learning outcomes

After studying this chapter, you should be able to:

2.1 Explain the importance of accurate documentation when working with medical records.
2.2 Compare the intent of HIPAA and ARRA/HITECH laws.
2.3 Describe the relationship between covered entities and business associates.
2.4 Explain the purpose of the HIPAA Privacy Rule.
2.5 Briefly state the purpose of the HIPAA Security Rule.
2.6 Explain the purpose of the HITECH Breach Notification Rule.
2.7 Explain how the HIPAA Electronic Health Care Transactions and Code Sets standards influence the electronic exchange of health information.
2.8 Explain how to guard against potentially fraudulent situations.
2.9 Explain how various organizations enforce HIPAA.
2.10 Assess the benefits of a compliance plan.

Key Terms

- abuse
- accountable care organization (ACO)
- accounting of disclosure
- American Recovery and Reinvestment Act (ARRA) of 2009
- audit
- authorization
- breach
- breach notification
- business associate (BA)
- Centers for Medicare and Medicaid Services (CMS)
- clearinghouse
- code set
- compliance plan
- covered entity (CE)
- de-identified health information
- designated record set (DRS)
- documentation
- electronic data interchange (EDI)
- encounter
- encryption
- evaluation and management (E/M)
- fraud
- Health Care Fraud and Abuse Control Program
- health information exchange (HIE)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- HIPAA Electronic Health Care Transactions and Code Sets (TCS)
- HIPAA National Identifiers
- HIPAA Privacy Rule
- HIPAA Security Rule
- informed consent
- malpractice
- meaningful use
- medical documentation and billing cycle
- medical record
- medical standards of care
- minimum necessary standard
- National Provider Identifier (NPI)
- Notice of Privacy Practices (NPP)
- Office for Civil Rights (OCR)
Medical insurance specialists work with important clinical data as well as demographic data. Health plans need patient clinical information to assess the medical necessity of claims sent for payment. To provide the right level of care, other physicians need to know the results of tests and examinations that patients have already had. Keeping all these patient data safe and secure is the job of everyone on the healthcare team. But it is no longer a job of managing stacks of paper files. Like shopping, buying tickets, banking, and sharing photos online, healthcare records are moving to a digital platform. Working in this environment requires knowledge of electronic health records and of the federal rules that regulate access to them.

2.1 Medical Record Documentation: Electronic Health Records

A patient's medical record contains facts, findings, and observations about that patient’s health history. The record also contains communications with and about the patient. In a physician practice, the medical record begins with a patient’s first contact and continues through all treatments and services. The record provides continuity and communication among physicians and other healthcare professionals who are involved in the patient’s care. Patients’ medical records are also used in research and for education.

Medical Records

Medical records, or charts, contain documentation of patients’ conditions, treatments, and tests that are created and shared by physicians and other providers to help make accurate diagnoses and to trace the course of care.

COMPLIANCE GUIDELINE

Medical Standards of Care and Malpractice

Medical standards of care are state-specified performance measures for the delivery of healthcare by medical professionals. Medical malpractice can result when a provider injures or harms a patient because of failure to follow the standards.

Example

A patient’s medical record contains the results of all tests a primary care physician (PCP) ordered during a comprehensive physical examination. To follow up on a problem, the PCP refers the patient to a cardiologist, also sending the pertinent data for that doctor’s review. By studying the medical record, the specialist treating a referred patient learns the outcome of previous tests and avoids repeating them unnecessarily.

Documentation means organizing a patient’s health record in chronological order using a systematic, logical, and consistent method. A patient’s health history, examinations, tests, and results of treatments are all documented. Complete and comprehensive documentation is important to show that physicians have followed the medical standards of care that apply in their state. Healthcare providers are liable (that is, legally responsible) for providing this level of care to their patients. The term medical professional liability describes this responsibility of licensed healthcare professionals.
Patient medical records are legal documents. Good medical records are a part of the physician’s defense against accusations that patients were not treated correctly. They clearly state who performed what service and describe why, where, when, and how it was done. Physicians document the rationale behind their treatment decisions. This rationale is the basis for medical necessity—the clinically logical link between a patient’s condition and a treatment or procedure.

Advantages of Electronic Health Records

Because of their advantages over traditional paper records, electronic health records are now used by nearly 60 percent of physician practices (National Center for Health Statistics, 2011 survey). Electronic health records (EHRs) are computerized lifelong healthcare records for an individual that incorporate data from all sources that treat the individual.

EHRs are different from electronic medical records (EMRs), which are computerized records of one physician’s encounters with a patient over time that are the physician’s legal record of patient care. EHRs are also different from a third type of electronic record, personal health records (PHRs), which are private, secure electronic files that are created, maintained, and controlled by patients and contain data such as their current medications, health insurance information, allergies, medical test results, family medical history, and more.

Documents in electronic health records may be created in a variety of ways, but they are ultimately viewed on a computer screen. For example, one general practice uses a number of medical-history-taking templates for gathering and recording “consistent history and physical information from patients.” The computer-based templates range in focus from abdominal pain to depression, with from ten to twenty questions each. The on-screen templates are filled out in the exam rooms. Responsible providers then sign the entries, using e-signature technology that verifies the identity of the signer.

EHRs offer both patients and providers significant advantages over paper records:

- **Immediate access to health information:** The EHR is simultaneously accessible from computers in the office and in other sites such as hospitals. Compared to sorting through papers in a paper folder, an EHR database can save time when vital patient information is needed. Once information is updated in a patient record, it is available to all who need access, whether across the hall or across town.

- **Computerized physician order management:** Physicians can enter orders for prescriptions, tests, and other services at any time. This information is then transmitted to the staff for implementation or directly to pharmacies linked to the practice.

- **Clinical decision support:** An EHR system can provide access to the latest medical research on approved medical websites to help medical decision making.

- **Automated alerts and reminders:** The system can provide medical alerts and reminders for office staff to ensure that patients are scheduled for regular screenings and other preventive practices. Alerts can also be created to identify patient safety issues, such as possible drug interactions.

- **Electronic communication and connectivity:** An EHR system can provide a means of secure and easily accessible communication between physicians and staff and in some offices between physicians and patients.

- **Patient support:** Some EHR programs allow patients to access their medical records and request appointments. These programs also offer patient education on health topics and instructions on preparing for common medical tests, such as an HDL cholesterol test.

- **Administration and reporting:** The EHR may include administrative tools, including reporting systems that enable medical practices to comply with federal and state reporting requirements.

- **Error reduction:** An EHR can decrease medical errors that result from illegible chart notes because notes are entered electronically on a computer or a handheld.
device. Nevertheless, the accuracy of the information in the EHR is only as good as the accuracy of the person entering the data; it is still possible to click the wrong button or enter the wrong letter.

**Documenting Encounters with Providers**

Every patient encounter—the face-to-face meeting between a patient and a provider in a medical office, clinic, hospital, or other location—should be documented with the following information:

- Patient's name
- Encounter date and reason
- Appropriate history and physical examination
- Review of all tests that were ordered
- Diagnosis
- Plan of care, or notes on procedures or treatments that were given
- Instructions or recommendations that were given to the patient
- Signature of the provider who saw the patient

In addition, a patient's medical record must contain:

- Biographical and personal information, including the patient's full name, Social Security number, date of birth, full address, marital status, home and work telephone numbers, and employer information as applicable
- Records of all communications with the patient, including letters, telephone calls, faxes, and e-mail messages; the patient's responses; and a note of the time, date, topic, and physician's response to each communication
- Records of prescriptions and instructions given to the patient, including refills
- Scanned records or original documents that the patient has signed, such as an authorization to release information and an advance directive
- Drug and environmental allergies and reactions, or their absence
- Up-to-date immunization record and history if appropriate, such as for a child
- Previous and current diagnoses, test results, health risks, and progress
- Records of referral or consultation letters
- Hospital admissions and release documents
- Records of any missed or canceled appointments
- Requests for information about the patient (from a health plan or an attorney, for example), and a detailed log of to whom information was released

Medicare’s general documentation standards are shown in Table 2.1 on page 39. Figure 2.1 shows a patient record screen.

**Evaluation and Management Services Reports**

When providers evaluate a patient’s condition and decide on a course of treatment to manage it, the service is called *evaluation and management (E/M)*. Evaluation and management services may include a complete interview and physical examination for a new patient or for a new problem presented by a person who is already a patient. There are many other types of E/M encounters, such as a visit to decide whether surgery is needed or to follow up on a patient's problem. An E/M service is usually documented with chart notes.

**BILLING TIP**

**SOAP Format**

A common documentation structure is the *problem-oriented medical record (POMR)* that contains SOAP notes—Subjective information from the patient, and three elements the provider enters: Objective data such as examination and/or test results, Assessment of the patient’s diagnosis, and Plan, the intended course of treatment, such as surgery or medication.
Table 2.1 Documentation Pointers

1. Medicare expects the documentation to be generated at the time of service or shortly thereafter.

2. Delayed entries within a reasonable time frame (twenty-four to forty-eight hours) are acceptable for purposes of clarification, error correction, and addition of information not initially available, and if certain unusual circumstances prevented the generation of the note at the time of service.

3. The medical record cannot be altered. Errors must be legibly corrected so that the reviewer can draw an inference about their origin. Corrections or additions must be dated, preferably timed, and legibly signed or initialed.

4. Every note stands alone—that is, the performed services must be documented at the outset.

5. Delayed written explanations will be considered for purposes of clarification only. They cannot be used to add and authenticate services billed and not documented at the time of service or to retrospectively substantiate medical necessity. For that, the medical record must stand on its own, with the original entry corroborating that the service was rendered and was medically necessary.

6. All entries must be legible to another reader to a degree that a meaningful review can be conducted.

7. All notes should be dated, preferably timed, and signed by the author.

**History and Physical Examination** A complete history and physical (H&P) is documented with four types of information: (1) the chief complaint, (2) the history and physical examination, (3) the diagnosis, and (4) the treatment plan.

The provider documents the patient’s reason for the visit, often using the patient’s own words to describe the symptom, problem, condition, diagnosis, or other factor. For clarity, the provider may restate the reason as a “presenting problem,” using medical terminology.

![Patient Chart](image-url)
The provider also documents the patient’s relevant medical history. The extent of the history is based on what the provider considers appropriate. It may include the history of the present illness (HPI), past medical history (PMH), and family/social history. There is usually also a review of systems (ROS), in which the provider asks questions about the function of each body system considered appropriate to the problem.

**COMPLIANCE GUIDELINE**

**Informed Consent**

If the plan of care involves significant risk, such as surgery, state laws require the provider to have the patient’s informed consent in advance. The provider discusses the assessment, risks, and recommendations with the patient and documents this conversation in the patient’s record. Usually, the patient signs either a chart entry or a consent form to indicate agreement.

The provider performs a physical examination and documents the diagnosis—the interpretation of the information that has been gathered—or the suspected problem if more tests or procedures are needed for a diagnosis. The treatment plan, or plan of care, is described. It includes the treatments and medications that the provider has ordered, specifying dosage and frequency of use.

