition:**
   - **Expiration Date**
   - **Expiration Event**
   - **Expiration Condition**

   If I fail to specify an expiration date, event, or condition, this authorization will expire within six (6) months.

5. **I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this form in order to assure treatment. I understand that I may inspect or copy the information to be used or disclosed, provided in CFR 164.534. I understand that any disclosure of information carries with it the potential for an unauthorized re-disclosure and may not be protected by federal confidentiality rules. If I have questions about disclosure of my health information, I can contact the Privacy Officer at Alfred State Medical Center.**

   **Signed:**
   - **Signature of Patient or Legal Representative**
   - **Date**
   - **Relationship to Patient**
   - **Signature of Witness**
   
   **Expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.**

   **Statement that information used or disclosed may be subject to re-disclosure by recipient and may no longer be protected by this rule.**

   **Signature of individual and date.**

   **If signed by personal representative, a description of the representative’s authority to act for the individual.**

---

*Figure 9-6  Authorization Form for Disclosure of Protected Health Information (Courtesy Delmar/Cengage Learning.*)*
The following penalties apply when covered entities misuse personal health information:

- **Civil monetary penalties** of $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated
- **Federal criminal penalties** of up to $50,000 and one year in prison for obtaining or disclosing protected health information, up to $100,000 and up to five years in prison for obtaining protected health information under “false pretenses,” and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm. It should be noted that penalties will be expanded in 2010 due to provisions in the HITECH Act.

**NOTE:** Special protection exists for psychotherapy notes that are used only by a psychotherapist, do not become part of the patient’s medical record, and are never intended to be shared with anyone else. In addition, when stronger state laws (e.g., disclosure of AIDS, HIV, and mental health records) exist, they preempt HIPAA privacy provisions. What this means is that, while the HIPAA privacy rule establishes a baseline for standards that protect the confidentiality and privacy of patient information, in some states patients will have additional protection. Many state health departments have developed documents that compare state law with HIPAA federal regulations. It should be noted that HIPAA also addresses disclosures for judicial and administrative proceedings.

**Security Rule**

The HIPAA **security rule** was published February 20, 2003, and it adopts standards and safeguards to protect health information that is collected, maintained, used, or transmitted electronically. Covered entities impacted by this rule include health plans, health care clearinghouses, and certain health care providers. CMS is responsible for overseeing compliance with and complaints about security rules; and covered entities, except small health plans, must comply with requirements by April 21, 2005. Small health plans must comply by April 21, 2006.

**NOTE:** The proposed standard for electronic signature is **digital**, which applies a mathematical function to the electronic document resulting in a **unique bit string** (computer code) called a message digest that is encrypted and appended to the electronic document. (Encrypt means to encode a computer file, making it safe for electronic transmission so that unauthorized parties cannot read it.) The recipient of the transmitted electronic document **decrypts** (decodes) the message digest and compares the decoded digest with the transmitted version. If they are identical, the message is unaltered and the identity of the signer is proven.

The DHHS Medicare Program, other federal agencies operating health plans or providing health care, state Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (e.g., patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of the **security rule** is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information, also known as EPHI. Prior to publication of the security rule, no standard measures existed in the health care industry to address all aspects of the security of electronic health information while it is being stored or during the exchange of that information between entities. In general, security provisions should include the following policies and procedures:

- Define authorized users of patient information to control access
- Implement a tracking procedure to sign out records to authorized personnel
- Limit record storage access to authorized users
- Lock record storage areas at all times
- Require that the original medical record remain in the facility at all times

**NOTE:** It is usually acceptable to submit a copy of the medical record for legal proceedings. If the original record is required, obtain a receipt from the court clerk and retain a copy of the record in the storage area. Be sure to properly protect the original record when transporting it to court by placing the record in a locked storage container. Make sure that the original record remains in the custody of health
EXCERPT FROM HIPAA LAW- 45 CFR §164.512(E)

(e) Standard: Disclosures for judicial and administrative proceedings

(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual’s location is unknown, to mail a notice to the individual’s last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(1) No objections were filed; or

(2) All objections filed by the individual have been resolved by the court or the administrative tribunal, and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to the lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.
care personnel transporting the record until entered into evidence.

HIPAA's security rule standards include the following safeguards:

- Administrative (Table 9-1A)
- Physical (Table 9-1B)
- Technical (Table 9-1C)

**NOTE:** While security and privacy are linked, be sure you do not confuse the purpose of each rule. The security rule defines administrative, physical, and technical safeguards to protect the availability, confidentiality, and integrity of electronic protected health information (PHI). The standards require covered entities to implement basic safeguards to protect electronic PHI from unauthorized access, alteration, deletion, and transmission. In contrast, the privacy rule establishes standards for how PHI should be controlled; it also establishes what uses (e.g., continuity of care) and disclosures (e.g., third-party reimbursement) are authorized or required as well as what rights patients have with respect to their health information (e.g., patient access).

**Exercise 9–3  Confidentiality of Information and HIPAA Privacy and Security Provisions**

True/False: Indicate whether each statement is True (T) or False (F).

1. The “accountability” aspect of HIPAA protects health information coverage for workers and their families when they change or lose their jobs.
2. The HIPAA privacy rule established standards to protect the confidentiality of individually identifiable health information.
3. The HIPAA privacy rule preempts stricter state laws, such as disclosure of mental health records.
4. Electronic transmission of protected health information is impacted by the HIPAA security rule.
5. National standards to protect the confidentiality and availability of electronic protected health information were established by the HIPAA security rule.

**LEGISLATION THAT IMPACTS HEALTH INFORMATION MANAGEMENT**

In the United States, protection of health information is generally divided between coverage for record-keeping systems maintained by federal (Table 9-2) and state (Table 9-3) government agencies and those maintained by the private sector. Federal protection measures are found in constitutional law, the Privacy Act of 1974, and statutes that regulate narrow areas of data use. State laws generally define the types of health information considered confidential and the circumstances under which the information can be shared without patient authorization. Information maintained by the private sector is regulated by laws that address specific types of organizations.

**NOTE:** The HITECH Act extends certain HIPAA privacy and security requirements and increases enforcement. For the most current information on the impact of the HITECH Act visit www.ahima.org and search on HITECH Act.

**Exercise 9–4  Legislation that Impacts Health Information Management**

Short Answer: Identify the federal law or regulation described below.

1. Requires that drug and alcohol abuse patient records be kept confidential and are not subject to disclosure except as provided by law.
2. Federal law that established the National Practitioners Data Base.
3. Established the Nursing Home Reform Act to ensure that residents of nursing facilities receive quality care and established a Residents’ Bill of Rights.
4. Created a data bank to combat fraud and abuse in the health care industry, alerting users to conduct a comprehensive review of health care providers’ past actions.
5. Federal legislation that mandated administrative simplification regulations to govern privacy, security, and electronic transaction standards for health care information.

