PRIVACY IN THE PHYSICIAN’S OFFICE

SCENARIO

Sabrina Ragland, a medical assistant with 12 years of experience, works for a gastroenterologist, Dr. Tim Taylor. Her mother-in-law, Elsa Ragland, has been a registered nurse (RN) for 40 years. For more than half of her career, Elsa has worked for a local internist, Dr. Royce Berry. A casual comment at a Ragland family picnic resulted in a medical professional liability lawsuit based on violation of patient privacy. Sabrina and Elsa’s careers were jeopardized by a simple exchange of what seemed to be innocent information.

Vivian Adams, a 42-year-old hospital insurance biller, saw Dr. Berry in his office for pain in the lower left quadrant. Ms. Adams was not a new patient, but she had not visited the office in approximately 2 years.

When she arrived for her appointment, she was presented with the office privacy policy and was asked to sign the document. Vivian glanced through it, signed it, and saw the doctor. He performed an examination and found that Vivian likely was suffering from irritable bowel syndrome (IBS); he then prescribed medication. Ms. Adams called the physician 1 week later, complaining that she was no better. Dr. Berry changed her medication without seeing her and did not hear from her again, other than her requests for refills of the IBS medication.

After 6 months with no improvement, Ms. Adams went to Dr. Taylor; he performed several diagnostic tests and told Ms. Adams that she had colon cancer. She was given a bleak prognosis. She told Dr. Taylor that she blamed Dr. Berry for not being more thorough in his testing. Sabrina was in the room and heard the comment.

That weekend at the picnic, Sabrina mentioned Ms. Adams to her mother-in-law and stated that the patient might sue Dr. Berry, although the patient never said those words. Elsa defended Dr. Berry and proclaimed that he was a good doctor, then expressed her hope that Ms. Adams would not sue her employer. One week later, Elsa was in a grocery store and saw Ms. Adams. Elsa immediately expressed her sympathy about the diagnosis and then asked whether there was anything she could do. Her intent was to be kind and to try to avert litigation against Dr. Berry. Her gesture might have been well received had Ms. Adams’ daughter, Terri, not been with her. Terri was not yet aware that her mother had been diagnosed with cancer. Ms. Adams had told no one about her illness at that point. After the incident at the grocery store, the first person Ms. Adams told was her attorney.

While studying this chapter, think about the following questions:
- When can the medical assistant discuss a patient, with whom, and under what circumstances?
- What has the Health Insurance Portability and Accountability Act (HIPAA) done for the medical industry and the patients it serves?
- When new policies and procedures are implemented, how can the staff embrace the changes and ease the transition?
- What happens if the patient refuses to sign the privacy policy?

LEARNING OBJECTIVES

1. Define, spell, and pronounce the terms listed in the vocabulary.
2. Explain how the HIPAA Privacy Rule benefits the healthcare industry and patients.
3. Explain the difference between Title I and Title II of the Privacy Rule.
4. List the rights of patients under the Privacy Rule.
5. List the elements that must be included in a Notice of Privacy Practices.
6. Briefly explain what is expected of healthcare providers under the Privacy Rule.
7. Describe an incidental disclosure.
8. List the three instances when a parent is not considered the child’s representative.
9. Explain the circumstances under which a provider may discuss protected health information with a patient’s family and family.
10. Discuss the role of the Notice of Privacy Practices in emergencies.
Vocabulary

avert To see coming and ward off or avoid.
bright Not hopeful or encouraging.
business associates Individuals or organizations that perform or assist a covered entity in the performance of a function or activity involving the use or disclosure of individually identifiable health information.
complainant (kuhm-pla’-nuhnt) The person making a complaint against another person or an organization.
covered entities As defined by HIPAA, organizations that transmit information in an electronic form during a transaction.
divulge (duh-vuhlj’) To make known, as a confidence or secret.
due diligence The effort made by an ordinarily prudent or reasonable party to prevent harm to another party or oneself; doing everything possible to prevent something negative from happening; also called due care.
electronic media The means of electronic transmission, including the Internet, private networks, dial-up phone lines, and fax modems; includes information moved from one place to another while stored on an electronic device.
healthcare providers Providers of medical or health services, individually or as organizations, that furnish, bill for, or are paid for services or products.
incidental disclosure A secondary use of health information that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted.
individually identifiable health information Any part of a patient’s health record that is created or received by a covered entity.
infused Derived as a conclusion from facts and premises.
Office for Civil Rights (OCR) The division of the federal government that enforces privacy standards.
personal health information (PHI) The patient’s own information that pertains to his or her health.
preclude To rule out in advance.
prevalent Generally or widely accepted, practiced, or favored.
privacy officer A person designated to ensure compliance with privacy standards for a covered entity.
protected health information (PHI) Any individually identifiable health information that may be transmitted and/or maintained in electronic form.
transactions As defined by HIPAA, transmissions of information between two parties to carry out financial or administrative activities related to healthcare.
verbiage A manner of expressing oneself in words.

The creation of privacy and security laws was a huge step toward more efficient healthcare and faster reimbursements. However, technology often forces organizations to move forward somewhat quickly. Healthcare facilities with already strapped budgets sometimes view such innovations as a hindrance. Compliance officers at larger facilities may wonder whether additional federal regulations are necessary.