**Other Chart Notes** Many other types of chart notes appear in patients’ medical records. Progress reports, as shown in Figure 2.2 below, document a patient’s progress and response to a treatment plan. They explain whether the plan should be continued or changed. Progress reports include:

- Comparisons of objective data with the patient’s statements
- Goals and progress toward the goals
- The patient’s current condition and prognosis
- Type of treatment still needed and for how long

**FIGURE 2.2 Progress Note in SOAP Format**

Medisoft Clinical
Discharge summaries are prepared during a patient’s final visit for a particular treatment plan or hospitalization. Discharge summaries include:

- The final diagnosis
- Comparisons of objective data with the patient’s statements
- Whether goals were achieved
- Reason for and date of discharge
- The patient’s current condition, status, and final prognosis
- Instructions given to the patient at discharge, noting any special needs such as restrictions on activities and medications

**Procedural Services Documentation**

Other common types of documentation are for specific procedures done either in the office or elsewhere:

- Procedure or operative reports for simple or complex surgery
- Reports for laboratory tests
- Radiology reports for the results of X-rays
- Forms for a specific purpose, such as immunization records, preemployment physicals, and disability reports

Figure 2.3 shows a follow-up order screen.
Using PM/EHRs: An Integrated Medical Documentation and Billing Cycle

The increased use of electronic health records in physician practices has changed office workflow. In a medical office, a flow of work that provides medical care to patients and collects payment for these services must be in place. When PM/EHRs are used, previous paper-based tasks, such as pulling file folders and making photocopies, are replaced by efficient electronic processes. The **medical documentation and billing cycle** explains how using EHRs is integrated with practice management programs as the ten-step billing process is performed. This cycle is illustrated in Figure 2.4. The inner circle represents the billing cycle, as explained in Chapter 1; the outer circle contains the medical documentation cycle.

As the illustration shows, the two cycles are interrelated. For example, a new patient phones for an appointment. During preregistration, both billing and clinical information must be collected during the phone call. From a billing perspective, the office wants to know whether the patient has insurance that will cover some or all of the cost of the visit, or whether the patient will pay for the visit. From a health or medical perspective, the staff wants to know the reason the person needs to see the doctor, known as the chief complaint.

![Medical Documentation and Billing Cycle](image-url)

**FIGURE 2.4** The Medical Documentation and Billing Cycle
Following the billing steps that establish financial responsibility and handle check-in, the professional medical staff gather clinical information. Often a medical assistant inputs vital signs, such as the patient’s temperature, pulse, respiration, blood pressure, height, and weight, in the EHR. The physician then documents the results of the physical examination, relevant history, and planned treatments.

As the medical documentation and billing cycle continues, so does the interaction between the two types of information. The physician or a medical coder assigns medical codes to the patient’s diagnosis and procedures, and the charges for those procedures are determined. Based on this information, the biller reviews coding and billing compliance and checks out the patient. When the biller then prepares and transmits claims, documentation may be studied to support medical necessity during claim creation and later during adjudication, if a payer requires it. During the steps of claim follow-up, patients’ statements and payment and collections are documented, and the process of managing and retaining patient data according to regulations is carried out.

Medical insurance specialists are knowledgeable about this PM/EHR cycle so that they can access the clinical information they need as they complete claims and provide documentation in support of their medical necessity.

THINKING IT THROUGH 2.1

1. Review the following letter that is in the patient medical record of John W. Wu.

Nicholas J. Kramer, MD
2200 Carriage Lane
Currituck, CT 07886
Consultation Report
on John W. Wu
(Birth date 12/06/1933)
Dear Dr. Kramer:
At your request, I saw Mr. Wu today. This is a seventy-seven-year-old male who stopped smoking cigarettes twenty years ago but continues to be a heavy pipe smoker. He has had several episodes of hemoptysis; a small amount of blood was produced along with some white phlegm. He denies any upper respiratory tract infection or symptoms on those occasions. He does not present with chronic cough, chest pain, or shortness of breath. I reviewed the chest X-ray done by you, which exhibits no acute process. His examination was normal.
A bronchoscopy was performed, which produced some evidence of laryngitis, tracheitis, and bronchitis, but no tumor was noted. Bronchial washings were negative.
I find that his bleeding is caused by chronic inflammation of his hypopharynx and bronchial tree, which is related to pipe smoking. There is no present evidence of malignancy.
Thank you for requesting this consultation.
Sincerely,
Mary Lakeland Georges, MD

A. What is the purpose of the letter?
B. How does it demonstrate the use of a patient medical record for continuity of care?

2. Consider the process of switching to EHRs from paper records in a practice having 2,000 patients. What are the pros and cons of moving all past patient records to the EHR at once versus doing so gradually?
2.2 Healthcare Regulation: HIPAA and HITECH

To protect consumers’ health, both federal and state governments pass laws that affect the medical services that must be offered to patients. To protect the privacy of patients’ health information, additional laws cover the way healthcare plans and providers exchange this information as they conduct business.

Federal Regulation

The main federal government agency responsible for healthcare is the Centers for Medicare and Medicaid Services, known as CMS (formerly the Health Care Financing Administration, or HCFA). An agency of the Department of Health and Human Services (HHS), CMS administers the Medicare and Medicaid programs to more than 90 million Americans. CMS implements annual federal budget acts and laws such as the Medicare Prescription Drug, Improvement, and Modernization Act that has created help in paying for drugs and for an annual physical examination for Medicare beneficiaries.

CMS also performs activities to ensure the quality of healthcare, such as:

▶ Regulating all laboratory testing other than research performed on humans
▶ Preventing discrimination based on health status for people buying health insurance
▶ Researching the effectiveness of various methods of healthcare management, treatment, and financing
▶ Evaluating the quality of healthcare facilities and services

CMS policy is often the model for the healthcare industry. When a change is made in Medicare rules, for example, private payers often adopt a similar rule.

State Regulation

States are also major regulators of the healthcare industry. Operating an insurance company without a license is illegal in all states. State commissioners of insurance investigate consumer complaints about the quality and financial aspects of healthcare. State laws ensure the solvency of insurance companies and managed care organizations, so that they will be able to pay enrollees’ claims. States may also restrict price increases on premiums and other charges to patients, require that policies include a guaranteed renewal provision, control the situations in which an insurer can cancel a patient’s coverage, and require coverage of certain diseases and preventive services.

HIPAA

The foundation legislation for the privacy of patients’ health information is called the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA contained five provisions called titles that focused on various aspects of healthcare:

Title I: Healthcare Access, Portability and Renewability
Title II: Preventing Healthcare Fraud and Abuse; Administrative Simplification
Title III: Tax-Related Health Provisions
Title IV: Application and Enforcement of Group Health Plan Requirements
Title V: Revenue Offsets

This law is designed to:

▶ Protect people’s private health information
▶ Ensure health insurance coverage for workers and their families when they change or lose their jobs
▶ Uncover fraud and abuse
▶ Create standards for electronic transmission of healthcare transactions
HITECH

The American Recovery and Reinvestment Act (ARRA) of 2009, also known as the Stimulus Package, contains additional provisions concerning the standards for electronic transmission of healthcare data. The most important rules are in the Health Information Technology for Economic and Clinical Health (HITECH) Act, which is Title XIII of ARRA. This law guides the use of federal stimulus money to promote the adoption and meaningful use of health information technology, mainly using electronic health records (EHRs). Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of HIPAA rules.

Meaningful Use

The portion of the HITECH Act that has received the most attention is the provision that provides financial incentives to physicians, hospitals, and other healthcare providers. Under the HITECH Act, physicians who adopt and use EHRs are eligible for payments of up to $44,000 from Medicare and Medicaid. Physicians who derive at least 30 percent or more of their income from Medicaid are eligible for up to $64,000, and doctors who practice in underserved areas are eligible for an extra 10 percent from Medicare.

To be eligible for the financial incentives, providers must do more than simply purchase EHRs; they must demonstrate meaningful use of the technology. Meaningful use is the utilization of certified EHR technology to improve quality, efficiency, and patient safety in the healthcare system. Incentives for achieving meaningful use are divided into three stages. The government has specified a series of objectives that determine whether meaningful use requirements have been met. In Stage 1 (2011–2012), these objectives consisted of a core set and a menu set. The objectives differ for physicians and hospitals. Physicians must meet fifteen core objectives and five of ten objectives from the menu set. The objectives for Stage 1 are listed in Table 2.2.

Stage 2 (expected to be implemented in 2013–2014) and Stage 3 (2015 or later) will expand on the objectives of Stage 1 with the addition of more mandatory clinical quality measures and requirements for improved patient outcomes.

Regional Extension Centers

Even with government financial incentives, successful implementation of EHRs is not expected to be quick or easy. Small practices, where most primary care is delivered, may lack the expertise and resources required to purchase, install, and use the new technology. Recognizing the challenges associated with implementing HIT, the HITECH Act called for the creation of regional extension centers (RECs). Patterned after the agriculture extension service the government created almost a century ago, the RECs offer information, guidance, training, and support services to primary care providers who are in the process of making the transition to an EHR system.

Health Information Exchange

To meet meaningful use criteria, providers must be able to exchange clinical information outside the organization. One of the ways that providers share information is through the use of local, state, and regional health information networks. A health information exchange (HIE) enables the sharing of health-related information among provider organizations according to nationally recognized standards. Examples of the use of an HIE include sharing patient records with physicians outside the physician’s own medical group, transmitting prescriptions to pharmacies, and ordering tests from an outside lab. The goal of an HIE is to facilitate access to clinical information for the purpose of providing quality care to patients. The National HIE Program, established by the HITECH Act, funds the development and maintenance of health information networks across the United States. 

Table 2.2: Objectives for Meaningful Use in Stage 1

<table>
<thead>
<tr>
<th>Core Objectives</th>
<th>Menu Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Exchange data</td>
<td>5. Access patient records</td>
</tr>
<tr>
<td>2. Electronic prescribing</td>
<td>6. Provide clinical decision support</td>
</tr>
<tr>
<td>3. Electronic problem lists</td>
<td>7. Implement computerized provider order entry</td>
</tr>
<tr>
<td>4. Electronic messaging</td>
<td>8. Implement and use clinical decision support systems</td>
</tr>
<tr>
<td>5. Use EHR for quality improvement</td>
<td>9. Implement and use clinical decision support systems</td>
</tr>
<tr>
<td>6. Use EHR for clinical coordination</td>
<td>10. Implement and use clinical decision support systems</td>
</tr>
</tbody>
</table>

Copyright © 2014 The McGraw-Hill Companies
Table 2.2  Meaningful Use Objectives

<table>
<thead>
<tr>
<th><strong>Core Set</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use computerized physician order entry for medications</td>
</tr>
<tr>
<td>Implement drug-drug and drug-allergy interaction checks</td>
</tr>
<tr>
<td>Generate and transmit permissible prescriptions electronically</td>
</tr>
<tr>
<td>Record patient demographics</td>
</tr>
<tr>
<td>Maintain up-to-date problem list of current and active diagnoses</td>
</tr>
<tr>
<td>Maintain active medication list and active medication allergy list</td>
</tr>
<tr>
<td>Record and chart vital signs</td>
</tr>
<tr>
<td>Record smoking status</td>
</tr>
<tr>
<td>Implement one clinical decision support rule and ability to track compliance with rule</td>
</tr>
<tr>
<td>Calculate and transmit Centers for Medicare &amp; Medicaid Services Quality Measure</td>
</tr>
<tr>
<td>Protect electronic copy of health information</td>
</tr>
<tr>
<td>Provide clinical summaries</td>
</tr>
<tr>
<td>Exchange key clinical information</td>
</tr>
<tr>
<td>Ensure privacy/security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Menu Set</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement drug formulary checks</td>
</tr>
<tr>
<td>Incorporate clinical laboratory test results into EHR system as structured data</td>
</tr>
<tr>
<td>Generate patient lists</td>
</tr>
<tr>
<td>Send patient reminders</td>
</tr>
<tr>
<td>Provide timely electronic access to health information</td>
</tr>
<tr>
<td>Identify patient-specific information</td>
</tr>
<tr>
<td>Perform medication reconciliation</td>
</tr>
<tr>
<td>Provide summary of care</td>
</tr>
<tr>
<td>Submit electronic immunization data to registries or information systems</td>
</tr>
<tr>
<td>Submit laboratory results to public health agencies</td>
</tr>
<tr>
<td>Submit electronic syndromic surveillance data to public health agencies</td>
</tr>
</tbody>
</table>

Health Information Network (NHIN) is a key component of the government’s HIT strategy that will provide a common platform for health information exchange across the country. The NHIN is currently in the trial stage.