**RELEASE OF PROTECTED HEALTH INFORMATION**

Individuals who work in health care settings have the responsibility for maintaining confidentiality of protected health information (PHI) and appropriately disclosing (releasing) that information if requested to do so. The medical record generated and maintained in the process of patient treatment contains PHI, and it is important to not only appropriately release a patient’s PHI but to not include information about care related...
### Table 9-1A HIPAA Security Rule—Administrative Safeguards and Implementation Specifications

<table>
<thead>
<tr>
<th>Administrative Safeguards</th>
<th>Implementation Specifications for Covered Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security management process</td>
<td>Policies and procedures to prevent, detect, contain, and correct security violations include:</td>
</tr>
<tr>
<td></td>
<td>• Risk analysis (assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI)</td>
</tr>
<tr>
<td></td>
<td>• Risk management (implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level)</td>
</tr>
<tr>
<td></td>
<td>• Sanction policy (apply appropriate penalties against workforce members who fail to comply with the security policies and procedures of the covered entity)</td>
</tr>
<tr>
<td></td>
<td>• Information system activity review (implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports)</td>
</tr>
<tr>
<td>Assigned security responsibility</td>
<td>Identify the security official responsible for development and implementation of security policies and procedures.</td>
</tr>
<tr>
<td>Workforce security</td>
<td>Ensure that all workforce members have appropriate access to electronic PHI, and prevent those workforce members who do not have access from obtaining access to electronic PHI:</td>
</tr>
<tr>
<td></td>
<td>• Authorization and/or supervision of workforce members who work with electronic PHI or in locations where PHI might be accessed</td>
</tr>
<tr>
<td></td>
<td>• Workforce clearance to determine that the access of a workforce member to electronic PHI is appropriate</td>
</tr>
<tr>
<td></td>
<td>• Terminating access to electronic PHI when the employment of a workforce member ends</td>
</tr>
<tr>
<td>Information access management</td>
<td>Authorizing access to electronic PHI:</td>
</tr>
<tr>
<td></td>
<td>• Isolating health care clearinghouse functions if a health care clearinghouse is part of a larger organization; the clearinghouse must implement policies and procedures that protect electronic PHI of the clearinghouse from unauthorized access by the larger organization</td>
</tr>
<tr>
<td></td>
<td>• Authorizing access to electronic PHI (e.g., workstation)</td>
</tr>
<tr>
<td></td>
<td>• Establishing and modifying access to a workstation, transaction, program, or process</td>
</tr>
<tr>
<td>Security awareness and training</td>
<td>Security awareness and training program for all workforce members:</td>
</tr>
<tr>
<td></td>
<td>• Security reminders via periodic security updates and protection from malicious software to guard against, detect, and report malicious software</td>
</tr>
<tr>
<td></td>
<td>• Log-in monitoring to investigate log-in attempts and report discrepancies</td>
</tr>
<tr>
<td></td>
<td>• Password management to create, change, and safeguard passwords</td>
</tr>
<tr>
<td>Security incident procedures</td>
<td>Address security incidents through response and reporting:</td>
</tr>
<tr>
<td></td>
<td>• Identify and respond to suspected or known security incidents</td>
</tr>
<tr>
<td></td>
<td>• Mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity</td>
</tr>
<tr>
<td></td>
<td>• Document security incidents and their outcomes</td>
</tr>
<tr>
<td>Contingency plan</td>
<td>Respond to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems containing electronic PHI:</td>
</tr>
<tr>
<td></td>
<td>• Data backup plan to create and maintain retrievable exact copies of electronic PHI</td>
</tr>
<tr>
<td></td>
<td>• Disaster recovery plan to restore any loss of data</td>
</tr>
<tr>
<td></td>
<td>• Emergency mode operation plan to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode</td>
</tr>
<tr>
<td></td>
<td>• Testing and revision procedures for periodic testing and revision of contingency plans</td>
</tr>
<tr>
<td></td>
<td>• Applications and data criticality analysis to assess the relative criticality of specific applications and data in support of other contingency plan components</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Perform periodic technical and nontechnical evaluations, based initially upon the standards implemented under this rule, and, subsequently in response to environmental or operational changes affecting the security of electronic PHI, which establishes the extent to which an entity’s security policies and procedures meet security requirements.</td>
</tr>
<tr>
<td>Associate contracts and other arrangements</td>
<td>Permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.</td>
</tr>
</tbody>
</table>
to another patient, peer review or quality management documents, correspondence or notes from attorneys, and aberrant or deviant statements.

- Filing documents in a patient’s record related to care provided to another patient occurs when material is misfiled in the wrong record. If these records are released in error, the provider is subject to possible civil lawsuit for breach of confidentiality.
- Including peer review, quality management documents, and correspondence or notes from attorneys in the patient record creates a dangerous situation—health care facilities generate these documents as internal documents for administrative purposes. Mistakenly including them in a patient’s record subjects them to disclosure upon a third party’s (e.g., plaintiff’s attorney) request for information.
- Aberrant or deviant statements about the patient do not belong in the record. (Author Michelle Green recalls a situation as director of medical records when a copy of a patient’s record was appropriately released to the patient. Upon review of the record, it was discovered that a nurse documented “. . . what a son of a bitch . . .” the patient was to care for. The hospital administrator instructed Green to have the nurse remove the comment and rewrite that page of notes; Green refused to carry out this instruction, stating it would be considered tampering with the record, which is illegal.)

**NOTE:** Disclosure of PHI is related to the ownership and physical control of the medical record (including X-ray films, scans, and so on).

**Remember!** While the health care provider owns the medical record, the patient owns the information contained in the medical record. This means that third parties that have a legitimate interest in medical record content have the legal right to request access to PHI. The provider is responsible for ensuring that PHI is released in accordance with federal (e.g., HIPAA Privacy Rule) and state laws.

---

**Table 9-1B HIPAA Security Rule—Physical Safeguards and Implementation Specifications**

<table>
<thead>
<tr>
<th>Physical Safeguards</th>
<th>Implementation Specifications for Covered Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility access controls</td>
<td>Limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed:</td>
</tr>
<tr>
<td></td>
<td>- Contingency operations to allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency</td>
</tr>
<tr>
<td></td>
<td>- Facility security plan to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft</td>
</tr>
<tr>
<td></td>
<td>- Access control and validation procedures to control and validate a person’s access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision</td>
</tr>
<tr>
<td></td>
<td>- Maintenance records to document repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks)</td>
</tr>
<tr>
<td>Workstation use</td>
<td>Specify proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.</td>
</tr>
<tr>
<td>Workstation security</td>
<td>Physical safeguards for all workstations that access electronic PHI to restrict access to authorized users.</td>
</tr>
<tr>
<td>Device and media controls</td>
<td>Govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility:</td>
</tr>
<tr>
<td></td>
<td>- Disposal of electronic PHI and/or the hardware or electronic media on which it is stored</td>
</tr>
<tr>
<td></td>
<td>- Media re-use to remove electronic PHI from electronic media before the media are made available for re-use</td>
</tr>
<tr>
<td></td>
<td>- Accountability to maintain a record of the movements of hardware and electronic media and any person responsible therefore</td>
</tr>
<tr>
<td></td>
<td>- Data backup and storage to create a retrievable, exact copy of electronic PHI, when needed, before relocating equipment</td>
</tr>
</tbody>
</table>
The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and state confidentiality laws control the disclosure of information from patient records, and the following must be considered:

- When an authorization to disclose PHI is required and when it is not required
- Special circumstances that impact disclosure of PHI (e.g., correctional facilities, HIV, military records)
- Patient access to records
- Accounting of disclosures of PHI

In most circumstances, the patient (or legal representative) controls the disclosure of PHI to third parties (e.g., insurance company) because an authorization for release of PHI must be obtained prior to disclosure. HIPAA and state laws establish standards for content of the authorization form, with state laws superseding HIPAA only if they contain stricter provisions.