Many healthcare workers believe that they can say nothing to anyone, about any patient, at any time. When employees of the physician’s office gain an understanding of the compliance HIPAA requires, they can feel secure in their dealings with patients and other individuals.

Health Insurance Portability and Accountability Act

HIPAA, which was enacted in 1996, is a group of laws that affect employees of healthcare facilities, insurance companies, or other covered entities and the patients they serve. The federal government required all covered entities to be in compliance with HIPAA by April 14, 2003 (small healthcare plans received an extra year to comply).

Effect of the HIPAA Privacy Rule

The HIPAA Privacy Rule creates national standards to protect individuals’ medical records and other personal health information (PHI). This group of laws was the first enacted to protect patient privacy. The Privacy Rule benefits both patients and healthcare providers:

- Patients have more control over their medical records.
- Patients are able to make informed choices about the use of their PHI.
- Boundaries are set on the use and release of health records.
- Safeguards are established that healthcare providers must ensure to protect the privacy of health information.
- Violators are held accountable and face both civil and criminal penalties if patients’ privacy rights are compromised.
- Public health is protected by the balance struck between public responsibility and disclosure of PHI.

Under the few laws that existed before the HIPAA Privacy Rule, personal health information could be distributed to others without notifying the patient or obtaining his or her authorization, even if the information exchange had nothing to do with the patient’s medical treatment or healthcare reimbursement. A health plan could pass patient information to a financial lender, who might then deny the patient a home mortgage or credit card based on the health history. Employers could obtain health information and use it in personnel decisions. Because computers make information exchange so much easier, laws had to be enacted to protect patients’ privacy.

Title I and Title II Provisions

HIPAA has two provisions, Title I and Title II. The Title I covers insurance reform, and Title II deals with administrative simpli-
fication. Title I limits the use of pre-existing health conditions, which in the past prevented an employee from obtaining health insurance coverage or limited that coverage. If an individual left a job with insurance coverage and attempted to secure new coverage, a pre-existing health condition often would preclude that person from obtaining coverage for that illness. Many individuals were refused any coverage at all, especially if the condition was a serious one, such as a heart condition or high blood pressure. Today, because of HIPAA laws, discrimination against individuals in poor health now or in the past is prohibited. The regulations limit the use of pre-existing condition exclusions and guarantee that certain individuals can purchase healthcare insurance after leaving or losing a job.

The Consolidated Omnibus Budget Reconciliation Act (COBRA) was passed by Congress in 1986. COBRA provides certain former employees, retirees, spouses, former spouses, and dependent children with group health coverage. The premium usually is higher than that paid during employment but still usually lower than for individual health coverage. Most people who lose their job for any reason have difficulty paying for COBRA coverage.

Certain criteria must be met to qualify for COBRA coverage. The company must have at least 50 employees to be required to offer COBRA to its employees. The employees need not be all full-time workers; certain calculations allow part-time workers to be counted to reach the 50-employee benchmark. Also, the employee must be a qualified beneficiary to receive COBRA benefits. A qualified beneficiary is an individual who was covered under the healthcare plan the day before a qualifying event. A qualifying event is an incident that would cause an employee to lose healthcare coverage. (For more information on COBRA qualifying events, visit the Evolve site at evolve.elsevier.com/kimm.)

The goal of Title II is to reduce administrative costs in the healthcare industry. Often goals sound simple, but many steps must be taken to reach a goal. The medical assistant who enters school sets graduation as the goal. However, to graduate (i.e., reach the goal), the medical assistant must study, pass tests, arrange for childcare, sacrifice sleep, adjust working hours, readjust to the school environment, and make any number of other adjustments. Likewise, to simplify the administrative costs involved in patient care, many different objectives must be met. Several agencies must work together and agree on various regulations. They must share information as well as resources. Agencies must compromise and “give and take” when forming policies or working toward administrative goals.

CRITICAL THINKING APPLICATION 17-1
- How does information sharing help to cut patient healthcare costs?
- What other reasons might exist for sharing patient information?

Provisions of Administrative Simplification

If given a choice between using a computer or an electric typewriter to write a report, most individuals would choose the computer. Because computers can perform so many duties much faster than those that were performed manually, they have become indispensable to the healthcare profession. Electronic media are used daily in modern physicians’ offices and healthcare facilities. However, as the use of computers has become prevalent, patients have begun to express concern about who sees protected health information (PHI) and what is done with that information.

Title II of HIPAA has two parts:
- Development and implementation of standardized electronic transactions using standard code sets
- Implementation of privacy and security procedures to prevent the misuse of health information by ensuring confidentiality

The second part of the administrative simplification provision deals with the privacy, confidentiality, and security of PHI and is the focus of this chapter.

Patients’ Rights

Separate from the Patients’ Bill of Rights, HIPAA provides for several patients’ rights:
- The right to notice of a facility’s privacy practices
- The right to have access to, view, and obtain a copy of their PHI
- The right to restrict certain parts or uses of their PHI
- The right to request that communications from the facility be kept confidential
- The right to request that the facility amend the PHI
- The right to receive notice of all disclosures of their PHI

These rights are the heart of the HIPAA Privacy Rule. They must be protected by all involved in the healthcare profession.