ACA and Accountable Care Organizations

Under the ACA (see Chapter 1), incentives are offered to foster the formation and operation of accountable care organizations (ACOs). An ACO is a network of doctors and hospitals that shares responsibility for managing the quality and cost of care provided to a group of patients. A network could include primary care physicians, specialists, hospitals, home healthcare providers, and so on. By making this group of providers jointly accountable for the health of their patients, the program provides incentives to coordinate care in a way that improves quality and saves money by avoiding unnecessary tests and procedures.
2.3 Covered Entities and Business Associates

Patients’ medical records—the actual progress notes, reports, and other clinical materials—are legal documents that belong to the provider who created them. But the provider cannot withhold the information in the records unless providing it would be detrimental to the patient’s health. The information belongs to the patient.

Patients control the amount and type of information that is released, except for the use of the data to treat them or to conduct the normal business transactions of the practice. Only patients or their legally appointed representatives have the authority to authorize the release of information to anyone not directly involved in their care.

Medical insurance specialists handle issues such as requests for information from patients’ medical records. They need to know what information about patients’ conditions and treatments can be released. What information can be legally shared with other providers and health plans? What information must the patient specifically authorize to be released? The answers to these questions are based on HIPAA Administrative Simplification provisions and their expansion under HITECH.

Congress passed the Administrative Simplification provisions partly because of rising healthcare costs. A significant portion of every healthcare dollar is spent on administrative and financial tasks. These costs can be controlled if the business transactions of healthcare are standardized and handled electronically.

Electronic Data Interchange

The Administrative Simplification provisions encourage the use of electronic data interchange (EDI). EDI is the computer-to-computer exchange of routine business information using publicly available standards. Practice staff members use EDI to exchange health information about their practices’ patients with payers and clearing-houses. Each electronic exchange is a transaction, which is the electronic equivalent of a business document.

EDI transactions are not visible in the way that an exchange of paperwork, such as a letter, is. An example of a nonmedical transaction is the process of getting cash from an ATM. In an ATM transaction, the computer-to-computer exchange is made up of computer language that is sent and answered between the machines. This exchange happens behind the scenes. It is documented on the customer’s end with the transaction receipt that is printed; the bank also has a record at its location.
The Three Administrative Simplification Provisions

The three parts of the Administrative Simplification provisions are:

1. **HIPAA Privacy Rule**: The privacy requirements cover patients’ health information.
2. **HIPAA Security Rule**: The security requirements state the administrative, technical, and physical safeguards that are required to protect patients’ health information.
3. **HIPAA Electronic Transaction and Code Sets Standards**: These standards require every provider who does business electronically to use the same healthcare transactions, code sets, and identifiers.

Complying with HIPAA and HITECH

Healthcare organizations that are required by law to obey HIPAA regulations are called **covered entities (CEs)**. A covered entity is an organization that electronically transmits any information that is protected under HIPAA. Other organizations that work for the covered entities must also agree to follow HIPAA rules.

**Covered Entities**

Under HIPAA, three types of covered entities must follow the regulations:

- **Health plans**: The individual or group plan that provides or pays for medical care
- **Healthcare clearinghouses**: Companies that help providers handle such electronic transactions as submitting claims and that manage electronic medical record systems
- **Healthcare providers**: People or organizations that furnish, bill, or are paid for healthcare in the normal course of business

Many physician practices are included under HIPAA. Excepted providers are only those who do not send any claims (or other HIPAA transactions) electronically and do not employ any other firm to send electronic claims for them. Because CMS requires practices to send Medicare claims electronically unless they employ fewer than ten full-time or equivalent employees, practices have moved to electronic claims. Electronic claims have the advantage of being paid more quickly, too, so practices may use them even when they are not required.

**Business Associates**

Business Associates (BAs) are organizations that work for covered entities but are not themselves CEs. Examples of BAs include law firms; outside medical billers, coders, and transcriptionists; accountants; and collection agencies. Under the initial HIPAA law, BAs had to have agreements with the covered entities for which they worked to perform their work as required by HIPAA provisions, but they were not directly accountable to the federal government for doing so. Under the HITECH Act, though, BAs are as responsible as CEs for following HIPAA rules. HITECH also expands the types of organizations that are considered BAs to include vendors of personal health records (PHRs).

**Business Associate Contracts**

Contracts with BAs should specify how they are to comply with HIPAA/HITECH in handling the practice’s PHI.
2.4 HIPAA Privacy Rule

The HIPAA Standards for Privacy of Individually Identifiable Health Information rule is known as the **HIPAA Privacy Rule**. It was the first comprehensive federal protection for the privacy of health information. Its national standards protect individuals’ medical records and other personal health information. Before the HIPAA Privacy Rule became law, the personal information stored in hospitals, physicians’ practices, and health plans was governed by a patchwork of federal and state laws. Some state laws were strict, but others were not.

The Privacy Rule says that covered entities must:

- Have a set of privacy practices that are appropriate for its healthcare services
- Notify patients about their privacy rights and how their information can be used or disclosed
- Train employees so that they understand the privacy practices
- Appoint a privacy official responsible for seeing that the privacy practices are adopted and followed
- Safeguard patients’ records

**Protected Health Information**

The HIPAA Privacy Rule covers the use and disclosure of patients’ **protected health information (PHI)**. PHI is defined as individually identifiable health information that is transmitted or maintained by electronic media, such as over the Internet, by computer modem, or on magnetic tape or compact disks. This information includes a person’s:

- Name
- Address (including street address, city, county, ZIP code)
- Names of relatives and employers
- Birth date
- Telephone numbers
- Fax number
- E-mail address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Serial number of any vehicle or other device
- Website address
- Fingerprints or voiceprints
- Photographic images

**Use and Disclosure for Treatment, Payment, and Healthcare Operations**

Patients’ PHI under HIPAA can be used and disclosed by providers for treatment, payment, and healthcare operations. **Use of PHI** means sharing or analysis within the entity that holds the information. **Disclosure of PHI** means the release, transfer, provision of access to, or divulging of PHI outside the entity holding the information.

**HIPAA Privacy Rule** law regulating the use and disclosure of patients’ protected health information (PHI)

**45 CFR Parts 160 and 164**

The HIPAA Privacy Rule is also often referred to by its number in the Federal Register, which is 45 CFR Parts 160 and 164.

**HIPAA/HITECH Tip**

Privacy Officers

The privacy official at a small physician practice may be the office manager who also has other duties. At a large health plan, the position of privacy official may be full time.
Both use and disclosure of PHI are necessary and permitted for patients’ treatment, payment, and healthcare operations (TPO). Treatment means providing and coordinating the patient’s medical care; payment refers to the exchange of information with health plans; and healthcare operations are the general business management functions.

Minimum Necessary Standard  When using or disclosing protected health information, a covered entity must try to limit the information to the minimum amount of PHI necessary for the intended purpose. The minimum necessary standard means taking reasonable safeguards to protect PHI from incidental disclosure. Incidental use or disclosure is a secondary use of patient information that cannot reasonably be prevented, is limited, and usually occurs as the result of another, permitted use.

Examples of HIPAA Compliance

A medical insurance specialist does not disclose a patient’s history of cancer on a workers’ compensation claim for a sprained ankle. Only the information the recipient needs to know is given.

A physician’s assistant faxes appropriate patient cardiology test results before scheduled surgery.

A physician sends an e-mail message to another physician requesting a consultation on a patient’s case.

A patient’s family member picks up medical supplies and a prescription.

Designated Record Set  A covered entity must disclose individuals’ PHI to them (or to their personal representatives) when they request access to, or an accounting of disclosures of, their PHI. Patients’ rights apply to a designated record set (DRS). For a provider, the designated record set means the medical and billing records the provider maintains. It does not include appointment and surgery schedules, requests for lab tests, and birth and death records. It also does not include mental health information, psychotherapy notes, and genetic information. For a health plan, the designated record set includes enrollment, payment, claim decisions, and medical management systems of the plan.

Within the designated record set, patients have the right to:

► Access, copy, and inspect their PHI
► Request amendments to their health information
► Obtain accounting of most disclosures of their health information
► Receive communications from providers via other means, such as in Braille or in foreign languages
► Complain about alleged violations of the regulations and the provider’s own information policies

Notice of Privacy Practices  Covered entities must give each patient a notice of privacy practice at the first contact or encounter. To meet this requirement, physician practices give patients their Notice of Privacy Practices (NPP) (see Figure 2.5 on pages 51–53) and ask them to sign an acknowledgment that they have received it (see the chapter about patient encounters and billing information). The notice explains how patients’ PHI may be used and describes their rights.

Practices may choose to use a layered approach to giving patients the notice. On top of the information packet is a short notice, like the one shown in Figure 2.5, that briefly describes the uses and disclosures of PHI and the person’s rights. The longer notice is placed beneath it.

PHI and Accounting for Disclosures  Patients have the right to an accounting of disclosure of their PHI other than for TPO. When a patient’s PHI is accidentally disclosed, the disclosure should be documented in the individual’s medical record,
Chapter 2  ELECTRONIC HEALTH RECORDS, HIPAA, AND HITECH  51

Valley Associates, PC

NOTICE OF PRIVACY PRACTICES
THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND SHARED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

OUR PRIVACY OBLIGATIONS
The law requires us to maintain the privacy of certain health information called “Protected Health Information” (“PHI”), Protected Health Information is the information that you provide us or that we create or receive about your healthcare. The law also requires us to provide you with this Notice of our legal duties and privacy practices. When we use or disclose (share) your Protected Health Information, we are required to follow the terms of this Notice or other notice in effect at the time we use or share the PHI. Finally, the law provides you with certain rights described in this Notice.

WAYS WE CAN USE AND SHARE YOUR PHI WITHOUT YOUR WRITTEN PERMISSION (AUTHORIZATION)
In many situations, we can use and share your PHI for activities that are common in many offices and clinics. In certain other situations, which we will describe below, we must have your written permission (authorization) to use and share your PHI. We do not need any type of permission from you for the following uses and disclosures:

A. Uses and Disclosures for Treatment, Payment and Healthcare Operations
We may use and share your PHI to provide "Treatment," obtain "Payment" for your Treatment, and perform our "Healthcare Operations." These three terms are defined as:
 Treatment: We use and share your PHI to provide care and other services to you—for example, to diagnose and treat your injury or illness. In addition, we may contact you to provide appointment reminders or information about treatment options. We may tell you about other health-related benefits and services that might interest you. We may also share PHI with other doctors, nurses, and others involved in your care.
 Payment: We may use and share your PHI to receive payment for services that we provide to you. For example, we may share your PHI with the person who you told us is primarily responsible for paying for your Treatment, such as your spouse or parent.
 Healthcare Operations: We may use and share your PHI for our healthcare operations, which include management, planning, and activities that improve the quality and lower the cost of the care that we deliver. For example, we may use PHI to review the quality and skill of our physicians, nurses, and other healthcare providers.