### Table 9-1C HIPAA Security Rule—Technical Safeguards and Implementation Specifications

<table>
<thead>
<tr>
<th>Technical Safeguards</th>
<th>Implementation Specifications for Covered Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights:</td>
</tr>
<tr>
<td></td>
<td>• Unique user identification to assign a unique name and/or number for identifying and tracking user identity</td>
</tr>
<tr>
<td></td>
<td>• Emergency access procedure to obtain necessary electronic PHI during an emergency</td>
</tr>
<tr>
<td></td>
<td>• Automatic logoff electronic procedures that terminate an electronic session after a predetermined time of inactivity</td>
</tr>
<tr>
<td></td>
<td>• Encryption and decryption mechanism to encrypt and decrypt electronic PHI</td>
</tr>
<tr>
<td>Audit controls</td>
<td>Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Protect electronic PHI from improper alteration or destruction:</td>
</tr>
<tr>
<td>Person or entity authentication</td>
<td>• Mechanism to authenticate electronic PHI to corroborate that information has not been altered or destroyed in an unauthorized manner</td>
</tr>
<tr>
<td>Transmission security</td>
<td>Verify that a person or entity seeking access to electronic PHI is the one claimed.</td>
</tr>
<tr>
<td>Business associate contracts or other arrangements</td>
<td>Technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network:</td>
</tr>
<tr>
<td>Requirements for group health plans</td>
<td>• Integrity controls to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.</td>
</tr>
<tr>
<td>Policies and procedures</td>
<td>• Encryption mechanism to encrypt electronic PHI whenever deemed appropriate</td>
</tr>
<tr>
<td>Documentation</td>
<td>Ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic PHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.</td>
</tr>
<tr>
<td></td>
<td>Comply with the standards, implementation specifications, or other requirements of the security rule.</td>
</tr>
<tr>
<td></td>
<td>Comply in written (which may be electronic) form; and if an action, activity, or assessment is required to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment:</td>
</tr>
<tr>
<td></td>
<td>• Time limit to retain required documentation is for six years from the date of its creation or the date when it last was in effect, whichever is later</td>
</tr>
<tr>
<td></td>
<td>• Availability—documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains</td>
</tr>
<tr>
<td></td>
<td>• Updates—documentation must be reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of the electronic PHI</td>
</tr>
</tbody>
</table>

### Table 9-2  Federal Legislation That Impacts Health Information Management

<table>
<thead>
<tr>
<th>Federal Law or Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions of Participation (CoP) and Conditions for Coverage</td>
<td>Federal regulations that health care organizations must meet to participate in the Medicare and Medicaid programs. Organizations include:</td>
</tr>
</tbody>
</table>
| (CiC)                                                          | • Ambulatory Surgery Centers (ASCs)  
• Comprehensive Outpatient Rehabilitation Facilities (CORFs)  
• Critical Access Hospitals (CAHs)  
• Diabetes Self-Management Training Services  
• End-Stage Renal Disease (ESRD) Facilities  
• Home Health Agencies (HHAs)  
• Hospice  
• Hospitals  
• Intermediate Care Facilities for Persons with Mental Retardation (ICFMR)  
• Long-Term Care Facilities  
• Organ Procurement Organizations (OPOs)  
• Outpatient Physical Therapy Providers  
• Programs of All-Inclusive Care for the Elderly (PACE)  
• Psychiatric Hospitals and Units  
• Rehabilitation Hospitals and Units  
• Religious Non-Medical Health Care Institutions  
• Rural Health Clinics (RHCs)/Federally Qualified Health Centers (FQHCs)  
• Transplant Hospitals                                                                                          |
| Drug Abuse and Treatment Act of 1972                          | Federal law that requires drug and alcohol abuse patient records be kept confidential and not subject to disclosure except as provided by law. This law applies to federally assisted alcohol or drug abuse programs, which are those that provide diagnosis, treatment, or referral for treatment of drug and/or alcohol abuse. |
| Emergency Medical Treatment and Labor Act (EMTALA)            | Federal statute that addressed the problem of hospitals failing to screen, treat, or appropriately transfer patients by establishing criteria for the discharge and transfer of Medicare and Medicaid patients. (EMTALA is also called the “antidumping” statute.) |
| Federal Patient Self-Determination Act                        | Requires consumers to be provided with informed consent, information about their right to make advance health care decisions (or advance directives), and information about state laws that impact legal choices in making health care decisions. |
| Freedom of Information Act of 1966                           | Allows open access to federal agency records, except for those with specific exemptions.                                                                 |
| Health Care Quality Improvement Act of 1986                   | Federal law that established the National Practitioner Data Base (NPDB), which contains information about practitioners’ credentials, including previous medical malpractice payment and adverse action history. |
| HIPAA                                                          | The HIPDB was created to combat fraud and abuse in health insurance and health care delivery by alerting users to conduct a comprehensive review of a practitioner’s, provider’s, or supplier’s past actions. |
| Healthcare Integrity and Protection Data Bank (HIPDB)         | The OSH Act created the **Occupational Safety & Health Administration (OSHA)**, whose mission is to ensure safe and healthful workplaces in America. Since the agency was created in 1971, workplace fatalities have been cut in half and occupational injury and illness rates have declined 40 percent. At the same time, United States employment has doubled from 56 million workers at 3.5 million worksites to 111 million workers at 7 million sites. Violations of workplace safety are subject to monetary penalties ranging from $5,000 to $70,000 per incident or per day. |

(Continues)
### Table 9-2 Federal Legislation That Impacts Health Information Management (Continued)

<table>
<thead>
<tr>
<th>Federal Law or Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omnibus Budget Reconciliation Act of 1987</td>
<td>Federal legislation that created the Nursing Home Reform Act, which ensures that residents of nursing homes receive quality care, requires the provision of certain services to each resident, and establishes a Residents’ Bill of Rights.</td>
</tr>
<tr>
<td>Omnibus Budget Reconciliation Act of 1990</td>
<td>Federal legislation that requires reporting of adverse actions by CMS to state medical boards and licensing agencies.</td>
</tr>
<tr>
<td>Patient Access to Records</td>
<td>The HIPAA Privacy Rule states that “an individual has the right to inspect and obtain a copy of the individual’s protected health information (PHI) in a designated record set,” except for:</td>
</tr>
<tr>
<td></td>
<td>• Psychotherapy notes</td>
</tr>
<tr>
<td></td>
<td>• Information compiled in anticipation or use in a civil, criminal, or administration action or proceeding</td>
</tr>
<tr>
<td></td>
<td>• PHI subject to Clinical Laboratory Improvements Amendments (CLIA) of 1988, which is the federal law that delineates requirements for certification of clinical laboratories</td>
</tr>
<tr>
<td></td>
<td>• PHI exempt from CLIA (e.g., information generated by facilities that perform forensic testing procedures)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Individual states (e.g., New York State) may have passed laws or established regulations for patient access to records; providers must follow these laws or regulations if they are stricter than HIPAA provisions.</td>
</tr>
<tr>
<td>Patient Safety and Quality Improvement Act of 2005</td>
<td>Federal legislation, which amends Title IX of the Public Health Service Act, encourages the confidential reporting of health care mistakes to Patient Safety Organizations. Hospitals, doctors, and other health care providers can voluntarily report to Patient Safety Organizations (PSO) health care mistakes. The PSO will analyze the reported information on a privileged and confidential basis. The legislation includes the following:</td>
</tr>
<tr>
<td></td>
<td>• Confidential protections for information that is gathered during the review process</td>
</tr>
<tr>
<td></td>
<td>• Requirements that entities must meet to become PCOs</td>
</tr>
<tr>
<td></td>
<td>• Processes for the review and acceptance of PSO certifications</td>
</tr>
<tr>
<td>Privacy Act of 1974</td>
<td>Federal code of fair information practices that mandates how government agencies (e.g., military) shall maintain records about individuals and applies to government records that:</td>
</tr>
<tr>
<td></td>
<td>• Contain information on individuals</td>
</tr>
<tr>
<td></td>
<td>• Are maintained by a government agency or its contractors</td>
</tr>
<tr>
<td></td>
<td>• Are retrieved by a personal identifier (e.g., person’s name, Social Security number, medical record number)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Individuals can request access to their own records in writing or in person, except when records contain information that could have an “adverse effect.” In that case, the record is sent to a representative (e.g., family doctor) willing to review the record and inform the individual of its contents.</td>
</tr>
<tr>
<td>Uniform Healthcare Information Act (UHIA)</td>
<td>Federal legislation that serves as a model for state adoption and provides rules about health information management. The legislation includes the following provisions:</td>
</tr>
<tr>
<td></td>
<td>• Providers are prohibited from disclosing information to a third party without patient authorization.</td>
</tr>
<tr>
<td></td>
<td>• Providers are not required to provide patient information during a legal proceeding unless the patient has provided authorization in writing to the release, except in certain circumstances (e.g., subpoena duces tecum).</td>
</tr>
<tr>
<td></td>
<td>• Patients can have access to their own records (but providers can deny access).</td>
</tr>
<tr>
<td></td>
<td>• Patients can request providers to amend or correct patient information (but providers can refuse to amend or correct information) (Figure 9-7).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> As of 1996, only Montana and Washington had enacted this model legislation. (This may explain HIPAA’s privacy provisions.)</td>
</tr>
</tbody>
</table>
### Table 9-3  State Legislation That Impacts Health Information Management