Right to Notice of Privacy Practices

Patients have the right to a copy of the Notice of Privacy Practices used in the physician’s office (Figure 17-1). A copy of this document also must be prominently displayed in the office. These privacy practices are developed by the individual facility and must be written in language that patient will understand. Patients should be given a copy of the Notice of Privacy Practices and should sign an acknowledgment that they received it. If a patient refuses to sign the acknowledgment, the medical assistant can note that the document was offered to the patient and the person refused to sign. This proves due diligence on the part of the office and that a good faith effort was made to provide the patient with privacy information. Most patients sign the document. Be prepared to explain the Notice of Privacy Practices to patients. It must include:
- How PHI is used and disclosed by the facility
- The duties of the provider in protecting health information
- The patient’s rights regarding PHI
- How complaints can be filed if patients believe their privacy has been violated
- Whom to contact at the facility for more information
- The effective date of the Notice of Privacy Practices

Right to Access Protected Health Information

Patients must be allowed access to their personal health information. The maker, not the patient, owns the record; however, the HIPAA Privacy Rule grants patients the right to access, inspect, and obtain a copy of their health information. Most physicians’ offices require patients to request access in writing and to act on
that request within 30 days (Figure 17-2). HIPAA does restrict access to psychotherapy notes, information compiled for use in legal proceedings, and information exempted from disclosure by the Clinical Laboratory Improvement Amendment (CLIA).

**CRITICAL THINKING APPLICATION 17-2**
- Why is patient access to protected health information important?
- When might the patient need access to his or her health records?

**Right to Request Restrictions on Certain Uses and Disclosures of Protected Health Information**

Patients can request restrictions on the use of their PHI. For instance, if a patient had an abortion many years ago and does not want that information released, she has the right to ask a provider not to divulge that information. The provider does not have to agree to the request but must review it and give a good reason for the restriction not to be honored. An appeal process should be in place for cases in which the provider does not agree with the restriction.

**Right to Request Confidential Communications**

Patients have the right to determine where they want to receive communications from the provider. The patient may prefer to be contacted on a cell phone instead of a home phone, or through e-mail. Providers must accommodate reasonable requests. Suppose a married female patient comes to the clinic for a pregnancy test. Further suppose that her husband has had a vasectomy. Clearly, a call to her home phone number with test results could initiate personal and private difficulties for the patient. Make sure the preferred method of communication is used when contacting any patient.
PROCEDURE 17-1

Apply HIPAA Rules in Regard to Privacy/Release of Information

GOAL: To follow HIPAA guidelines so that patient confidentiality is kept and the patient’s health information is protected.

EQUIPMENT and SUPPLIES
- HIPAA Rule
- Office policy and procedure manual
- Release of information forms
- Notice of privacy policy

PROCEDURAL STEPS
1. Review the HIPAA law, office policy and procedure manual, and the facility’s notice of privacy practices.
   PURPOSE: To make certain that all applicable laws and policies are followed when releasing medical information.
2. Examine the document requesting release of patient information.
   PURPOSE: To determine if the document is valid and that the information can be released to the requesting party. Most medical facilities require that all information requests be addressed in writing, and some require a specific time period for response, such as 1 week.
3. Compare the request to the facility’s own information release form. Send the requestor a facility form, if necessary, by mail or fax.
   PURPOSE: To obtain all of the information that the facility requires in releasing information. Some requests are not complete when received, and the medical assistant must make certain that all of the required information is provided before the release of patient information.
4. Determine what information is being requested.
   PURPOSE: The medical facility should not release any additional information other than what is specifically requested.
5. Make copies of the information for the requestor.
6. Mail or fax the information, depending upon their requested method of delivery. Make certain that fax submissions contain a confidentiality statement.
   PURPOSE: To ensure patient confidentiality.
7. Document the release of information in the patient’s medical record, if required by office policy.
   PURPOSE: To provide a reference point as to when the request was completed and mailed.

REQUEST TO ACCESS MEDICAL RECORD

Patients have the right to access their personal health information. We will be happy to accommodate any patient who wishes to exercise this access to inspect or obtain a copy of the record. Please provide the information requested on this form. This request will be acted upon within thirty (30) days. Standard copy charges will apply.

Patient Name ____________________________
Date of Birth ____________________________
Address ________________________________
City __________________ State ____________ ZIP ____________
Email Address __________________________
Date of Last Office Visit __________________

Please note below what information should be copied or provided:
_____________________________________
_____________________________________
_____________________________________
_____________________________________

Please note below the following change(s) that need to be addressed:
_____________________________________
_____________________________________

I wish to receive a regular accounting of non-routine disclosures of my protected health information.
☐ Yes ☐ No

Patient Signature ________________________ Date ____________

FOR OFFICE USE ONLY
Date Copied __________________ Date Mailed __________________
Certified Mail # _______________________

FIGURE 17-2 Request to access a medical record.
Right to Request Amendment of Protected Health Information

If patients inspect their medical record and find an error, they can request that changes be made to the record. This request should be made in writing. Providers must review the request and act on it in a timely manner, generally within 60 days. The request may be denied if the provider was not the creator of the record, as in the case of records provided by a consulting physician. Or, the provider may believe that the information is correct and complete. A review process must be in place by which such requests can be considered.