B. Your Other Healthcare Providers
We may also share PHI with other healthcare providers when they need it to provide Treatment to you, to obtain Payment for the care they give to you, to perform certain Healthcare Operations, such as reviewing the quality and skill of healthcare professionals, or to review their actions in following the law.

C. Disclosure to Relatives, Close Friends and Your Other Caregivers
We may share your PHI with your family member/relative, a close personal friend, or another person who you identify if we
(1) First provide you with the chance to object to the disclosure and you do not object;
(2) Infer that you do not object to the disclosure; or
(3) Obtain your agreement to share your PHI with these individuals. If you are not present at the time we share your PHI, or you are not able to agree or disagree to our sharing your PHI because you are not capable or there is an emergency circumstance, we may use our professional judgment to decide that sharing the PHI is in your best interest. We may also use or share your PHI to notify (or assist in notifying) these individuals about your location and general condition.

D. Public Health Activities
We are required or are permitted by law to report PHI to certain government agencies and others. For example, we may share your PHI for the following:

FIGURE 2.5  Example of a Notice of Privacy Practices
(1) To report health information to public health authorities for the purpose of preventing or controlling
disease, injury, or disability;
(2) To report abuse and neglect to the state Department of Children and Family Services, the state
Department of Human Services, or other government authorities, including a social service or
protective services agency, that are legally permitted to receive the reports;
(3) To report information about products and services to the U.S. Food and Drug Administration;
(4) To alert a person who may have been exposed to a communicable disease or may otherwise be
at risk of developing or spreading a disease or condition;
(5) To report information to your employer as required under laws addressing work-related illnesses
and injuries or workplace medical surveillance; and
(6) To prevent or lessen a serious and imminent threat to a person for the public's health or safety, or
to certain government agencies with special functions such as the State Department.

E. Health Oversight Activities
We may share your PHI with a health oversight agency that oversees the healthcare system and
ensures the rules of government health programs, such as Medicare or Medicaid, are being followed.

F. Judicial and Administrative Proceedings
We may share your PHI in the course of a judicial or administrative proceeding in response to a legal
order or other lawful process.

G. Law Enforcement Purposes
We may share your PHI with the police or other law enforcement officials as required or permitted by
law or in compliance with a court order or a subpoena.

H. Decedents
We may share PHI with a coroner or medical examiner as authorized by law.

I. Organ and Tissue Procurement
We may share your PHI with organizations that facilitate organ, eye, or tissue procurement, banking,
or transplantation.

J. Research
We may use or share your PHI in related research processes.

K. Workers' Compensation
We may share your PHI as permitted by or required by state law relating to workers' compensation or
other similar programs.

L. As required by law
We may use and share your PHI when required to do so by any other law not already referred to
above.

USES AND DISCLOSURES REQUIRING YOUR WRITTEN PERMISSION (AUTHORIZATION)

A. Use or Disclosure with Your Permission (Authorization)
For any purpose other than the ones described above, we may only use or share your PHI when you
grant us your written permission (authorization). For example, you will need to give us your permission
before we send your PHI to your life insurance company.

B. Marketing
We must also obtain your written permission (authorization) prior to using your PHI to send you any
marketing materials. However, we may communicate with you about products or services related to
your Treatment, case management, or care coordination, or alternative treatments, therapies,
healthcare providers, or care settings without your permission. For example, we may not sell your PHI
without your written authorization.

C. Uses and Disclosures of Your Highly Confidential Information
Federal and state law requires special privacy protections for certain highly confidential information
about you ("Highly Confidential Information"), including any portion of your PHI that is:
(1) Kept in psychotherapy notes;
(2) About mental health and developmental disabilities services;
(3) About alcohol and drug abuse prevention, treatment and referral;
(4) About HIV/AIDS testing, diagnosis or treatment;
(5) About sexually transmitted disease(s);
(6) About genetic testing;

FIGURE 2.5 (Continued)
(7) About child abuse and neglect;
(8) About domestic abuse of an adult with a disability;
(9) About sexual assault; or
(10) In vitro Fertilization (IVF). Before we share your Highly Confidential Information for a purpose other than those permitted by law, we must obtain your written permission.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

A. For Further Information; Complaints

If you want more information about your privacy rights, are concerned that we have violated your privacy rights, or disagree with a decision that we made about access to your PHI, you may contact our Compliance Officer. You may also file written complaints with the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services. When you ask, the Compliance Officer will provide you with the correct address for the OCR. We will not take any action against you if you file a complaint with us or with the OCR.

B. Right to Receive Confidential Communications

You may ask us to send papers that contain your PHI to a different location than the address that you gave us, or in a special way. You will need to ask us in writing. We will try to grant your request if we feel it is reasonable. For example, you may ask us to send a copy of your medical records to a different address than your home address.

C. Right to Revoke Your Written Permission (Authorization)

You may change your mind about your authorization or any written permission regarding your PHI by giving or sending a written “revocation statement” to the Compliance Officer. The revocation will not apply to the extent that we have already taken action where we relied on your permission.

D. Right to Inspect and Copy Your Health Information

You may request access to your medical record file, billing records, and other records used to make decisions about your Treatment and payment for your Treatment. You can review these records and/or ask for copies. Under limited circumstances, we may deny you access to a portion of your records. If you want to access your records, you may obtain a record request form and return the completed form to the registration desk. If you request copies, we will charge you the amount listed on the rate sheet. We will also charge you for our postage costs, if you request that we mail the copies to you. For a copy of records, material, or information that cannot routinely be copied on a standard photocopy machine, such as x-ray films or pictures, we may charge for the reasonable cost of the copy.

E. Right to Amend Your Records

You have the right to request that we amend PHI maintained in medical record files, billing records, and other records used to make decisions about your Treatment and payment for your Treatment. If you want to amend your records, you may submit an amendment request form to the Compliance Officer. We will comply with your request unless we believe that the information that would be amended is correct and complete or that other circumstances apply. In the case of a requested amendment concerning information about the Treatment of a mental illness or developmental disability, you have the right to appeal to a state court our decision not to amend your PHI.

F. Right to Receive an Accounting of Disclosures

You may ask for an accounting of certain disclosures of your PHI made by us on or after April 14, 2003. These disclosures must have occurred before the time of your request, and we will not go back more than six (6) years before the date of your request. If you request an accounting more than once during a twelve (12) month period, we will charge you based on the rate sheet. Direct your request for an accounting to the Compliance Officer.

G. Right to Request Restrictions

You have the right to ask us to restrict or limit the PHI we use or disclose about you for treatment, payment, or healthcare operations. With one exception, we are not required to agree to your request. If we do agree, we will comply unless the information is needed to provide emergency treatment. Your request for restrictions must be made in writing and submitted to the Compliance Officer. We must grant your request to a restriction on disclosure of your PHI to a health plan if you have paid for the healthcare item in full out of pocket.

H. Right to Receive Paper Copy of this Notice

If you ask, you may obtain a paper copy of this Notice, even if you have agreed to receive the notice electronically.

You may contact the compliance officer at:
Valley Associates, PC
ATTN: Compliance Officer
1400 West Center Street
Toledo, OH 43601-0123
555-321-0987

Questions and Answers on HIPAA Privacy Policies
www.hhs.gov/ocr/privacy

HIPAA/HITECH TIP

PHI and Medical Office Staff

Be careful not to discuss patients’ cases with anyone outside the office, including family and friends. Avoid talking about cases, too, in the practice’s reception areas where other patients might hear. Close charts on desks when they are not being worked on. Position computer screens so that only the person working with a file can view it.
because the individual did not authorize it and it was not a permitted disclosure. An example is faxing a discharge summary to the wrong physician’s office.

Also, under HITECH, patients can request an accounting of all disclosures—not just those other than for TPO—for the past three years if their PHI is stored in an EHR.

**Authorizations for Other Use and Disclosure**

For use or disclosure other than for TPO, the covered entity must have the patient sign an **authorization** to release the information. Information about substance (alcohol and drug) abuse, sexually transmitted diseases (STDs) or human immunodeficiency virus (HIV), and behavioral/mental health services may not be released without a specific authorization from the patient. The authorization document must be in plain language and include the following:

- A description of the information to be used or disclosed
- The name or other specific identification of the person(s) authorized to use or disclose the information
- The name of the person(s) or group of people to whom the covered entity may make the use or disclosure
- A description of each purpose of the requested use or disclosure
- An expiration date
- The signature of the individual (or authorized representative) and the date

In addition, the rule states that a valid authorization must include:

- A statement of the individual’s right to revoke the authorization in writing
- A statement about whether the covered entity is able to base treatment, payment, enrollment, or eligibility for benefits on the authorization
- A statement that information used or disclosed after the authorization may be disclosed again by the recipient and may no longer be protected by the rule

A sample authorization form is shown in Figure 2.6.

Uses or disclosures for which the covered entity has received specific authorization from the patient do not have to follow the minimum necessary standard. Incidental use and disclosure are also allowed. For example, the practice may use reception-area sign-in sheets.

**Exceptions**

There are a number of exceptions to the usual rules for release:

- Court orders
- Workers’ compensation cases
- Statutory reports
- Research
- Self-pay requests for restrictions

All these types of disclosures must be logged, and the release information must be available to the patient who requests it.

**Release Under Court Order** If the patient’s PHI is required as evidence by a court of law, the provider may release it without the patient’s approval if a judicial order is received. In the case of a lawsuit, a court sometimes decides that a physician or medical practice staff member must provide testimony. The court issues a *subpoena*, an order of the court directing a party to appear and testify. If the court requires the witness to bring certain evidence, such as a patient medical record, it issues a *subpoena duces tecum*, which directs the party to appear, to testify, and to bring specified documents or items.

**Workers’ Compensation Cases** State law may provide for release of records to employers in workers’ compensation cases (see the chapter about workers’ compensation.) The law may also authorize release to the state workers’ compensation administration board and to the insurance company that handles these claims for the state.
FIGURE 2.6 Example of an Authorization to Use or Disclose Health Information
Statutory Reports  Some specific types of information are required by state law to be released to state health or social services departments. For example, physicians must make statutory reports for patients’ births and deaths and for cases of abuse. Because of the danger of harm to patients or others, communicable diseases such as tuberculosis, hepatitis, and rabies must usually be reported.

A special category of communicable disease control is applied to patients with diagnoses of human immunodeficiency virus (HIV) infection and acquired immunodeficiency syndrome (AIDS). Every state requires AIDS cases to be reported. Most states also require reporting of the HIV infection that causes the syndrome. However, state law varies concerning whether just the fact of a case is to be reported or if the patient’s name must also be reported. The practice guidelines reflect the state laws and must be strictly observed, as all these regulations should be, to protect patients’ privacy and to comply with the regulations.