<table>
<thead>
<tr>
<th>State Law or Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mental Health Records</td>
<td>State laws govern patient access and restrictions on disclosure of mental health records. <strong>EXAMPLE:</strong> California statutes specify that “no provider of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization . . .”</td>
</tr>
<tr>
<td>Reportable Diseases</td>
<td>Each state establishes a list of reportable communicable and other diseases for which providers must submit patient information to appropriate state agencies. • <strong>Local county public health department and the state department of health:</strong> cancer, human immunodeficiency virus (HIV), infectious diseases including isolated cases as well as community and/or facility outbreaks (e.g., encephalitis), nursing facility elder abuse, rabies, and sexually transmitted diseases (e.g., syphilis). <strong>NOTE:</strong> Any infectious diseases involving military personnel are also reported to the local military base’s office of preventive medicine (e.g., MacDill Air Force Base in Tampa, Florida).</td>
</tr>
<tr>
<td>Reportable Events</td>
<td>Each state establishes a list of reportable events for which providers must submit patient information to appropriate agencies. • <strong>Local law enforcement agencies:</strong> assault and battery, child abuse, child malnourishment, child neglect, dog bites, gunshot wounds, motor vehicle accidents, rape, sexual assault, stabbings, and any accidental injuries occurring on public property. (Assault is an unlawful threat or attempt to do bodily harm to another, such as threatening to withhold medication from a patient or to place the patient in restraints. <strong>Battery</strong> is unlawful touching, such as a surgeon performing a procedure on a patient without having obtained consent.) <strong>NOTE:</strong> State departments of health usually provide a toll-free number to report child abuse, child malnourishment, and child neglect. • <strong>State poison control centers:</strong> any overdose, regardless of whether accidental or intentional. • <strong>Organ and tissue donor agencies:</strong> deaths and imminent deaths of patients who are initially screened (by telephone) for potential donation. If a patient meets initial screening criteria, further workup may lead to an eventual request to the family for organ donation. • <strong>State department of health:</strong> hospital-wide reportable events, such as wrong patient, wrong site (surgical procedures), incorrect procedure or treatment, unintentionally retained foreign body due to inaccurate surgical count or break in procedural technique, cardiac and/or respiratory arrest requiring basic life support (BLS) or advanced cardiac life support (ACLS) intervention, errors of omission or delay in treatment resulting in death or serious injury related to the patient’s underlying condition, malfunction of equipment during treatment or diagnosis or a defective product causing death or serious injury. <strong>NOTE:</strong> Some states require adverse events to be reported using special software, such as the New York Patient Occurrence Reporting Tracking System (NYPORTS), and the data is made available to the public. In addition a <strong>root cause analysis</strong> must be performed on any event assigned ICD-9-CM codes 900–963, which is a process intended to find out what happened, why it happened, and what the facility can do to prevent it from happening again.</td>
</tr>
<tr>
<td>Retention of Records</td>
<td>State laws govern retention of records. Refer to the Chapter 7 discussion of this topic.</td>
</tr>
</tbody>
</table>
REQUEST FOR CORRECTION/AMENDMENT OF PROTECTED HEALTH INFORMATION

5 U.S.C. 522a(d) and 45 CFR 164.526

I agree to allow IHS to release any amended information to individuals or entities as described above.

In the event that IHS grants your request, in some situations where IHS previously disclosed the disputed record, IHS is required by law to notify the recipient of the corrective action taken. In addition, subject to your agreement IHS will make reasonable efforts to provide the amendment to other persons who IHS knows received the information in the past and who may have relied, or are likely to rely, on such information to your detriment.

I agree to allow IHS to release any amended information to individuals or entities as described above.

Would you like this amendment sent to anyone else who received the information in the past?

Yes ☐  No ☐  If yes, please specify the name and address of the organization(s) or individual(s) below.

SIGNATURE OF PATIENT OR LEGAL REPRESENTATIVE (If Legal Representative signs, state relationship to patient)  DATE

FOR IHS USE ONLY

DATE RECEIVED  AMENDMENT HAS BEEN ☐ Accepted ☐ Denied

IF DENIED, CHECK REASON FOR DENIAL:

☐ PHI is not part of the patient’s designated record set
☐ IHS did not create record
☐ Record is not available to the patient for inspection under federal law
☐ Record is accurate and complete

SIGNATURE OF SERVICE UNIT DIRECTOR OR DESIGNEE  DATE

COMMENTS OF HEALTHCARE PROVIDER (If applicable)

SIGNATURE OF HEALTHCARE PROVIDER (If applicable)  TITLE  DATE

Figure 9-7 Request to Correct/Amend PHI (Permission to reprint in accordance with IHS.gov Web reuse policy.)
Authorization to Disclose PHI Is Not Required

According to HIPAA, the following uses and disclosures of PHI do not require the covered entity (e.g., provider) to obtain consent or authorization from the patient, or to provide the opportunity for the patient to agree or object to disclosure:

- Health oversight activities
- Public health activities
- Law enforcement purposes
- Judicial and administrative proceedings
- Identification and location purposes
- Decedents
- Research purposes
- Food & Drug Administration (FDA)
- Specialized government functions (e.g., military and veterans activities)
- Workers’ compensation

Health Oversight Activities Authorized by Law

The covered entity (e.g., provider) may disclose PHI to health oversight agencies for activities authorized by law, including:

- Audits (e.g., quality improvement organization, QIO, studies)
- Civil, administrative, or criminal investigations (e.g., state office of professional misconduct)
- Inspections (e.g., state department of health on-site inspection, OSHA)
- Licensure or disciplinary actions (e.g., physician disciplinary action)
- Civil, administrative, or criminal proceedings or actions (e.g., subpoena duces tecum issued for records in a medical malpractice lawsuit)
- Other activities necessary for appropriate oversight of health care system (e.g., government benefit programs such as Medicare and Medicaid)

NOTE: If a covered entity is also a health oversight agency, the covered entity may use PHI for health oversight activities as outlined above.