Right to Receive an Accounting of Disclosures of Protected Health Information

Patients may request that the physician provide an accounting of all disclosures of the patient's PHI that are not nonroutine (as defined in the facility's Notice of Privacy Practices). Patients are entitled to receive this accounting annually without charge, but the provider can charge patients for additional accountings.

### SEVEN COMPONENTS OF A HIPAA COMPLIANCE PROGRAM

- The Office of the Inspector General (OIG) of the Department of Health and Human Services has developed seven components of an effective HIPAA compliance program:
  1. Conducting internal monitoring and auditing
  2. Implementing compliance and practice standards
  3. Designating a compliance officer or contact
  4. Conducting appropriate training and education
  5. Responding appropriately to detected offenses and developing corrective action
  6. Developing open lines of communication
  7. Enforcing disciplinary standards through well-publicized guidelines

### Responsibilities of Providers or Health Plans

The responsibilities placed on providers and health plans seems extensive when one reads the actual verbiage of the law. Do not be intimidated when reading a publication written by the federal government. These documents are rarely written for ease of understanding and may need to be reread several times before the reader grasps the meaning of a regulation.

In general, the HIPAA Privacy Rule requires activities such as the following:

- Notifying patients of their privacy rights
- Explaining how their health information might be used
- Developing privacy procedures in the facility
- Implementing those privacy procedures
- Training employees so that they understand the procedures
- Designating an individual to be responsible for implementation
- Securing medical records so that they are not available to those who do not need them

### PERMISSION TO DISCLOSE PROTECTED HEALTH INFORMATION

Once the patient has signed the Notice of Privacy Practices, the physician may disclose PHI in the manner that is described in the policy. Virtually all the daily operations that involve PHI are covered under the privacy practices document.

Some offices ask patients to sign a receipt of the Notice of Privacy Practices annually. Others simply post the current policy prominently in the office and state where it can be found on the original notice that the patient signs. With either method, every current medical record should contain a signed Notice of Privacy Practices, an acknowledgement that the patient received the Notice of Privacy Practices, or a statement that the patient refused to sign it. Physicians also use separate release of information forms that detail exactly where to call a patient, whether the patient prefers e-mail communications, and/or specific releases for information related to human immunodeficiency virus (HIV) infection or psychotherapy (Figures 17-3 and 17-4).

At times, conflicting permissions may be an issue in the disclosure of PHI. Suppose a patient requests that a copy of his or her medical record be sent to a third party, such as an attorney. The patient signs the release at an office visit. Before the medical record is copied and sent, the attorney forwards a signed release for just the progress notes. Call the patient first and attempt to verify what he or she wants sent. Another option is to adhere to the most restrictive request; in this case, send only the progress notes. Always document any form of communication about the patient's preference in writing. The medical assistant may find it necessary to ask the patient to sign a new permission form. Do not hesitate to contact the patient if any question arises about what the person wants released.

### Identifying the Patient

Providers see numerous patients each day, and the medical assistant may not know each one by sight. Always insist on identification when releasing any type of health information to anyone. A state-issued driver's license or identification card is the best means of identification, but alternates may be necessary for those who do not have that particular document. The office policy and procedures manual should list acceptable forms of identification. When making any type of disclosure, make sure to note the reason the person has the authority to request and receive the PHI.

### Patient Names and Sign-In Sheets

A staff member in a physician's office may call out a patient's name when it is time to see the physician. Sign-in sheets that list patient names may also be used. Covered entities are permitted to make such incidental disclosures if they comply with the minimum necessary requirements of HIPAA (Figure 17-5). An incidental disclosure is a secondary use that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted.

The Privacy Rule is not intended to impede customary and necessary healthcare communications or practices or to require that all risk of incidental use or disclosure be eliminated to satisfy
Patient Consent to the Use and Disclosure of Health Information for Treatment, Payment, or Health Care Operations

I understand that as part of my health care, the practice organizes and maintains paper and/or electronic records describing my health history, symptoms, examination and test results, diagnoses, treatment, and any plans for future care or treatment. I understand that this information serves as:

- A basis for planning my care and treatment,
- A means of communication among professionals who contribute to my care,
- A source of information for applying my diagnosis and treatment information to my bill,
- A means by which a third-party payer can verify that services billed were actually provided,
- A tool for routine health care operations, such as assessing quality and reviewing the competence of staff.

I have been provided the opportunity to review the "Notice of Patient Privacy Information Practices" that provides a more complete description of information uses and disclosures. I understand that I have the following rights:

- The right to review the "Notice" prior to acknowledging this consent,
- The right to restrict or revoke the use or disclosure of my health information for other uses or purposes, and
- The right to request restrictions as to how my health information may be used or disclosed to carry out treatment, payment, or health care operations.

Restrictions:

I request the following restrictions to the use or disclosure of my health information:

[ ] May discuss treatment, payment, or health care operation with the following persons:

(Please check all that apply) Spouse [ ] Your Children [ ] Relatives [ ] Others [ ] Parents [ ]

Please list the names and relationship, if you checked "Relatives" or "Others" above

Messages or Appointment Reminders: (Please check all that apply)

May we leave a message on your answering machine at home [ ] or at work [ ]? Do not leave a message [ ]

May we leave a message with someone at your home using the doctor's name or the practice name? Yes [ ] No [ ]

May we leave a message with someone at your work using the doctor's name or the practice name? Yes [ ] No [ ]

Messages will be of a non-sensitive nature, such as appointment reminders.