Research Data  PHI may be made available to researchers approved by the practice. For example, if a physician is conducting clinical research on a type of diabetes, the practice may share information from appropriate records for analysis. When the researcher issues reports or studies based on the information, specific patients’ names may not be identified.

Self-Pay Requests for Restrictions  Under HITECH, patients can restrict the access of health plans to their medical records if they pay for the service in full at the time of the visit.

De-Identified Health Information  There are no restrictions on the use or disclosure of de-identified health information that neither identifies nor provides a reasonable basis to identify an individual. For example, these identifiers must be removed: names, medical record numbers, health plan beneficiary numbers, device identifiers (such as pacemakers), and biometric identifiers, such as fingerprints and voiceprints.

Psychotherapy Notes  Psychotherapy notes have special protection under HIPAA. According to the American Health Information Management Association Practice Brief on Legal Process and Electronic Health Records,

Under the HIPAA Privacy Rule, psychotherapy notes are those recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the content of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record. Notes exclude medication prescription and monitoring, counseling session start or stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. The privacy rule gives such notes extra protection as may state law. (Available online at www.ahima.org/resources/ehr.aspx)

State Statutes  Some state statutes are more stringent than HIPAA specifications. Areas in which state statutes may differ from HIPAA include the following:

- Designated record set
- Psychotherapy notes
- Rights of inmates
- Information compiled for civil, criminal, or administrative court cases

Each practice’s privacy official reviews state laws and develops policies and procedures for compliance with the HIPAA Privacy Rule. The tougher rules are implemented.
2.5 HIPAA Security Rule

The HIPAA Security Rule requires covered entities to establish safeguards to protect PHI. The security rule specifies how to secure such protected health information on computer networks, the Internet, and storage disks such as CDs.

Encryption Is Required

Information security is needed when computers exchange data over the Internet. Security measures rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it. Practice management programs (PMPs) encrypt data traveling between the office and the Internet, such as patients’ Social Security numbers, so that the information is secure.

Security Measures

A number of other security measures help enforce the HIPAA Security Rule. These include:

▶ Secure Internet connections
▶ Access control, passwords, and log files to keep intruders out
▶ Backups to replace items after damage
▶ Security policies to handle violations that do occur

Access Control, Passwords, and Log Files

Most practices use role-based access, meaning that only people who need information can see it. Once access rights have been assigned, each user is given a key to the designated databases. Users must enter a user ID and a password (the key) to see files to which they have been granted access rights.

For example, receptionists may view the names of patients coming to the office on one day, but they should not see those patients’ medical records. However, the nurse or physician needs to view the patient records. Receptionists are given individual computer passwords that let them view the day’s schedule but that deny entry to patient records. The physicians and nurses possess computer passwords that allow them to see all patient records.

The PMP also creates activity logs of who has accessed—or tried to access—information, and passwords prevent unauthorized users from gaining access to information on a computer or network.

Figure 2.7 on page 58 shows how a practice management program is used to set up security. Each person who will be using the program is given a log-in name and has a password. The person has also been assigned an access level based on the information he or she needs to use, as shown in the Security Setup screen. The Security Warning screen illustrates the PMP’s access denial message.

THINKING IT THROUGH 2.4

Based on the information in Figure 2.5 on pages 51–53:

1. Is permission needed to share a patient’s PHI with his or her life insurance company?
2. Is written authorization from a patient needed to use or disclose health information in an emergency?
3. What is the purpose of an “accounting of disclosures”?

HIPAA Security Rule

law requiring covered entities to establish safeguards to protect health information

encryption method of converting a message into encoded text

password confidential authentication information

HIPAA/HITECH TIP

The Association for Integrity of Healthcare Documentation (formerly the American Association for Medical Transcription) advises against using a patient’s name in the body of a medical report. Instead, place identification information only in the demographic section, where it can be easily deleted when the report data are needed for research.

BILLING TIP

Internet Security Symbol

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

COMPLIANCE GUIDELINE

Don’t Share!

Never share your log-in or passwords. Sharing makes you responsible if someone else access and breaches HIPAA information with your identification.

Copyright © 2014 The McGraw-Hill Companies
Internet Security

Information is exchanged over the Internet between the practice and those outside of the office a number of ways, especially by e-mail, the most important business communication method. Additionally, practices may have their own websites and patient portals for access to the physicians and for marketing purposes; take calls from patients’ mobile phones; and send medical records to health plans via attachments. HIPAA, HITECH, and many states have laws for data security that require the use of antivirus software programs and encrypting confidential patient data that are transmitted.

Backups

Backing up is the activity of copying files to another medium so that they will be preserved in case the originals are no longer available. A successful backup plan is critical in recovering from either a minor or major security incident that jeopardizes critical data. To be secure, backups must also be encrypted.

THINKING IT THROUGH 2.5

1. Imagine that you are employed as a medical insurance specialist for Family Medical Center. Make up a password that you will use to keep your files secure.

2. As an employee, how would you respond to another staff member who asked to see your latest claim files in order to see how you handled a particular situation?

Security Policy

Practices have security policies that inform employees about their responsibilities for protecting electronically stored information. Many practices include this information in handbooks distributed to all employees. These handbooks contain general information about the organizations, their structures, and their policies as well as specific information about employee responsibilities.

2.6 HITECH Breach Notification Rule

The HITECH Act requires covered entities to notify affected individuals following the discovery of a breach of unsecured health information. A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI and that could pose a significant risk of financial, reputational, or...
other harm to the affected person. Covered entities are required to monitor their handling of PHI to be sure to discover breaches, and if a breach occurs, to follow breach notification procedures.

**Guidance on Securing PHI**

The HITECH Act refers to *unsecured PHI* as unprotected health information that is not secured through the use of technologies or methods that HHS has specified. These methods involve either encrypting or destroying the data. If PHI has not been secured through one or more of these methods and there is a breach, covered entities are required to follow the provision’s breach notification procedures.

Although covered entities do not have to follow the guidance on acceptable methods, if the encryption and destruction methods specified are used to secure data, covered entities may be exempt from the breach notification requirements for breaches of that data. In addition, the rule notes several exceptions to the definition of “breach,” including certain good faith uses and disclosures among a company’s workforce members, as long as the private information is not further acquired, accessed, used, or disclosed without authorization.

**Breach Notification Procedures**

Following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed in the breach. Additionally, following the discovery of a breach by a business associate, the business associate must notify the covered entity of the breach and identify for the covered entity the individuals whose unsecured PHI has been, or is reasonably believed to have been, breached. The act requires the notifications to be made without unreasonable delay but in no case later than 60 calendar days after discovery of the breach. An exception may be made to the 60-calendar-day deadline only in a situation in which a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security.

HITECH specifies the following:

- Notice to patients of breaches “without reasonable delay” within 60 days
- Notice to covered entities by business associates (BAs) when BAs discover a breach
- Notice to “prominent media outlets” on breaches involving more than 500 individuals
- Notice to “next of kin” on breaches involving patients who are deceased
- Notice to the secretary of HHS about breaches involving 500 or more individuals without reasonable delay
- Annual notice to the secretary of HHS about breaches of “unsecured PHI” involving less than 500 individuals that pose a significant financial risk or other harm to the individual, such as reputation

The document notifying an individual of a breach, called the *breach notification*, must include the following points: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code); (3) the steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which include a toll-free telephone number, an e-mail address, website, or postal address.

In addition, as part of the rule, the secretary of HHS must annually prepare and submit to Congress a report regarding the breaches for which the
secretary was notified and all enforcement actions taken. This means that covered entities must maintain a log of breaches involving fewer than 500 individuals, which they submit annually to HHS. HHS must post the report on the HHS public website. It is hoped that the negative publicity of the public posting will act as a deterrent, offering greater incentive for covered entities and business associates to prevent breaches.

### Case: Breach Notification

Some 1.7 million individuals are being notified of a health information breach incident involving data from The New York City Health and Hospitals Corp. It is the largest breach reported so far under the HITECH Act breach notification rule, which went into effect in September 2009.

Computer backup tapes from the New York provider were stolen on December 23, 2010, from a truck that was transporting them to a secure storage location, according to a website statement from the NYC organization and its letter to those affected. The unencrypted tapes included information on patients and hospital staff. Also on the tapes was information the hospitals’ occupational health services collected about employees of vendors and contractors.

The information lost, which was collected during the past 20 years, includes: names, addresses, Social Security numbers, patient medical histories and the occupational/employee health information of staff, vendors, contractors and others, according to the statement.

All those affected are being offered one year of free credit protection services.

### THINKING IT THROUGH 2.6

1. The breach notification rule states “if there is no significant risk of harm to the individual, then no breach has occurred, and no notification is required.” If PHI from a medical office is inadvertently disclosed to the wrong business associate (for instance, if a list of patients with overdue account information is sent to the wrong medical billing vendor), and the vendor informs you of the mistake, in your opinion has a breach occurred?

2. Review the HITECH specifications above regarding breaches and business associates. If a business associate causes a breach, who is responsible for notifying the individuals affected?

### 2.7 HIPAA Electronic Health Care Transactions and Code Sets

The HIPAA Electronic Health Care Transactions and Code Sets (TCS) standards make it possible for physicians and health plans to exchange electronic data using a standard format and standard code sets.
Standard Transactions

The HIPAA transactions standards apply to the electronic data that are regularly sent back and forth between providers, health plans, and employers. Each standard is labeled with both a number and a name. Either the number (such as “the 837”) or the name (such as the “HIPAA Claim”) may be used to refer to the particular electronic document format.

<table>
<thead>
<tr>
<th>Number</th>
<th>Official Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>X12 837</td>
<td>Healthcare Claims or Equivalent Encounter Information/Coordination of Benefits—coordination of benefits refers to an exchange of information between payers when a patient has more than one health plan</td>
</tr>
<tr>
<td>X12 276/277</td>
<td>Healthcare Claim Status Inquiry/Response</td>
</tr>
<tr>
<td>X12 270/271</td>
<td>Eligibility for a Health Plan Inquiry/Response</td>
</tr>
<tr>
<td>X12 278</td>
<td>Referral Certification and Authorization</td>
</tr>
<tr>
<td>X12 835</td>
<td>Healthcare Payment and Remittance Advice</td>
</tr>
<tr>
<td>X12 820</td>
<td>Health Plan Premium Payments</td>
</tr>
<tr>
<td>X12 834</td>
<td>Health Plan Enrollment and Disenrollment</td>
</tr>
</tbody>
</table>

Medical insurance specialists use the first five transactions in performing their jobs. Each of these is covered in later text chapters.

Operating Rules

The ACA requires the adoption of operating rules for each of the HIPAA standard transactions. The operating rules improve interoperability between the data systems of different entities, such as health plans and providers, and so increase their usefulness. They define the rights and responsibilities of those who are conducting the transactions, setting forth the security requirements, EDI transmission formats, response times, and error resolution.