Public Health Activities

The covered entity (e.g., provider) may disclose PHI for public health activities and purposes to:

- Public health authorities authorized by law to collect or receive reportable disease and/or event information (e.g., births, deaths, cancer cases)
- Public health authority or other government authority authorized by law to receive reports of child abuse or neglect (e.g., local law enforcement)
- Food and Drug Administration (FDA) for the purpose of tracking products; enabling product recalls, repairs, or replacement; and conducting post-marketing surveillance (e.g., adverse events, product defects or problems, or biological product deviations)
- Person(s) who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition (e.g., sexually transmitted disease)
- Employer, about an employee, to evaluate whether the individual has a work-related illness or injury (e.g., employee uses Workers’ Compensation benefits to receive health care services)

Law Enforcement Agencies

A covered entity may disclose PHI about victims of abuse, neglect, or domestic violence to a governmental authority that is authorized to receive such reports. The covered entity must promptly inform the individual that a report has been or will be made unless the covered entity:

- Believes that notification would place the individual at risk of serious harm
- Would be notifying a personal representative who is responsible for the abuse, neglect, or other injury (and, as such, would not be in the individual’s best interests)

A covered entity may also disclose PHI to law enforcement officials:

- When reporting certain types of wounds and injuries (e.g., gunshot wounds)
- In response to a law enforcement official’s request to assist in identifying or locating a suspect, fugitive, material witness, or missing person; only the following information may be disclosed:
  - Name and address
  - Date and place of birth
  - Social security number (SSN)
  - ABO blood type and Rh factor
  - Type of injury
  - Date and time of treatment
  - Date and time of death
• Distinguishing physical characteristics, including weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos

**NOTE:** The covered entity may *not* disclose for identification or location purposes any PHI relating to DNA or DNA analysis; dental records; or typing, samples, or analysis of body fluids or tissues.

The covered entity may disclose PHI in response to a law enforcement official’s request relating to an individual who is (or is suspected of being) a victim of a crime if the:

• Individual (alleged victim) agrees
• Covered entity is unable to obtain an individual’s agreement because of incapacity or other emergency provided that the:
  • Law enforcement official needs the information to determine if someone else committed a crime, and the PHI will not be used against the victim
  • Immediate law enforcement activity that depends on disclosure of the PHI would be materially and adversely affected by waiting
  • Covered entity, exercising professional judgment, believes disclosure is in the best interest of the victim

The covered entity may disclose a decedent’s (dead person’s) PHI to law enforcement if the death is suspected as resulting from criminal conduct and/or there is possible evidence that a crime was committed on the premises of the covered entity. Typically, suspicious deaths become coroner or medical examiner cases. A **coroner** is a public officer who investigates deaths due to other than natural causes. A **medical examiner** is a physician officially authorized by a governmental agency to determine causes of deaths, especially those due to other than natural causes.

**NOTE:** A medical examiner is always a physician, but a coroner might not be a physician. Coroners are elected individuals who are interested in this field (e.g., funeral director, veterinarians, and even health care professors).

A covered entity that provides off-site emergency medical care may report PHI to alert law enforcement as to the commission and nature of a crime, location of the crime and of crime victim(s), and the identity, description, and location of the perpetrator. PHI may be disclosed to a correctional institution or to a law enforcement official with custody of the individual when PHI is necessary to provide care to the individual, or for the health and safety of the individual, other inmates, correctional employees, transport employees, law enforcement personnel at the location, and for the safety, security, and good order of the institution. Covered entities that are correctional institutions may use PHI for any purpose. An individual is no longer an inmate once released on parole, probation or supervised release, or is otherwise no longer in lawful custody.

**Judicial or Administrative Proceedings**

A covered entity may disclose PHI in the course of any judicial or administrative proceeding in response to a(n):

• Court order, but only the PHI expressly authorized for release by such order
• *Subpoena duces tecum*, if the covered entity has satisfactory assurance:
  • From the party seeking the PHI that reasonable efforts have been made to give the individual notice of the request
  • From the party seeking the PHI that reasonable efforts have been made to secure a qualified protective order
  • That the individual has been given notice. This condition may be met by provision of a written statement and accompanying documentation demonstrating that the
    • party requesting the PHI has made a good faith attempt to provide written notice to the individual
    • notice includes sufficient information about the litigation or proceeding to permit the individual to raise an objection in the tribunal and
    • time to raise objections has lapsed and either no objection was filed or objections have been resolved in a manner consistent with disclosure
  • That reasonable efforts have been made to secure a qualified protective order. This may be met by provision of a written statement and accompanying documentation demonstrating that the parties to the dispute have agreed to a qualified protective order and presented it to the tribunal, or the party seeking the PHI has requested a qualified protective order from the tribunal.

A **qualified protective order** prohibits the use or disclosure of PHI for any purpose beyond the litigation at hand, and requires that the PHI, and all copies, be returned to the covered entity or destroyed when the litigation is over.
Identification and Location Purposes
Information for the identification and location of an individual is limited to the following:

- Name and address
- Date and place of birth
- Social security number
- ABO blood type and Rh factor
- Type of injury
- Date and time of treatment
- Date and time of death
- Description of physical characteristics

**NOTE:** DNA, dental records, typing samples, or analysis of body fluids or tissue cannot be disclosed unless the request for information is accompanied by appropriate legal documents or the individual authorizes disclosure.

The de-identification of protected health information (PHI) contains no identification information about an individual; de-identified information can be disclosed (e.g., for research purposes) if nothing can individually identify the patient. The following identifiers are removed:

- Names
- Addresses and other geographic identifiers
- Relatives
- Employers or household members
- Zip codes
- All dates (except years) related to an individual
- Numbers
  - Telephone
  - Fax
  - SSN
  - Medical records
  - Beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - VIN numbers
  - License plate numbers
  - Device identifiers and serial numbers
  - URLs
  - IP address
  - Biometric identifiers
  - Photographic images and any other unique identifying number, characteristic, or code

Decedents
Covered entities are allowed to disclose PHI to the following in order to carry out their duties with respect to the deceased person:

- Coroners and medical examiners
- Funeral directors
- Cadaver organ, eye, or tissue donation purposes

Research Purposes
Most health care providers routinely allow medical professionals engaged in clinical or epidemiological research to access patient records, abstract individually identifiable information (e.g., date of birth, birthplace, and so on), and exchange that information with other researchers. A covered entity may use or disclose protected health information (PHI) without obtaining written authorization of the individual for activities and purposes associated with research that has been approved by an Institutional Review Board (IRB) or a privacy board. While it is not practical to require researchers to obtain authorizations from patients, it is necessary to review and approve research projects so that patients’ privacy is protected.

**NOTE:** An authorization for the use and disclosure of PHI is required when research includes the actual treatment of the individual.

**EXAMPLE 1**
The search for the cause of “Legionnaires’ Disease” would have been almost impossible to conduct if researchers had been required to obtain patient authorizations before reviewing medical records. (Some victims were not located until months after the event.)