I understand that as part of treatment, payment, or health care operations, it may become necessary to disclose health information to another entity, i.e., it relates to other health care providers, labs, and/or other individuals or agencies as permitted or required by state or federal law.

I fully understand and accept the information provided by this consent.

Signature _____________________________ Print name of person signing _____________________________ Date _______________

*If other than patient is signing, are you the parent, legal guardian, custodian, or have Power of Attorney for this patient for treatment, payment, or health care operations? Yes [ ] No [ ]

FOR OFFICE USE ONLY

[ ] Patient refused to sign the consent form.
[ ] Restrictions were added by the patient (see restrictions listed above) on (date)
[ ] "Consent form" received and reviewed by _____________________________ on (date)
[ ] "Consent form" placed in the patient's medical record on (date)

FIGURE 17-3 Example of a HIPAA-compliant patient disclosure form. (From Klinger DM: Saunders essentials of medical assisting, ed 2, St Louis, 2010, WB Saunders.)

the rule's standards. Disclosures that could occur as a byproduct of engaging in healthcare communications or practices may be considered acceptable under the Privacy Rule. Incidental disclosures might include:

- Confidential conversations between providers or with patients, if a possibility exists that they may be overheard (e.g., by hearing the patient and physician talking through the wall when in an adjacent examination room)
- Seeing other patient names when signing in
- A person not authorized to see PHI walks by medical equipment and sees material containing individually identifiable health information (e.g., sees a patient's name on an ultrasound screen)
- Physicians speaking with patients in semiprivate hospital rooms
- Healthcare staff orally coordinating patient care services at a nurses' station or central location in an office
- A pharmacist discussing a patient with a physician on the phone when another person is standing nearby

Most physicians' offices have implemented sign-in sheets that ideally allow only one patient to sign in at a time and prevent them from seeing other patient names. Sign-in sheets that use pressure-
sensitive stickers are a good example. The patient signs in on the form, then the sticker is removed and placed either in the patient's medical record or on a log sheet. Some offices are more technologically advanced and have a computer sign-in system. The patient arrives and goes to the computer screen, sees his or her name, and then presses "enter" to signify that he or she has arrived for the appointment. The patient's name appears only for 15 minutes or so before the appointment and for 15 minutes after. If the name is not on the screen, the patient is directed to see the office staff. This subtly teaches the patient to be on time for appointments. These devices save time, although the patient must receive brief training in how to use the system. The short time the patient's name is on the screen is an incidental exposure, but it is acceptable according to HIPAA guidelines, as explained previously.

Placement of Patient Medical Records

Many physicians' offices place medical records inside a wall folder just outside the examination room. By turning the record so that the name cannot be seen by someone passing in the hallway, the facility meets the minimum necessary requirement to protect patient privacy. The hallway area should be supervised, and non-employees should be escorted when in the clinical area of the office.
HIPAA MINIMUM NECESSARY STANDARD
[45 CFR 164.502(b), 164.514(d)]

Background
The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule’s requirements for minimum necessary standards are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

How the Rule Works
The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual’s authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity’s business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

http://www.hhs.gov/ocr/hipaa/

FIGURE 17-5 Overview for HIPAA’s minimum necessary standard.

CRITICAL THINKING APPLICATION 17-3
- Why is it important to safeguard the names of patients in hallways?
- How might Patient A be affected if Patient B sees Patient A’s name on a chart in the medical facility?

FIGURE 17-6 In most cases the parent is considered the child’s representative and is allowed to see the child’s medical records.

Children’s Health Records
The Privacy Rule does allow parents to see the medical records of their children as long as this is not inconsistent with state law. In most cases the parent is the child’s personal representative under the Privacy Rule (Figure 17-6). However, under some circumstances, the parent is not considered the child’s personal representative, such as:

- When the minor is the one who consents to care and the parent’s consent is not required under state or other applicable law (e.g., an emancipated minor)
- When the minor obtains care at the direction of a court or a person appointed by the court
- When the parent agrees that the minor and healthcare provider may have a confidential relationship

Discussing Information with Family and Friends
The Privacy Rule specifically permits covered entities to share information directly relevant to the patient’s care with a spouse, family members, friends, or other individuals identified by the patient. The covered entity also may share relevant information with the family and these other people if it can reasonably be inferred, based on professional judgment, that the patient does not object or that the action is in the patient’s best interest. Remember that if the patient has requested that such information not be shared with others, the provider must honor that request unless it is deemed unreasonable.

Both covered entities and business associates can discuss a patient’s bill with a person other than the patient to obtain reimbursement. No limit is placed on those to whom such a disclosure may be made. However, the Privacy Rule does require a covered entity or business associate to reasonably limit the amount of information disclosed for such purposes to the minimum necessary and to abide by any reasonable requests by the patient for confidential communications and restrictions.
PROCEDE 17-2

Perform Risk Management Procedures

**GOAL:** To prevent risk and liability in the physician's office.

**EQUIPMENT and SUPPLIES**
- Copy of laws affecting the physician's practice
- Computer with Internet access
- Office policy and procedure manual

**PROCEDURAL STEPS**

1. Research laws that affect the medical office on the Internet.
   **PURPOSE:** To determine the laws that will influence the operations of a medical office and how they affect the role of the medical assistant.
2. Become familiar with office policies and procedures.
   **PURPOSE:** To make certain that policies and procedures are followed when carrying out daily operations at the medical facility.
3. Determine common risks that occur in the medical facility.