Standard Code Sets

Under HIPAA, a code set is any group of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, or medical procedure codes. Medical code sets used in the healthcare industry include coding systems for diseases; treatments and procedures; and supplies or other items used to perform these actions. These standards, listed in Table 2.3, are covered in later text chapters.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes for diseases, injuries, impairments, and other health-related problems</td>
<td>Before October 1, 2014: International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), Volumes 1 and 2 After October 1, 2014: International Classification of Diseases, 10th Revision, Clinical Modification</td>
</tr>
<tr>
<td>Codes for dental services</td>
<td>Current Dental Terminology (CDT-4)</td>
</tr>
<tr>
<td>Codes for other medical services</td>
<td>Healthcare Common Procedures Coding System (HCPCS)</td>
</tr>
</tbody>
</table>
HIPAA National Identifiers

HIPAA National Identifiers are for:

- Employers
- Healthcare providers
- Health plans
- Patients

Identifiers are numbers of predetermined length and structure, such as a person’s Social Security number. They are important because the unique numbers can be used in electronic transactions. These unique numbers can replace the many numbers that are currently used. Two identifiers have been set up, and two—health plans and patients—are to be established in the future.

Employer Identification Number (EIN)

The employer identifier is used when employers enroll or disenroll employees in a health plan (X12 834) or make premium payments to plans on behalf of their employees (X12 820). The Employer Identification Number (EIN; also called the tax identification number) issued by the Internal Revenue Service is the HIPAA standard.

National Provider Identifier (NPI)

The National Provider Identifier (NPI) is the standard for the identification of providers when filing claims and other transactions. The NPI has replaced other identifying numbers that had been used, such as the UPIN for Medicare and the numbers that have been assigned by each payer to the provider. The older numbers are known as legacy numbers.

The NPI has nine numbers and a check digit, for a total of ten numbers. The federal government assigns the numbers to individual providers, such as physicians and nurses, and to provider organizations such as hospitals, pharmacies, and clinics. CMS maintains the NPIs as they are assigned in the National Plan and Provider Enumerator System (NPPES), a database of all assigned numbers. Once assigned, the NPI will not change; it remains with the provider regardless of job or location changes.

All healthcare providers who transmit health information electronically must obtain NPIs, even if they use business associates to prepare the transactions. Most health plans, including Medicare, Medicaid, and private payers, and all clearinghouses must accept and use NPIs in HIPAA transactions. This includes small health plans as well.

BILLING TIP

Physician and Group NPIs

If a physician is in a group practice, both the individual doctor and the group have NPIs.

THINKING IT THROUGH 2.7

1. Gloria Traylor, an employee of National Bank, called Marilyn Rennagel, a medical insurance specialist who works for Dr. Judy Fisk. The bank is considering hiring one of Dr. Fisk’s patients, Juan Ramirez, and Ms. Traylor would like to know if he has any known medical problems. Marilyn, in a hurry to complete the call and get back to work on this week’s claims, quickly explains that she remembers that Mr. Ramirez was treated for depression some years ago, but that he has been fine since that time. She adds that she thinks he would make an excellent employee.

A. In your opinion, did Marilyn handle this call correctly?
B. What problems might result from her answers?

COMPLIANCE GUIDELINE

HPID

A ten-digit “health plan identifier” is assigned to covered entities such as health plans.

BILLING TIP

A ten-digit “health plan identifier” is assigned to entities that are not required to have NPIs but need to be identified in the standard transactions, such as third-party administrators who work for health plans.
2.8 Fraud and Abuse Regulations

Almost everyone involved in the delivery of healthcare is trustworthy and is devoted to patients’ welfare. However, some people are not. Healthcare fraud and abuse laws help control cheating in the healthcare system. Is this really necessary? The evidence says that it is. During 2011, the federal government recovered an estimated $4.1 billion in fraud-related judgments and settlements. The National Health Care Anti-Fraud Association has projected that of the estimated $2 trillion spent on healthcare every year, at least 3 percent—or $50 billion—is lost to fraud.

The Health Care Fraud and Abuse Control Program

HIPAA’s Title II required the **Health Care Fraud and Abuse Control Program** to uncover and prosecute fraud and abuse. The HHS **Office of the Inspector General (OIG)** has the task of detecting healthcare fraud and abuse and enforcing all laws relating to them. OIG works with the U.S. Department of Justice (DOJ), which includes the Federal Bureau of Investigation (FBI), under the direction of the U.S. attorney general to prosecute those suspected of medical fraud and abuse.

**False Claims Act, Fraud Enforcement and Recovery Act, and State Laws**

The federal False Claims Act (FCA) (31 USC § 3729), a related law, prohibits submitting a fraudulent claim or making a false statement or representation in connection with a claim. It also encourages reporting suspected fraud and abuse against the government by protecting and rewarding people involved in *qui tam*, or whistle-blower, cases. The person who makes the accusation of suspected fraud is called the **relator**. Under the law, the relator is protected against employer retaliation. If the lawsuit results in a fine paid to the federal government, the whistle-blower may be entitled to 15 to 25 percent of the amount paid. People who blow the whistle are current or former employees of insurance companies or medical practices, program beneficiaries, and independent contractors.

The federal **Fraud Enforcement and Recovery Act (FERA)** of 2009 strengthens the provisions of the FCA. Also enforced by DOJ, FERA extends whistle-blower protection to agents and contractors of an employer, as well as to employees. It also makes it illegal to knowingly keep an overpayment received from the government. (Handling such overpayments correctly is covered in the chapter about payments, appeals, and secondary claims.)

The 2010 Affordable Care Act further strengthened the tools that DOJ and HHS have to pursue fraud investigations. The act provides additional funding so that providers can be subject to fingerprinting, site visits, and criminal background checks before they are allowed to bill the Medicare and Medicaid programs.

Nearly half of the states also have passed versions of the federal False Claims Act. These laws allow private individuals to bring an action alone or by working with the state attorney general against any person who knowingly causes the state to pay a false claim. These laws generally provide for civil penalties and damages related to the cost of any losses sustained because of the false claim.

**Additional Laws**

Additional laws relating to healthcare fraud and abuse control include:

- An antikickback statute that makes it illegal to knowingly offer incentives to induce referrals for services that are paid by government healthcare programs. Many financial actions are considered to be incentives, including illegal direct payments to other physicians and routine waivers of coinsurance and deductibles.
Self-referral prohibitions (called Stark rules) that make it illegal for physicians (or members of their immediate families) to have financial relationships with clinics to which they refer their patients, such as radiology service clinics and clinical laboratory services. (Note, however, that there are many legal exceptions to this prohibition under various business structures.)

The Sarbanes-Oxley Act of 2002 that requires publicly traded corporations to attest that their financial management is sound. These provisions apply to for-profit healthcare companies. The act includes whistle-blower protection so that employees can report wrongdoing without fear of retaliation.

Definition of Fraud and Abuse

**Fraud** is an intentional act of deception used to take advantage of another person. For example, misrepresenting professional credentials and forging another person's signature on a check are fraudulent. Pretending to be a physician and treating patients without a valid medical license is also fraudulent. Fraudulent acts are intentional; the individual expects an illegal or unauthorized benefit to result.

Claims fraud occurs when healthcare providers or others falsely report charges to payers. A provider may bill for services that were not performed, overcharge for services, or fail to provide complete services under a contract. A patient may exaggerate an injury to get a settlement from an insurance company or may ask a medical insurance specialist to change a date on a chart so that a service is covered by a health plan.

**Fraud Versus Abuse**

To bill when the task was not done is fraud; to bill when it was not necessary is abuse. Remember the rule: If a service was not documented, in the view of the payer it was not done and cannot be billed. To bill for undocumented services is fraudulent.

**Case**

Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona, has agreed to pay the U.S. Department of Health and Human Services (HHS) a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the protected health information of its patients.

The settlement with the physician practice follows an extensive investigation by the HHS Office for Civil Rights (OCR) for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

The incident giving rise to OCR’s investigation was a report that the physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible. On further investigation, OCR found that Phoenix Cardiac Surgery had implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules and had limited safeguards in place to protect patients’ electronic protected health information (ePHI).

“This case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules,” said Leon Rodriguez, director of OCR. “We hope that healthcare providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules demand higher levels of protection for patient health information.”

Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity.”
OCR’s investigation also revealed the following issues:
▶ Phoenix Cardiac Surgery failed to implement adequate policies and procedures to appropriately safeguard patient information;
▶ Phoenix Cardiac Surgery failed to document that it trained any employees on its policies and procedures on the Privacy and Security Rules;
▶ Phoenix Cardiac Surgery failed to identify a security official and conduct a risk analysis; and
▶ Phoenix Cardiac Surgery failed to obtain business associate agreements with Internet-based e-mail and calendar services where the provision of the service included storage of and access to its ePHI.
Under the HHS resolution agreement, Phoenix Cardiac Surgery has agreed to pay a $100,000 settlement amount and a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules.

In federal law, abuse means an action that misuses money that the government has allocated, such as Medicare funds. Abuse is illegal because taxpayers’ dollars are misspent. An example of abuse is an ambulance service that billed Medicare for transporting a patient to the hospital when the patient did not need ambulance service. This abuse—billing for services that were not medically necessary—resulted in improper payment for the ambulance company. Abuse is not necessarily intentional. It may be the result of ignorance of a billing rule or of inaccurate coding.

**Examples of Fraudulent or Abusive Acts**
A number of billing practices are fraudulent or abusive. Investigators reviewing physicians’ billing work look for patterns like these:
▶ Intentionally billing for services that were not performed or documented
  *Example* A lab bills Medicare for two tests when only one was done.
  *Example* A physician asks a coder to report a physical examination that was just a telephone conversation.
▶ Reporting services at a higher level than was carried out
  *Example* After a visit for a flu shot, the provider bills the encounter as a comprehensive physical examination plus a vaccination.
▶ Performing and billing for procedures that are not related to the patient’s condition and therefore not medically necessary
  *Example* After reading an article about Lyme disease, a patient is worried about having worked in her garden over the summer, and she requests a Lyme disease diagnostic test. Although no symptoms or signs have been reported, the physician orders and bills for the *Borrelia burgdorferi* (Lyme disease) confirmatory immunoblot test.
Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, Leon Rodriguez, Director of the HHS Office for Civil Rights (OCR), announced. BCBST has also agreed to a corrective action plan to address gaps in its HIPAA compliance program. The enforcement action is the first resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule.

The investigation followed a notice submitted by BCBST to HHS reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the protected health information (PHI) of over 1 million individuals, including member names, Social Security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR’s investigation indicated BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

“This settlement sends an important message that OCR expects health plans and healthcare providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program,” said OCR Director Leon Rodriguez. “The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients’ right to private and secure health information.”

In addition to the $1,500,000 settlement, the agreement requires BCBST to review, revise, and maintain its Privacy and Security policies and procedures, to conduct regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA, and to perform monitor reviews to ensure BCBST compliance with the corrective action plan.

THINKING IT THROUGH 2.8

1. Discuss the difference between fraud and abuse. Which is likely to create the most severe punishment?

2.9 Enforcement and Penalties

The HIPAA final enforcement rule became law and was required to be implemented on March 16, 2006. Its purpose is to reconcile differences in enforcement procedures that had existed between the privacy and the security standards by imposing a single rule. It makes clear that both acts—things that are done—and omissions—things that are not done, like failure to implement a particular provision—may be HIPAA
violations. Enforcing HIPAA is the job of a number of government agencies. Which agency performs which task depends on the nature of the violation and is determined by the HIPAA Enforcement rule.

**Office for Civil Rights**

Civil violations (those that are based on civil law, such as trespassing, divorce cases, and breach of contract proceedings) of the HIPAA privacy and security standards are enforced by the Office for Civil Rights (OCR), an agency of HHS. OCR has the authority to receive and investigate complaints as well as to issue subpoenas for evidence in cases it is investigating. It is charged with enforcing the privacy standards because privacy and security of one's health information are considered a civil right. It is important to note, though, that individuals themselves do not have the right to sue a covered entity that may have disclosed their PHI inappropriately; OCR must take action on individuals’ behalf.