**EXAMPLE 2**
A researcher conducting a follow-up study of individuals who had been enrolled in a methadone maintenance program had the name and address of one individual who had been enrolled several years previously. The researcher went to the individual’s residence on a Saturday night, interrupting a party, and announced “Hi, I am so-and-so from such-and-such an organization, and we are doing a follow-up study of patients who had been enrolled in the methadone maintenance program.”

Food and Drug Administration (FDA)
A covered entity may disclose protected health information (PHI) without obtaining authorization from the individual to the jurisdiction of the Food and Drug Administration (FDA) regarding FDA-regulated products or activities related to quality, safety, or effectiveness of products or activities and to collect or report adverse events, product defects, or problems. Such disclosure allows for the tracking of FDA-regulated products to enable recalls, repairs, or
replacements. Individuals can be located and notified about product defects or problems, and post-marketing surveillance can be conducted.

**Specialized Government Functions**

A covered entity may use or disclose protected health information (PHI) without obtaining authorization from the individual for the following:

- Medicare
- Medicaid
- Military and veterans activities
- Armed forces personnel
- National security and intelligence activities
- Protective services for the president and others
- Medical suitability determinations
- Correctional institutions for the provision of health care

**NOTE:** Proper procedure and appropriate documentation is required from the requesting source.

**EXAMPLE**

Army patients often transport their own medical records from one military location to another, and in the process soldiers occasionally discard their records accidentally. Many military bases release medical records in a “can” so that “garbage pickers” can go through dumpsters on a weekly basis to look for the cans and return them (with medical records inside) to the medical records department. Some soldiers place their medical records at the bottom of their duffel bag and forget about them. When the soldier cannot find the record, the Army gets blamed for the loss. Sometimes soldiers even remove reports from their records because they are afraid that such information will be held against them for promotion purposes. The Army recognizes these problems and is taking several steps to resolve them. The electronic medical record (EMR) is one such measure, another is ensuring that the permanent record does not deploy with the soldier, and the Army is also working on a SMART card that would contain a computer chip of the soldier’s medical record.

**Workers’ Compensation**

A covered entity may disclose protected health information to comply with Workers’ Compensation laws that provide benefits for work-related injuries or illness regardless of fault.

**NOTE:** Many state laws prohibit disclosure of PHI for Workers’ Compensation purposes unless the patient has signed an authorization for release of information.

In these circumstances, state law supersedes the HIPAA privacy standard. This means you must follow state law and obtain patient authorization to release information for Workers’ Compensation purposes.

**Authorization to Disclose PHI Is Required**

The patient’s authorization to disclose protected health information (PHI) must be obtained for the following circumstances:

- Attorney requests (except the provider’s attorney when the PHI is released during a normal course of business, such as to prepare for a medical malpractice lawsuit)
- Employers (except when PHI is released to report work-related illnesses or injuries)
- Government agencies (e.g., Department of Social Services, Bureau of Disability Determinations, and so on)
- Health care providers that did not render care to the patient
- HIV-related information
- Internal Revenue Service (IRS)
- Law enforcement (e.g., police, FBI, CIA, and so on, except when no authorization is required by HIPAA)
- Marketing communications (e.g., reports to news media)
- Patient or patient representative (except when no authorization is required by HIPAA)
- Research that includes treatment of an individual
- Third-party payers (e.g., insurance companies, except in the course of TPO)
- Workers’ Compensation carriers (when required by state law)

Covered entities are allowed to maintain a directory of the following patient information (unless the patient objects): patient name, location in the facility, condition described in general terms that do not communicate specific medical information, and religious affiliation. Directory information can be disclosed to members of the clergy or to other persons who ask for the individual by name.

**Attorney Requests**

The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all attorneys, except the provider’s attorney when the PHI is released during a normal course of business, such as to prepare for a medical malpractice lawsuit.
Prior to processing a request for the release of PHI to an attorney, notify your facility’s risk manager to determine if a review of the record should be conducted. Such a review could alert appropriate facility personnel to the potential for a lawsuit where the facility is named as defendant.

**NOTE:** Upon review of the record, the risk manager will search for any incident reports completed on the patient.

**Remember!** Incident reports are *never* filed in the medical record because that would subject them to disclosure. Incident reports are internal administrative documents completed by health care personnel about the events of an incident. They allow those called to testify (e.g., primary care nurse) in a lawsuit to review the events of an incident prior to testimony.

**Employers**

The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all employers, *except* when PHI is released to report work-related illnesses or injuries. In addition, as permitted by state law, covered entities may release information to self-insured employers when PHI is needed to process payment for health care provided. In this situation, self-insured employers must agree to protect the individual’s data from internal disclosure that would affect the individual.

**Government Agencies**

The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all government agencies, *except* as required by HIPAA. This means that government agencies such as the Department of Social Services and the Bureau of Disability Determinations must provide a patient authorization to release PHI before receiving that information.

**Health Care Providers**

The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all health care providers, *except* those involved in direct care of the patient.

**NOTE:** When a health care provider contacts you to request PHI during an emergency situation, be sure to implement the call-back method, which involves obtaining the requesting provider’s main number from the phonebook or directory assistance. Call the main number and ask to be connected to the requesting provider to ensure that you are speaking with an individual authorized to obtain PHI. As a follow-up, require the requesting provider to obtain the patient’s authorization to release PHI and mail it to your attention.

**HIV-Related Information**

Confidential human immunodeficiency virus (HIV) related information is any information indicating that a person had an HIV-related test; or has HIV infection, HIV-related illness, or Acquired Immunodeficiency Syndrome (AIDS); or any information that could indicate a person has been potentially exposed to HIV. Many states have passed legislation governing the release of HIV-related information, including New York State, which states

[C]onfidential HIV related information can only be disclosed after the patient has signed a written release [Figure 9-8]. Exceptions to this disclosure law include those who need to know a patient’s HIV status to provide medical care and services, including:

- Medical care providers
- Persons involved with foster care or adoption
- Parents and guardians who consent to care of minors
- Jail, prison, probation, and parole employees
- Emergency response workers
- Other workers in hospitals, other regulated settings, or medical offices, who are exposed to blood/body fluids in the course of their employment
- Organizations that review the services the patient received

State law also allows HIV information to be released under limited circumstances:

- Special court order
- Public health officials as required by law
- Insurers as necessary to pay for care and treatment

Under State law, anyone who illegally discloses HIV related information may be punished by a fine of up to $5,000 and a jail term of up to one year.

The covered entity must obtain the patient’s authorization to disclose HIV-related PHI.

**Internal Revenue Service (IRS)**

The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to the Internal Revenue Service (IRS).
Legal Aspects of Health Information Management

Figure 9-8  Authorization for Release of Confidential HIV-Related Information (This form, and any updates to it, is available to the public on the New York State Department of Health Web site, http://www.health.state.ny.us.)
Law Enforcement Agencies
The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all law enforcement agencies, except when no authorization is required by HIPAA.

Marketing Communications
The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) for all marketing communications, including reports to news media. This means that a provider cannot sell PHI to a company that wants to market its products and services.

NOTE: HIPAA does allow for the marketing of fund-raising activities if the only PHI used or disclosed is demographic information and dates of service. However, the facility’s privacy notice must describe the use and/or disclosure of individually identifiable PHI for fund raising and include information on how an individual can opt out of fund-raising mailings.

Patient or Patient Representative
The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to the patient or patient representative, except when no authorization is required by HIPAA.