   **PURPOSE:** To learn what issues or situations might result in losses at a medical facility and determine ways to avoid such risks.
4. Perform a risk assessment at the medical facility.
   **PURPOSE:** To determine specific risks that are present at a medical facility.
5. Discuss the risks with office management or in a staff meeting.
6. Determine ways to eliminate the risks found during the assessment.
   **PURPOSE:** To work as a team to eliminate possible risks.
7. Devise a plan to eliminate or reduce risk in the medical office based upon the risk assessment.
   **PURPOSE:** To take specific steps toward the reduction of risk in the facility.
8. Document all risk assessments and management efforts.
   **PURPOSE:** To provide proof that risks were assessed and managed as needed by regulatory and/or compliance agencies.

### Telephone Messages and Faxes

Medical assistants must communicate with patients, and that communication often is initiated with a telephone call. At times the patient is not at home or available, and the medical assistant must use professional judgment about leaving a message and how much information to disclose to the person who answers the telephone. Even leaving a message on an answering machine can be questionable, because no one is sure who will hear a message containing PHI.

If the patient has requested that the provider or provider's employees communicate only in a confidential manner, such as by alternative means or at an alternative location, the provider must honor that request if it is reasonable. For instance, requests to receive calls at work instead of at home are reasonable requests, unless there are extenuating circumstances.

A fax can be sent containing PHI to another healthcare provider for treatment purposes or to another individual as requested by the patient. Use reasonable care in sending a fax, such as verifying the correct numbers, directing the fax to a certain person, and using cover sheets that stress confidentiality. All fax machines should be located in secure areas to prevent unauthorized access to PHI. Information used for treatment purposes can be shared by fax, e-mail, or telephone with other healthcare providers.

### Emergencies

Healthcare providers and facilities, such as hospitals, with a direct treatment relationship with individuals are not required to provide their Notice of Privacy Practices to patients at the time they are providing emergency treatment (Figure 17-7). In such situations, the HIPAA Privacy Rule requires only that providers give patients a notice when it is practical to do so after the emergency situation has resolved. In addition, the Privacy Rule does not require that providers make a good faith effort to obtain the patient's written acknowledgment of receipt of the notice.

### Complaints about Privacy Violations

When a patient has a complaint about a violation of the privacy of his or her information, the first person he or she should talk to is the privacy officer at the facility where the incident occurred. If the complaint is not resolved, the patient should be directed to the office manager or physician. In the event the patient's issue has still not been resolved, he or she may file a written complaint, either on paper or electronically, with the Office for Civil Rights (OCR). The complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred. The OCR may waive the 180-day time limit if good cause is shown. Complaints must meet the following criteria:

- They must be filed in writing, either on paper or electronically.
- They must name the entity that is the subject of the complaint.
- They must describe the acts or omissions believed to be in violation of the Privacy Rule.
- They must be filed within 180 days of the incident.
- They must apply to an incident that occurred after April 14, 2003 (2004 for small health plans).

The OCR has 10 regional offices, each covering certain states. Complaints must be filed with the regional office that has jurisdiction over the state in which the incident occurred. A complaint form is available on the OCR Web site. The Office of the Inspector General (OIG) conducts investigations and audits when a question arises regarding privacy laws.

### HIPAA and EMERGENCY PREPAREDNESS

During major catastrophes and evacuations, healthcare providers face significant challenges in keeping their patients and staff members safe while providing continuity of their healthcare plans. Also, individuals with disabilities make the process more
difficult; sometimes the healthcare provider and the patient are the only two resources available to find a safe place for themselves.

Medical offices must have a safety evacuation plan that covers major disasters and allows healthcare professionals to be available in case they are needed at a disaster site. The best plans are developed by the actual site that will use them, so that they are customized for that particular facility, area, and its resources. For instance, if the medical office is next door to the hospital where the physician has staff privileges, transporting patients would be easier than if the hospital were several blocks away. For this reason, we suggest that the office staff discuss the problems that would be faced in an emergency and plan for the individual needs of both the staff and the patients. The patients' privacy is a primary factor during any emergency, so the plan must include contingencies for maintaining that privacy.

The office staff must be aware of the acceptable times to communicate with others about patient care, especially in emergency situations. Just because an emergency exists does not mean that the medical assistant is automatically free to release health information about the facility's patients.