**Department of Justice**

Criminal violations (those that involve crimes, such as kidnapping, robbery, and arson) of HIPAA privacy standards are prosecuted by the federal government’s Department of Justice (DOJ). DOJ is America’s “law office” and central agency for enforcement of federal laws.

**Office of E-Health Standards and Services**

The other standards are enforced by the Office of E-Health Standards and Services (OESS), part of CMS. In addition to its major task of administering the Medicare and Medicaid programs, HHS has also authorized CMS to investigate complaints of noncompliance and enforce these HIPAA standards:

- The Electronic Health Care Transaction and Code Set Rule (TCS)
- The National Employer Identifier Number (EIN) Rule
- The National Provider Identifier Rule

**Office of Inspector General**

OIG was directed by the original HIPAA law to combat fraud and abuse in health insurance and healthcare delivery.

Most billing-related accusations under the False Claims Act are based on the guideline that providers who knew or should have known that a claim for service was false can be held liable. The intent to commit fraud does not have to be proved by the accuser in order for the provider to be found guilty. Actions that might be viewed as errors or occasional slips might also be seen as establishing a pattern of violations, which constitute the knowledge meant by “providers knew or should have known.”

OIG has the authority to investigate suspected fraud cases and to audit the records of physicians and payers. In an audit, which is a methodical examination, investigators review selected medical records to see if the documentation matches the billing. The accounting records are often reviewed as well. When problems are found, the investigation proceeds and may result in charges of fraud or abuse against the practice.

Although OIG says that “under the law, physicians are not subject to civil, administrative, or criminal penalties for innocent errors, or even negligence,” decisions about whether there are clear patterns and inadequate internal procedures can be subjective at times, making the line between honest mistakes and fraud very thin. Medical practice staff members must avoid any actions that could be perceived as noncompliant.
Civil and Criminal Money Penalties

Most privacy complaints have been settled by voluntary compliance. But if the covered entity does not act to resolve the matter in a way that is satisfactory, the enforcing agency can impose civil money penalties (CMPs). HITECH has a tiered system for deciding the level and penalty of each privacy violation. CMS and OCR can supersede these limits, but with a cap of $50,000 per violation and $1.5 million for the calendar year for the same type of violation.

If OCR or CMS receives a complaint that may lead to a criminal case, the agency will usually refer the complaint to DOJ for investigation. For criminal cases, such as for selling unique health identifiers for identity theft purposes, these criminal penalties can be imposed:

<table>
<thead>
<tr>
<th>Offense</th>
<th>Fine</th>
<th>Prison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowingly obtaining PHI in violation of HIPAA</td>
<td>$50,000</td>
<td>1 year</td>
</tr>
<tr>
<td>Offenses done under false pretenses</td>
<td>$100,000</td>
<td>5 years</td>
</tr>
<tr>
<td>Using PHI for profit, gain, or harm</td>
<td>$250,000</td>
<td>10 years</td>
</tr>
</tbody>
</table>

Ongoing Compliance Education

As explained in the next section, medical office staff members receive ongoing training and education in current rules, so that they can avoid even the appearance of fraud.

COMPLIANCE GUIDELINE

A Changing Mandate

Because of ACA provisions, mandated—rather than voluntary—compliance plans are soon to be the law.

THINKING IT THROUGH 2.9

1. Mary Kelley, a patient of the Good Health Clinic, asked Kathleen Culpepper, the medical insurance specialist, to help her out of a tough financial spot. Her medical insurance authorized her to receive four radiation treatments for her condition, one every thirty-five days. Because she was out of town, she did not schedule her appointment for the last treatment until today, which is one week beyond the approved period. The insurance company will not reimburse Mary for this procedure. She asks Kathleen to change the date on the record to last Wednesday so that it will be covered, explaining that no one will be hurt by this change and, anyway, she pays the insurance company plenty.

A. What type of action is Mary asking Kathleen to do?

B. How should Kathleen handle Mary’s request?

2.10 Compliance Plans

Because of the risk of fraud and abuse liability, medical practices must be sure that billing rules are followed by all staff members. In addition to responsibility for their own actions, physicians are liable for the professional actions of employees they supervise. This responsibility is a result of the law of respondeat superior, which states that an employer is responsible for an employee’s actions. Physicians are held to this doctrine, so they can be charged for the fraudulent behavior of any staff member.

A wise slogan is that “the best defense is a good offense.” For this reason, medical practices write and implement compliance plans to uncover compliance problems and correct them to avoid risking liability. A compliance plan is a process for finding, correcting, and preventing illegal medical office practices. It is a written document prepared by a compliance officer and committee that sets up the steps needed to (1) audit and monitor compliance with government regulations, especially in the area of coding and billing, (2) have policies and procedures that are consistent, (3) provide for ongoing staff training and communication, and (4) respond to and correct errors.

The goals of the compliance plan are to:

▶ Prevent fraud and abuse through a formal process to identify, investigate, fix, and prevent repeat violations relating to reimbursement for healthcare services
▶ Ensure compliance with applicable federal, state, and local laws, including employment and environmental laws as well as antifraud laws
Help defend the practice if it is investigated or prosecuted for fraud by substantiating the desire to behave compliantly and thus reduce any fines or criminal prosecution.

Having a compliance plan demonstrates to outside investigators that the practice has made honest, ongoing attempts to find and fix weak areas.

Compliance plans cover more that just coding and billing. They also cover all areas of government regulation of medical practices, such as Equal Employment Opportunity (EEO) regulations (for example, hiring and promotion policies) and Occupational Safety and Health Administration (OSHA) regulations (for example, fire safety and handling of hazardous materials such as blood-borne pathogens).

**Parts of a Compliance Plan**

Generally, according to OIG, voluntary plans should contain seven elements:

1. Consistent written policies and procedures
2. Appointment of a compliance officer and committee
3. Training
4. Communication
5. Disciplinary systems
6. Auditing and monitoring
7. Responding to and correcting errors

Following OIG’s guidance can help in the defense against a false claims accusation. Having a plan in place shows that efforts are made to understand the rules and correct errors. This indicates to OIG that the problems may not add up to a pattern or practice of abuse, but may simply be errors.

**Compliance Officer and Committee**

To establish the plan and follow up on its provisions, most medical practices appoint a compliance officer who is in charge of the ongoing work. The compliance officer may be one of the practice’s physicians, the practice manager, or the billing manager. A compliance committee is also usually established to oversee the program.

**Code of Conduct**

The practice’s compliance plan emphasizes the procedures that are to be followed to meet existing documentation, coding, and medical necessity requirements. It also has a code of conduct for the members of the practice, which covers:

- Procedures for ensuring compliance with laws relating to referral arrangements
- Provisions for discussing compliance during employees’ performance reviews and for disciplinary action against employees, if needed
- Mechanisms to encourage employees to report compliance concerns directly to the compliance officer to reduce the risk of whistle-blower actions

Promoting ethical behavior in the practice’s daily operations can also reduce employee dissatisfaction and turnover by showing employees that the practice has a strong commitment to honest, ethical conduct.

**Ongoing Training**

**Physician Training**

Part of the compliance plan is a commitment to keep physicians trained in pertinent coding and regulatory matters. Often the medical insurance specialist or medical coder is assigned the task of briefing physicians on changed codes or medical necessity regulations. The following guidelines are helpful in conducting physician training classes:

Model Compliance Programs

http://oig.hhs.gov/fraud/complianceguidance.asp

**COMPLIANCE GUIDELINE**

**Medical Liability Insurance**

Medical liability cases for fraud often result in lawsuits. Physicians purchase professional liability insurance to cover such legal expenses. Although they are covered under the physician’s policy, other medical professionals often purchase their own liability insurance. Medical coders and medical insurance specialists who perform coding tasks are advised to have professional liability insurance called error and omission (E&O) insurance, which protects against financial loss due to intentional or unintentional failure to perform work correctly.
Keep the presentation as brief and straightforward as possible.

In a multispecialty practice, issues should be discussed by specialty; all physicians do not need to know changed rules on dermatology, for example.

Use actual examples, and stick to the facts when presenting material.

Explain the benefits of coding compliance to the physicians, and listen to their feedback to improve job performance.

Set up a way to address additional changes during the year, such as an office newsletter or compliance meetings.

**Staff Training**

An important part of the compliance plan is a commitment to train medical office staff members who are involved with coding and billing. Ongoing training also requires having the current annual updates, reading health plans’ bulletins and periodicals, and researching changed regulations. Compliance officers often conduct refresher classes in proper coding and billing techniques.

**THINKING IT THROUGH 2.10**

1. As a medical insurance specialist, why would ongoing training be important to you?

---

### Chapter Summary

<table>
<thead>
<tr>
<th>Learning Objective</th>
<th>Key Concept/Examples</th>
</tr>
</thead>
</table>
| **2.1** Explain the importance of accurate documentation when working with medical records. Pages 36–43 | • Medical records are created based on a variety of different types of documentation for patient encounters to provide the best possible care.  
• Both electronic health records (EHRs) and paper records are forms of medical documentation.  
EHRs offer several advantages:  
• Immediate access to health information  
• Computerized physician order management  
• Clinical decision support  
• Automated alerts and reminders  
• Electronic communication and connectivity  
• Patient support  
• Administration and report  
• Error reduction |
| **2.2** Compare the intent of HIPAA and ARRA/HITECH laws. Pages 44–47 | HIPAA is a law designed to:  
• Protect people’s private health information  
• Ensure health insurance coverage for workers and their families when they change or lose their jobs  
• Uncover fraud and abuse  
• Create standards for electronic transmission of healthcare transactions  
The ARRA of 2009, which includes the rules in the HITECH Act:  
• Contains additional provisions concerning the standards for electronic transmission of healthcare data  
• Guides the use of federal stimulus money to promote the adoption and meaningful use of health information technology, mainly using EHRs |
### Learning Objective