If urgent or continuing care is required and the patient is incapacitated, state health information disclosure laws contain provisions for a patient representative to authorize the release of PHI. If a state law does not exist, AHIMA’s practice brief on disclosure states, “Information may be disclosed without patient authorization as required for continued care.” In emergency situations, case law recognizes exceptions to authorization to release PHI. In an emergency situation, be sure to follow the call-back method discussed earlier in this chapter.

NOTE: For additional information, refer to the discussion of patient access to records that follows.

Research That Includes Treatment of an Individual
The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all health care providers, except those involved in direct care of the patient.

Third-Party Payers
The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all third-party payers, except in the course of treatment, payment, and health care operations (TPO).

Workers’ Compensation Carriers
The covered entity must obtain the patient’s authorization to disclose protected health information (PHI) to all Workers’ Compensation carriers, when required by state law.

Patient Access to Records
An individual has the right to access his or her own protected health information (PHI) for the purpose of inspection and to obtain a copy, except for the following:

• Psychotherapy notes
• Information compiled for use in a civil, criminal, or administrative action
• PHI maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA)

NOTE: An emancipated minor may authorize disclosure of PHI. State laws define emancipated minors as married, living away from home and self-supporting, declared legally emancipated by a court of law, pregnant and unmarried, on active duty with the United States Armed Forces, at least 16 years of age and living independently from parents or guardians. In addition, if state laws permit a minor to seek alcohol or drug abuse treatment, the minor can authorize disclosure of PHI.

A covered entity can deny an individual the right to access his or her PHI if the:

• PHI is exempt from the right of access (above)
• Individual’s access to PHI was created or obtained by a covered entity during research—including treatment that may be suspended while the research is in progress, if the individual agreed to the denial of access when consenting to participate in the research and if the provider informed the individual that right of access would be reinstated upon completion of research
• Individual’s access to PHI is contained in records subject to the Privacy Act, which may be denied in accordance with the requirements of the Act
• PHI was obtained from someone other than a covered entity under a promise of confidentiality and the access would likely reveal the source of the information.

• Covered entity is a correctional institution or a covered health care provider acting under direction of a correctional institution.

**NOTE:** Correctional institutions may deny an inmate’s access to PHI if access would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or entity responsible for transporting the inmate.

The covered entity may deny an individual access to PHI, provided the individual is given a right to have such denials reviewed, in the following circumstances:

• A licensed health care professional has determined, in the exercise of professional judgment, that access is likely to endanger the life or physical safety of the individual or another person.

• The PHI makes reference to another person (not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.

• The request for access is made by the individual’s personal representative and the PHI makes reference to another person (not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual or another person.

**NOTE:** If patient access to PHI is denied and the individual has the right to have the denial reviewed, that review must be conducted by a licensed health care professional who is designated as a reviewing official and who did not participate in the original decision to deny access.

A covered entity may require individuals to make requests for access to PHI in writing if it has informed individuals of this requirement. The covered entity must comply with a patient access request no later than 30 days after receipt of the request, as follows:

• If the request is for access to PHI that is not maintained or accessible to the covered entity on-site, the covered entity must act on the request no later than 60 days from receipt of the request.

• If the covered entity is unable to act on the request within the appropriate time limit (30 or 60 days, as applicable), it may extend the time for such actions by no more than 30 days (if the individual has been notified in writing about the delay).

**NOTE:** The covered entity may charge a reasonable cost-based fee for copying PHI, postage, and/or preparing an explanation or summary of the PHI, if agreed to by the individual. The covered entity may not charge a fee for retrieval of PHI or monitoring an individual’s review of PHI.

### Prohibition on Redisclosure

When copies of protected health information (PHI) are appropriately released to a provider, they are usually filed in the patient’s current medical record. That provider is prohibited from redisclosing another entity’s copies of PHI unless authorized to do so, as follows:

• The Drug Abuse and Treatment Act of 1972 requires that the following notice accompany each disclosure of PHI:

  This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

• The HIPAA Final Privacy Rule requires that the patient authorization to disclose PHI contain a general statement that

  PHI may no longer be protected by the Privacy Rule once it is disclosed by the covered entity.

This means a provider is allowed to redisclose PHI created by another if disclosure is for a purpose permitted by the privacy rule (e.g., treatment).

When releasing copies of PHI from a patient’s medical record, be sure to include a cover sheet that
includes a statement prohibiting redisclosure unless authorized. The following language is suggested:

This protected health information (PHI) has been disclosed to you from confidential records that are protected by Federal and State law. You are prohibited from redisclosure of this PHI without the specific written authorization of the individual to whom it pertains (or his representative), or as permitted by State law, or as otherwise permitted by Federal law (e.g., to provide urgent patient care). Any unauthorized redisclosure in violation of Federal or State law may result in a fine or jail sentence or both.

**Tracking Disclosures of PHI**

Health information departments have traditionally maintained a release of information log to document patient information released to authorized requestors, and data was entered manually (e.g., three-ring binder) or using tracking software. The HIPAA privacy rule requires covered entities to track the release of protected health information (PHI) so that individuals can obtain an accounting of disclosures for the six years prior to the date of their request, retroactive to April 16, 2003. To respond to this requirement, each covered entity must establish a tracking mechanism and reporting process that includes the following:

- Date of disclosure
- Name and address of the entity or person who received the PHI
- Description of the PHI disclosed
- Statement of reason for disclosure (or a copy of the written request for disclosure)

**NOTE:** If an entity releases PHI to the same entity for the same reason, the first disclosure is documented along with the number of disclosures made during the accounting period and the date of the last disclosure in the accounting period.

An individual has the right to receive an accounting of all disclosures of protected health information (PHI) made by a covered entity during the six years prior to the date an accounting is requested, except for disclosures:

- To carry out treatment, payment, and health care operations (TPO)
- To individuals, themselves, of PHI
- Entered in the facility’s directory
- To persons involved in the individual’s care
- For other notification purposes, such as:
  - National security or intelligence purposes
  - Correctional institutions or law enforcement officials
  - Those that occurred prior to the compliance date for the covered entity

**NOTE:** A covered entity must temporarily suspend an individual’s right to an accounting of disclosures if a health oversight agency or law enforcement official notifies the covered entity in writing that such an accounting would be reasonably likely to impede the agency’s activities. The temporary suspension must include an expiration date.

When an individual requests an accounting of disclosed PHI, the covered entity has 60 days to act on the request and one 30-day extension is allowed. If there is a delay in responding to the individual’s request for an accounting, the covered entity must inform the individual of the delay in writing and provide a reason for the delay and the date the accounting will be provided.

Covered entities should select a method for tracking disclosures that will work best for them such as a(n):

- Computerized tracking system (use database or spreadsheet software to collect required elements and to automate production of an individual’s accounting report) (Figure 9-9, Figure 9-10, Figure 9-11)
- Manual PHI disclosure record (generate a log sheet for each individual, a copy of which serves as an individual’s accounting report) (Figure 9-12)
- Authorization form (e.g., store authorization forms signed by an individual in one folder to track disclosure of PHI, copies of which serve as an individual’s accounting report) (NOTE: The problem with this method is that not all disclosures require patient authorization, so this results in an incomplete accounting.)

A covered entity must provide an individual with one free accounting report during any 12-month period. Subsequent reports generated during the 12-month period can be assessed a reasonable fee (based on the entity’s costs of providing the accounting report). The covered entity must inform an individual of any required fee and allow the individual an opportunity to amend his or her request to avoid or reduce the fee.
**Figure 9-9** Flow of Released PHI Using Automated Tracking Software (Permission to reprint granted by IO Datasphere, Inc.)