CIRCUMSTANCES IN WHICH HEALTHCARE PROVIDERS MAY COMMUNICATE WITH FAMILY, FRIENDS, OR OTHERS INVOLVED IN A PATIENT'S CARE

- If the patient does not object, healthcare providers can communicate with family, friends, and others involved in the patient's care.
- If the patient is unconscious, healthcare providers may communicate with others if they feel it is in the patient's best interests; however, they may not share any personal information about past conditions unrelated to the current incident.
- The provider should obtain written permission from the patient to share information; however, this is not mandatory and not always practical.
- Healthcare providers must set their own rules for verifying requests for information (e.g., a driver's license must be shown before copies of a patient's records are discussed or provided) and for determining whether the individual is entitled to the information.
Guidelines for HIPAA Privacy Compliance

1. Consider that conversations occurring throughout the office could be overheard. The reception area and waiting room are often linked, and it is easy to hear the scheduling of appointments and exchange of confidential information. It is necessary to observe areas and maximize efforts to avoid unauthorized disclosures. Simple and affordable precautions include using privacy glass at the front desk and having conversations away from settings where other patients or visitors are present. Health care providers can move their dictation stations away from patient areas or wait until no patients are present before dictating. Phone conversations by providers in front of patients, even in emergency situations, should be avoided. Providers and staff must use their best professional judgment.

2. Be sure to check in the patient medical record and in the computer system to see if there are any special instructions for contacting the patient regarding scheduling or reporting test results. Follow these requests as agreed by the office.

3. Patient sign-in sheets are permissible, but limit the information requested when a patient signs in, and change it periodically during the day. A sign-in sheet must not contain information such as reason for visit because some providers specialize in treating patients with sensitive issues. Showing that a particular individual has an appointment with the physician may pose a breach of confidentiality.

4. Make sure patients sign a form acknowledging receipt of the NPP. The NPP allows the physician to release the patient’s confidential information for billing and other purposes. If the practice has other confidentiality statements and policies besides HIPAA mandates, these must be reviewed to ensure they meet HIPAA requirements.

5. Format policies for transferring and accepting outside PHI must address how the office keeps this information confidential. When using courier services, billing services, transcription services, or email, ensure that transferring PHI is done in a secure and compliant manner.

6. Computers are used for a variety of administrative functions, including scheduling, billing, and managing medical records. Computers typically are present at the reception area. Keep the computer screen turned so that viewing is restricted to authorized staff. Screen savers should be used to prevent unauthorized viewing or access. The computer should automatically log off the user after a period of being idle, requiring the staff member to reenter their password.

7. Keep usernames and passwords confidential, and change them often. Do not share this information. An authorized staff member such as the PO will have administrative access to reset passwords if they are lost or if someone discovers the password. Also, practice management software can track users and follow their activity. Do not ever give out a password. Safeguards include password protection for electronic data and storing paper records securely.

8. Safeguard the work area; do not place notes with confidential information in areas that are easy to view by nonstaff. Cleaning services will access the building usually after business hours; ensure that PHI is protected.

9. Place medical record charts face down at reception areas so the patient’s name is not exposed to other patients or visitors to the office. Also, when placing medical records on the floor of an examination room, turn the chart so that the identifying information faces the door. If medical record are kept on countertops or in receptacles, ensure that non-staff persons will not access the records. Handling and storing medical records will certainly change because of HIPAA guidelines.

10. Do not post the health care provider’s schedule in areas viewable by non-staff individuals. The schedules are often posted for professional staff convenience, but this may be a breach in patient confidentiality.

11. Fax machines should not be placed in patient examination rooms or in any reception area where non-staff persons may view incoming or sent documents. Only staff members should have access to the faxes.

12. Direct mail and phone calls only to the appropriate staff members.

13. Recognize, learn, and use HIPAA TCS if involved in coding and billing.

14. Send all privacy-related questions or concerns to the appropriate staff member.

15. Immediately report any suspected or known improper behavior to supervisors or the PO so that the issue may be documented and investigated.

16. Direct all questions to the supervisors or PO.

**FIGURE 17-8** Guidelines for HIPAA Privacy Compliance.

---

**CLOSING COMMENTS**

Every employee of the physician’s office must read the policy and procedures manual to make sure he or she clearly understands the HIPAA Privacy Rule and how it relates to the individual office (Figure 17-8). Medical assistants are responsible for learning and following the guidelines set forth by HIPAA. If they are uncertain about any situation, they should contact the office’s privacy officer for direction, or they should research the question on the HIPAA Web site. Never assume that a patient will not mind if certain information is disclosed. Always check the medical record to deter-
mine the patient’s preferences. Keep current on changes in HIPAA regulations. Embrace changes designed to improve patient care and treatment.

**Patient Education**

HIPAA regulations can be confusing to even seasoned medical professionals, so one can imagine the confusion that patients might feel when attempting to understand privacy regulations. Be patient when explaining the uses of health information in the medical facility. Take the time to review the information with the patient and use terms that the person will understand. The medical assistant should stress that the privacy regulations put the patient more in control of his or her health information. Remember to tell patients that they can change expressed preferences, if necessary, by completing a new privacy notification.

---

**Legal and Ethical Issues**

Any government regulation takes several readings to understand. One of the facility’s primary goals must be to remain in strict compliance, not only with HIPAA, but also with all laws and regulations that affect the medical office. The medical assistant may have to devote some study time to federal regulations to understand them adequately and be able to act on the provisions.

Patient confidentiality is one of the most important facets of medical practice, but some medical professionals feel that the information about the patient belongs only to the physician or the facility. The information about the patient belongs to the patient and must be disclosed, according to office policies, when the patient requests it. Never release medical information without a written release signed by the patient.