<table>
<thead>
<tr>
<th>Learning Objective</th>
<th>Key Concept/Examples</th>
</tr>
</thead>
</table>
| **2.3** Describe the relationship between covered entities and business associates. Pages 47–49 | - Under HIPAA, a covered entity is a health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a HIPAA transaction.  
- A business associate, such as a law firm or billing service that performs work for a covered entity, must agree to follow applicable HIPAA regulations to safeguard protected health information (PHI).  
- Electronic data interchange is used to facilitate transactions of information. |
| **2.4** Explain the purpose of the HIPAA Privacy Rule. Pages 49–57 | - It regulates the use and disclosure of patients’ PHI.  
- Both use and disclosure of PHI are necessary and permitted for patients’ treatment, payment, and healthcare operations (TPO).  
- PHI may also be released in some court cases, workers’ compensation cases, statutory reports, and research.  
- Providers are responsible for protecting their patients' PHI, following the minimum necessary standard in releasing it, and creating procedures to follow in regard to PHI. |
| **2.5** Briefly state the purpose of the HIPAA Security Rule. Pages 57–58 | - The rule requires covered entities to establish administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of health information.  
- Providers follow this rule through the use of encryption, access control, passwords, log files, backups to replace items after damage, and by developing security policies to handle violations when they do occur. |
| **2.6** Explain the purpose of the HITECH Breach Notification Rule. Pages 58–60 | - The rule requires covered entities to notify affected individuals following the discovery of a breach of unsecured health information.  
- Covered entities have specific breach notification procedures that they must follow in the event of a breach.  
- When a breach occurs, they must send the corresponding individual a breach notification, which must include five key points of information. |
- The standards require the covered entities to use common electronic transaction methods and code sets.  
- The four National Identifiers are for employers, healthcare providers, health plans, and patients. |
| **2.8** Explain how to guard against potentially fraudulent situations. Pages 63–66 | - Fraud and abuse regulations have been enacted to prevent fraud and abuse in healthcare billing.  
- OIG has the task of detecting healthcare fraud and abuse and related law enforcement.  
- The FCA prohibits submitting a fraudulent claim or making a false statement or representation in connection with a claim.  
- FERA strengthens the provisions of the FCA. |
| **2.9** Explain how various organizations enforce HIPAA. Pages 66–68 | - They were created to reconcile differences in enforcement procedures that had existed between the privacy and security standards.  
- The Office for Civil Rights enforces the HIPAA privacy standards, while CMS enforces all other standards.  
- OIG combats fraud and abuse in health insurance and healthcare delivery. |
Learning Objective

2.10 Assess the benefits of a compliance plan.
Pages 68–70

<table>
<thead>
<tr>
<th>Key Concept/Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance plans include:</td>
</tr>
<tr>
<td>• Consistent written policies and procedures</td>
</tr>
<tr>
<td>• Appointment of a compliance officer and committee</td>
</tr>
<tr>
<td>• Training plans</td>
</tr>
<tr>
<td>• Communication guidelines</td>
</tr>
<tr>
<td>• Disciplinary systems</td>
</tr>
<tr>
<td>• Ongoing monitoring and auditing of claim preparation</td>
</tr>
<tr>
<td>• Responding to and correcting errors</td>
</tr>
<tr>
<td>• A formal process that is a sign that the practice has made a good-faith effort to achieve compliance</td>
</tr>
</tbody>
</table>

Review Questions

Match the key terms with their definitions.

1. **LO 2.4 HIPAA Privacy Rule**
2. **LO 2.6 breach**
3. **LO 2.4 minimum necessary standard**
4. **LO 2.3 business associate**
5. **LO 2.3 clearinghouse**
6. **LO 2.4 Notice of Privacy Practices**
7. **LO 2.7 code set**
8. **LO 2.5 HIPAA Security Rule**
9. **LO 2.3 covered entity**
10. **LO 2.1 documentation**

A. **Law under the Administrative Simplification provisions of HIPAA requiring covered entities to establish administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of health information**
B. **The systematic, logical, and consistent recording of a patient’s health status—history, examinations, tests, results of treatments, and observations—in chronological order in a patient’s medical record**
C. **A person or organization that performs a function or activity for a covered entity but is not part of its workforce**
D. **The principle that individually identifiable health information should be disclosed only to the extent needed to support the purpose of the disclosure**
E. **Under HIPAA, a health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a HIPAA transaction**
F. **Law under the Administrative Simplification provisions of HIPAA regulating the use and disclosure of patients’ protected health information—individually identifiable health information that is transmitted or maintained by electronic media**
G. **A HIPAA-mandated document that presents a covered entity’s principles and procedures related to the protection of patients’ protected health information**
H. **A coding system used to encode elements of data**
I. **A company that offers providers, for a fee, the service of receiving electronic or paper claims, checking and preparing them for processing, and transmitting them in proper data format to the correct carriers**
J. **Impermissible use or disclosure of PHI that could pose significant risk to the affected person**

Enhance your learning at mcgrawhillconnect.com!

- Practice Exercises
- Worksheets
- Activities
- Integrated eBook
Select the letter that best completes the statement or answers the question.

1. **LO 2.2** Which of the following laws is designed to uncover fraud and abuse?
   A. Fraud and Abuse Act
   B. ARRA
   C. HIPAA
   D. HITECH Act

2. **LO 2.4** A Notice of Privacy Practices is given to
   A. a practice’s patients
   B. a practice’s business associates
   C. the health plans with which a practice contracts
   D. all physicians who refer patients to the practice

3. **LO 2.4** Patients’ PHI may be released without authorization to
   A. local newspapers
   B. employers in workers’ compensation cases
   C. social workers
   D. family and friends

4. **LO 2.4** Which government group has the authority to enforce the HIPAA Privacy Rule?
   A. CIA
   B. OIG
   C. OCR
   D. Medicaid

5. **LO 2.4** Patients always have the right to
   A. withdraw their authorization to release information
   B. alter the information in their medical records
   C. block release of information about their communicable diseases to the state health department
   D. restrict the release of all de-identified health information associated with them

6. **LO 2.4** The authorization to release information must specify
   A. the number of pages to be released
   B. the Social Security number of the patient
   C. the entity to whom the information is to be released
   D. the name of the treating physician

7. **LO 2.4** Health information that does not identify an individual is referred to as
   A. protected health information
   B. authorized health release
   C. statutory data
   D. de-identified health information

8. **LO 2.6** Analyze the following scenarios to determine which would likely warrant a breach notification.
   A. de-identified health information is accessed by an outside provider
   B. a company’s workforce members use information in good faith
   C. the database of a large insurance company is accessed by a hacker
   D. information is released to the government for statistical purposes

9. **LO 2.5** The main purpose of the HIPAA Security Rule is to
   A. regulate electronic transactions
   B. protect research data
   C. control the confidentiality and integrity of and access to protected health information
   D. protect medical facilities from criminal acts such as robbery

10. **LO 2.10** A compliance plan contains
    A. consistent written policies and procedures
    B. medical office staff names
    C. the practice’s main health plans
    D. a list of all the practice’s patients

I. Define the following abbreviations:

1. **LO 2.9** OCR ____________________________
2. **LO 2.4** PHI ____________________________
3. **LO 2.7** TCS ____________________________
4. **LO 2.4** DRS ____________________________
5. **LO 2.1** EHR ____________________________
6. **LO 2.1** CC ____________________________
7. **LO 2.7** NPI ____________________________
8. **LO 2.4** NPP ____________________________
9. **LO 2.8** OIG ____________________________

Enhance your learning at mcgrawhillconnect.com!

- Practice Exercises
- Worksheets
- Activities
- Integrated eBook
Applying Your Knowledge

Case 2.1  Working with HIPAA
In each of these cases of release of PHI, was the HIPAA Privacy Rule followed? Why or why not?

A. **LO 2.4** A laboratory communicates a patient’s medical test results to a physician by phone.

B. **LO 2.4** A physician mails a copy of a patient’s medical record to a specialist who intends to treat the patient.

C. **LO 2.4** A hospital faxes a patient’s healthcare instructions to a nursing home to which the patient is to be transferred.

D. **LO 2.4** A doctor discusses a patient’s condition over the phone with an emergency room physician who is providing the patient with emergency care.

E. **LO 2.4** A doctor orally discusses a patient’s treatment regimen with a nurse who will be involved in the patient’s care.

F. **LO 2.4** A physician consults with another physician by e-mail about a patient’s condition.

G. **LO 2.4** A hospital shares an organ donor’s medical information with another hospital treating the organ recipient.

H. **LO 2.4** A medical insurance specialist answers questions from a health plan over the phone about a patient’s dates of service on a submitted claim.

Case 2.2  Applying HIPAA

**LO 2.4** Rosalyn Ramirez is a medical insurance specialist employed by Valley Associates, PC, a midsized multispecialty practice with an excellent record of complying with HIPAA rules. Rosalyn answers the telephone and hears this question:

“This is Jane Mazloum, I’m a patient of Dr. Olgivy. I just listened to a phone message from your office about coming in for a checkup. My husband and I were talking about this. Since this is my first pregnancy and I am working, we really don’t want anyone else to know about it yet. Has this information been given to anybody outside the clinic?” How do you recommend that she respond?
Patient Name: Angelo Diaz  
Health Record Number: AD100  
Date of Birth: 10-12-1945  

1. I authorize the use or disclosure of the above named individual’s health information as described below.

2. The following individual(s) or organization(s) are authorized to make the disclosure: Dr. L. Handlesman  

3. The type of information to be used or disclosed is as follows (check the appropriate boxes and include other information where indicated)

- [ ] problem list  
- [ ] medication list  
- [ ] list of allergies  
- [ ] immunization records  
- [ ] most recent history  
- [ ] most recent discharge summary  
- [ ] lab results (please describe the dates or types of lab tests you would like disclosed):  
- [ ] x-ray and imaging reports (please describe the dates or types of x-rays or images you would like disclosed):  
- [ ] consultation reports from (please supply doctors’ names):  
- [ ] entire record  
- [ ] other (please describe): Progress notes

4. I understand that the information in my health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV). It may also include information about behavioral or mental health services, and treatment for alcohol and drug abuse.

5. The information identified above may be used by or disclosed to the following individuals or organization(s):

   Name: Blue Cross & Blue Shield  
   Address:  

6. This information for which I’m authorizing disclosure will be used for the following purpose:

- [ ] my personal records  
- [ ] sharing with other healthcare providers as needed/other (please describe):  

7. 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.

8. This authorization will expire (insert date or event): 3-1-2016  
If I fail to specify an expiration date or event, this authorization will expire six months from the date on which it was signed.

9. I understand that once the above information is disclosed, it may be redisclosed by the recipient and the information may not be protected by federal privacy laws or regulations.

10. I understand authorizing the use or disclosure of the information identified above is voluntary. I need not sign this form to ensure healthcare treatment.

Signature of patient or legal representative: Angelo Diaz  
Date: 3-1-2016  
If signed by legal representative, relationship to patient

Signature of witness:  
Date:

Distribution of copies: Original to provider; copy to patient; copy to accompany use or disclosure

Note: This sample form was developed by the American Health Information Management Association for discussion purposes. It should not be used without review by the issuing organization’s legal counsel to ensure compliance with other federal and state laws and regulations.
Case 2.3 Handling Authorizations

LO 2.4 Angelo Diaz signed the authorization form on page 75. When his insurance company called for an explanation of a reported procedure that Dr. Handlesman performed to treat a stomach ulcer, George Welofar, the clinic's registered nurse, released copies of his complete file. On reviewing Mr. Diaz's history of treatment for alcohol abuse, the insurance company refused to pay the claim, stating that Mr. Diaz's alcoholism had caused the condition. Mr. Diaz complained to the practice manager about the situation.

Should the information have been released?

Case 2.4 Working with Medical Records

The following chart note contains typical documentation abbreviations and shortened forms for words.

65-yo female; hx of right breast ca seen in SurgiCenter for bx of breast mass. Frozen section reported as benign tumor. Bleeding followed the biopsy. Reopened the breast along site of previous incision with coagulation of bleeders. Wound sutured. Pt adm. for observation of post-op bleeding. Discharged with no bleeding recurrence.

Final Dx: Benign neoplasm, left breast.

Research the meaning of each abbreviation (see the Abbreviations list at the end of the text), and write their meanings:

A. LO 2.1 yo
B. LO 2.1 hx
C. LO 2.1 ca
D. LO 2.1 bx
E. LO 2.1 Pt
F. LO 2.1 adm.
G. LO 2.1 op
H. LO 2.1 Dx