**Figure 9-10** Disclosure Tracking Software Screen (Permission to reprint granted by IO Datasphere, Inc.)
Exercise 9–5 Release of Protected Health Information

Short Answer: For each scenario, provide an appropriate response.

1. Miss Molly, a release of information clerk at New Directions Medical Center, received a call from the Pathway Drug and Alcohol Rehabilitation Center. Pathway is assuming care for a patient who is being discharged from New Directions today. Pathway is requesting that a copy of the patient's biopsychosocial report be faxed to them. What action should Miss Molly take?

2. Ms. Marie, a health information department staff member at New Directions Medical Center, received a call from the emergency room at St. John’s Hospital requesting that all previous records for a patient named Sally Smith be faxed to them immediately. (Sally Smith was a health information department staff member at New Directions, and she resigned last year to return to college full-time.) Because of the urgency of her medical condition, Sally Smith is being taken to the surgery suite immediately. Ms. Marie knows Sally’s family and is considering calling Sally’s sister. What action should Ms. Marie take?

3. Pam Page, an office manager for Dr. Brown, receives an email from a patient requesting that she reply with his lab test results. Pam knows that the office’s email system does not encrypt messages. What action should Pam take?

INTERNET LINKS

Go to http://hipaa.yale.edu for information on HIPAA. The privacy rule is enforced by the DHHS Office for Civil Rights (OCR), and more information can be found at http://www.hhs.gov/ocr/hipaa.
### PROTECTED HEALTH INFORMATION (PHI) DISCLOSURE RECORD

**Patient Name:**

**DOB:**

**Authorized Methods of Communication**

- Residence Telephone
- Work Telephone
- Written Correspondence
- Other (Specify)

<table>
<thead>
<tr>
<th>Residence Telephone</th>
<th>Work Telephone</th>
<th>Written Correspondence</th>
<th>Other (Specify)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number: ( )</td>
<td>Number: ( )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leave call back number only; do not leave message</td>
<td>Leave call back number only; do not leave message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Okay to leave detailed message with person</td>
<td>Okay to leave detailed message with operator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Okay to leave detailed message on answering machine</td>
<td>Okay to leave detailed message on personal voicemail</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Patient Signature:**

**Date:**

**Record of Disclosures**

<table>
<thead>
<tr>
<th>Date of Disclosure</th>
<th>Disclosed To</th>
<th>Description of PHI Disclosed and Purpose of Disclosure (If a copy of the authorization or request is attached, check “O” below)</th>
<th>Type of Disclosure</th>
<th>Person Receiving</th>
<th>Method of Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* T = Treatment, P = Payment, O = Health Care Operations Activities
** M = Mail, P = Telephone, F = Fax, E = Email, OT = Other (and specify mode of delivery)

---

**Figure 9-12** Manual PHI Disclosure Record (Reprinted with permission of Bibbero Systems, Inc., Petaluma, CA. (800) 242-2376. www.bibbero.com.)
Go to http://www.ahima.org and search on HIPAA for a wealth of information on the regulation.
Go to http://cms.hhs.gov/cop. Locate the CMS Conditions of Participation (CoP) and Conditions for Coverage (CfC).
Go to the Electronic Privacy Information Center (EPIC) at http://www.epic.org, to find location and information about privacy.
The official United States gateway to government information is http://www.usa.gov.
The Privacy Rights Clearinghouse at http://www.privacy.org has lots of resources, including fact sheets that explain HIPAA privacy regulations.
The federal regulatory clearinghouse at http://www.regulations.gov contains a link to regulations published in the Federal Register.
Visit the Occupational Safety & Health Administration (OSHA) at http://www.osha.gov.
Go to http://www.himss.org, and search on the words privacy, security, and HIPAA for information on these topics.
Go to http://www.AllLaw.com and click on the STATE link where you can search for state legislation (e.g., consents).

SUMMARY
There are numerous sources of laws that impact health care: the Constitution of the United States, individual state constitutions, administrative law, case law (or common law), and statutory law. The medical record is a legal business record that must be maintained according to accreditation standards, legal principles, professional practice standards, and regulations. The Health Insurance Portability and Accountability Act of 1996 established privacy and security provisions. Both federal and state legislation impacts health information management, and HIM professionals must manage health information according to the strictest legislation.

STUDY CHECKLIST
- Read the textbook chapter, and highlight key concepts. (Use colored highlighter sparingly throughout the chapter.)
- Create an index card for each key term. (Write the key term on one side of the index card and the concept on the other. Learn the definition of each key term, and match the term to the concept.)
- Access chapter Internet links to learn more about concepts.
- Answer the chapter Exercises and Review questions, verifying answers with your instructor.
- Complete the chapter StudyWare activities.
- Complete WebTutor assignments and take online quizzes.
- Complete lab manual assignments, verifying answers with your instructor.
- Form a study group with classmates to discuss chapter concepts in preparation for an exam.

CHAPTER REVIEW
True/False: Indicate whether the statement is True (T) or False (F).
1. The plaintiff is the individual who initiates a civil complaint and has the burden of proof.
2. Res ipsa loquitur is Latin for “things done,” which means that something is self-evident.
3. Medical malpractice results when a physician acts in an improper manner and the patient is not satisfied with the care given.
4. The HIPAA security rule specifies that facilities implement workstation security measures, which establish physical safeguards for all workstations that access electronic protected health information (PHI) to restrict access to authorized users only.
5. A breach of confidentiality occurs when a health care provider releases patient information to others who do not have a right to access the information.

Multiple Choice: Select the most appropriate response.
6. A security management process that assesses potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information is a(n)
   a. information system activity review.
   b. risk analysis.
   c. risk management review.
   d. security policy.
7. Public law deals with relationships between individuals and the government, and includes
   a. criminal law and torts.
   b. contracts and torts.
   c. criminal law and regulations.
   d. contracts and regulations.
8. The Latin phrase for “let the master answer,” which means an employer is responsible for the legal consequences of an employee’s actions, is called
   a. res gestae.
   b. respondeat superior.
   c. stare decisis.
   d. subpoena ad testificandum.

9. Safeguards that are implemented to ensure that facilities, equipment, and patient information are safe from damage, theft, or unauthorized access are known as ______ safeguards.
   a. administrative
   b. implementation
   c. privacy
   d. security

10. A technical safeguard that records and examines activity in information systems that contain or use electronic protected health information is called
    a. access control.
    b. audit control.
    c. security safeguard.
    d. security control.

Fill-In-The-Blank: Enter the appropriate term(s) to complete each statement.

11. The HIPAA privacy rule establishes standards for how ______ should be controlled.

12. Any information communicated by a patient to a health care provider is private and is also considered ______.

13. When patient information is released to individuals who do not have a right to access the information, ______ occurs.

14. The HIPAA privacy rule established provisions for all medical records and other individually identifiable health information used or disclosed by a covered entity in any form including electronic, ______, or ______.

15. Providers are required to obtain ______ before disclosing information for treatment, payment, and health care operations.

Short Answer: Briefly respond to each question.

16. Civil monetary and federal criminal penalties apply when covered entities misuse protected health information. Discuss the penalties.

17. Sources of law include administrative, case, and statutory law. Discuss each type of law.

18. For a medical record to be considered admissible as evidence, the records must be maintained according to four principles. Discuss the four principles.

19. Define protected health information (PHI).

20. Policies and procedures should be established by covered entities to meet the HIPAA privacy rule standards. Outline what covered entities should do to meet this standard.