---

**SUMMARY OF SCENARIO**

Sabrina and Elsa will experience many challenges as a result of the information exchange they shared at the family picnic. Their conversation probably began like any other, but once Sabrina told Elsa the details of Ms. Adams’ visit, they violated patient privacy laws. Their future in the medical field is now uncertain.

Ms. Adams suffered emotionally after the breach of privacy. Her daughter, Terri, does not understand why her mother did not tell her about the illness. The relationship between the mother and daughter is now stressful, an interference with their normal bond during this critical time. The family questions whether to pursue the matter legally or spend the time they have left together in more productive ways. They have many decisions to make.

Dr. Taylor placed Sabrina on probation for 3 months. Before this incident, she had never received any type of disciplinary action. Elsa was not formally disciplined, largely because of her long-standing relationship with Dr. Barry. Still, there is sharp tension between them in the office now, as he faces a possible medical professional liability lawsuit and complaints about the privacy of Ms. Adams’ PHI. Neither Sabrina nor Elsa will look at her job the same as before the incident; everything is different. They both feel that they have disappointed their employers, their patients, and themselves.

The medical assistant must remember that patients should be discussed only with others who are directly involved in the patient’s medical care. The HIPAA Privacy Rule has made great strides in protecting patient privacy and in simplifying administrative processes. However, the rule is effective only if office policies are established and practiced. New policies may be difficult to implement, but gaining an understanding of the reason for the policy and its major goals can help the medical assistant embrace changes more readily.

---

**SUMMARY OF LEARNING OBJECTIVES**

1. Define, spell, and pronounce the terms listed in the vocabulary.

   Spelling and pronouncing medical terms correctly bolster the medical assistant’s credibility. Knowing the definition of these terms promotes confidence in communication with patients and co-workers.

2. Explain how the HIPAA Privacy Rule benefits the healthcare industry and patients.

   HIPAA’s Privacy Rule gives patients more control over their medical records. They are able to make informed choices on how their personal health information is used, and boundaries are set on the use and release of health records. Safeguards are established that healthcare providers must ensure to protect the privacy of health information. Violators are held accountable and face both civil and criminal penalties if a patient’s privacy rights are compromised. The Privacy Rule also protects public health by striking a balance when public responsibility supports disclosure of personal health information.

3. Explain the difference between Title I and Title II of the Privacy Rule.

   Title I of the Privacy Rule covers the insurance industry. It limits the use of pre-existing health conditions that in the past would have prevented an employee from obtaining health insurance coverage or limited the coverage. Title II deals with administrative simplification. This section is the source of the privacy and security laws that affect the patient. The goal of Title II is to reduce administrative costs in the healthcare industry.

4. List the rights of patients under the Privacy Rule.

   Patients have several rights under the Privacy Rule, including the right to notice of a facility’s privacy practices; the right to have access to, view, and obtain a copy of their personal health information; the right to restrict certain parts or uses of their PHI; the right to request that communications from the facility be kept confidential; the right to ask...
the facility to amend the PHI; and the right to receive notice of all disclosures of their PHI.

5. List the elements that must be included in a Notice of Privacy Practices.
   A Notice of Privacy Practices must include details on how PHI is used and disclosed by the facility; the duties of the provider to protect health information; the patient’s rights regarding PHI; how complaints can be filed if patients believe their privacy has been violated; whom to contact at the facility for more information; and the effective date of the Notice of Privacy Practices.

6. Briefly explain what is expected of healthcare providers under the Privacy Rule.
   Healthcare providers are expected to notify patients of their privacy rights; explain how their health information might be used; develop privacy procedures in the facility; implement those privacy procedures; train employees so that they understand the procedures in place; designate an individual to be responsible for implementation; and secure medical records so that they are not available to those who do not need them.

7. Describe an incidental disclosure.
   An incidental disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted.

8. List the three instances when a parent is not considered the child’s representative.
   A parent is not considered the child’s representative if: (1) the minor consents to care and the parent’s consent is not required under state or other applicable law (e.g., in the case of an emancipated minor); (2) the minor obtains care at the direction of a court or a person appointed by the court; or (3) the parent agrees to confidentiality between the minor and healthcare provider.

9. Explain the circumstances under which a provider may discuss protected health information with a patient’s friends and family.
   A provider may discuss PHI with a patient’s family or friends unless the patient has limited disclosure and has requested that he or she receive only confidential communication with the provider. Unless the patient makes this request, which should be in writing, the provider may discuss the patient with others as long as good judgment is used and the communication is related to the patient’s treatment.

10. Discuss the role of the Notice of Privacy Practices in emergencies.
    Healthcare providers and facilities (e.g., hospitals) with a direct treatment relationship with individuals are not required to provide their notices of privacy practices to patients at the time they provide emergency treatment. The HIPAA Privacy Rule requires only that providers give patients a privacy notice when it is practical to do so after the emergency situation has resolved.

CONNECTIONS

Study Guide Connection: Go to the Chapter 17 Study Guide. Read and complete the activities.

Evolve Connection: Go to Chapter 17 link at evolve.elsevier.com/ to complete the Chapter Review and Chapter Quiz. Penuse other resources listed for this chapter to increase your knowledge of Privacy in the Physician’s Office.