

The Cooper Health System

HIPAA COMPLIANCE TRAINING SELF-LEARNING MODULE

What's HIPAA?

In 1996 Congress passed a federal law entitled the Health Insurance Portability and Accountability Act, or "HIPAA" for short. There are three purposes for this law:

- I. It establishes a **uniform standard for processing electronic health care claims** in the United States. This will greatly reduce the cost of processing health care bills.
- II. It establishes new standards for protecting the **security of patient information**.
- III. It establishes new **privacy rules** that *all health care providers (as well as health plans and clearinghouses) must follow when handling patient information*. The privacy rules give patients greater control over how their health information is used. They also include specific changes in behavior that every member of a covered entity's workforce must adopt.

This training focuses on changes you will need to understand and follow to comply with the privacy rules.

Learning Objectives

The learning objectives of this program are:

- Review the main points of the new regulations
- Identify who must comply
- Discuss the legalities and their everyday applications in health care
- Illustrate strategies for compliance that Cooper associates must follow

Background

Why Do We Need A Privacy Rule?

HIPAA came about as a result of concerns from patients regarding breaches in confidentiality. For example, a hospital in Michigan accidentally posted the medical records of thousands of patients on the Internet. In a separate incident, a Nevada woman purchased a computer at an auction and later found the prescription records of patients were still in the computer's memory. These privacy violations are a source of concern to patients. Occasionally an unwanted release of medical record information can lead to a damaging experience for the patient. For instance, several years ago a congressional candidate complained after her campaign was derailed when newspapers published evidence of her having had prior psychiatric treatment following a suicide attempt. Confidential information was unnecessarily disclosed to others in each of these examples.

Facts:

- One out of every five Americans believes their health information is used inappropriately.
- One in six report that they have provided inaccurate information to their health care provider because they don't feel it will be kept confidential.

These stories are unfortunate examples of how trust has eroded in the health care system and of the critical need for a national effort to restore that trust. HIPAA seeks to eradicate all unnecessary

disclosures of private health information. It establishes the rule that patient information can be disclosed to persons responsible for providing direct treatment, to those responses for payment of health care and for purposes of health care operations. All other persons have no real need to know the information, and should not have access to the information.

To comply with the new law, greater efforts must be made to prevent private health information from falling into inappropriate hands. At Cooper this begins with individual behavior changes. Your contribution is required to yield positive changes for our patients.

Why are health providers affected?

Providers are a “covered entity” under HIPAA and are subject to the privacy regulation. HIPAA clearly defines both permitted and illegal behaviors and outlines the consequences of sharing patient information improperly.

One thing every associate must realize: HIPAA is a federal law, and compliance is not voluntary. It is mandatory. As an employee, staff member or volunteer at a health care facility, even if you work from home, *you must be aware of the laws and of your obligations in protecting the privacy of our patients.*

HIPAA General Information You Will Need To Know

A. Who is Covered?

Because you work or volunteer for a health care provider, you are subject to the rules. Health insurance plans and health care clearinghouses (organizations that process health care bills) are also covered. Essentially, HIPAA covers persons and organizations that provide, bill or pay for medical care.

B. When?

The regulations take effect April 14, 2003.

C. What Health Information is Covered?

Health information is defined as any information -- whether spoken, electronic or written -- that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. In other words, the law applies to information relating to a patient that is printed, discussed verbally, or is maintained in any form, such as electronic storage. As such, medical records, magnetic disks with patient information, and your learning at work that your neighbor is in the hospital with cancer—all are examples of health information that is protected under HIPAA and must be kept confidential.

Protected Health Information (or PHI) is health information created or received by a covered entity, regardless of form, that could be used to identify the individual patient. PHI includes both the demographic information about a patient (name, address, employer, etc.) and the medically related information (diagnosis, treatment, condition, etc). In other words, you can violate HIPAA’s confidentiality rules merely by inappropriately sharing patient names and addresses, even if no medical information about the patient is disclosed.

Example:

An employee contacts his wife at home saying, “Did you know our neighbor, Mary, is in the hospital?”

This violates Mary’s privacy—and HIPAA--unless the employee has permission from Mary to disclose the fact of her hospitalization to his wife.

D. When May PHI be Disclosed?

As a general rule, PHI may be used or disclosed, without a patient’s authorization, in the following circumstances:

- For treatment, payment and health care operations (TPO)
- For other purposes if the patient has authorized the disclosure
- For certain public and research purposes, even if the patient has not authorized the disclosure.

Examples of payment activities include such things billing and collections, utilization review, reviewing health care services for medical necessity, coverage, justification of charges, and determining eligibility or coverage.

Examples of health care operations include such things as quality assessment and improvement, credentialing and peer review, compliance, auditing services, business planning and development, legal services, training health care and non-health care professionals, accreditation, certification and licensing.

E. Uses and Disclosures

Generally, health care workers may use or disclose PHI to anyone who has a “**need to know**” the information for treatment, for processing a patient’s bill, or for purposes of health care operations. The “need to know” standard means you must have a need to know — **arising from your responsibility for caring for a patient or processing the patient’s claim** — in order to access information lawfully.

Health care workers may only share PHI with persons who *need to know* the information. Use of a patient’s information outside of these circumstances is unlawful under HIPAA. Additionally, health care workers must limit access to only those individuals who *need the information for a legitimate purpose*.

Examples:

- Hospital policy does not grant a housekeeper access to a patient’s medical records, but it does provide the charge nurse and nurse manager access to PHI of patients for whom they are responsible.
- A nurse should not access the X-ray results of a physician hospitalized on her floor just because she is curious. Unless one is responsible for a patient, one does not “need to know” this information. By accessing the physician’s records, the nurse is reviewing private medical information for personal or malicious purposes. This is a violation of HIPAA regulations, and the nurse could be suspended or terminated for this activity.

Incidental Disclosures. Many Cooper associates may become concerned about violating HIPAA even though they have done everything reasonable to avoid it. For instance, sometimes a patient overhears a conversation because it occurs in a crowded treatment area. This type of disclosure is an “incidental disclosure.” It is a disclosure that cannot be reasonably prevented, is limited in

nature, and occurs as a by-product of otherwise permitted use or disclosure. **Incidental disclosures do not violate HIPAA.**

Examples:

- Though a physician is exercising discretion in talking to a patient in a semi-private, emergency treatment room, a patient in the next bed overhears a patient's conversation with a doctor.

This would be an incidental disclosure because it could not be reasonably prevented. HIPAA does not require that the hospitals erect new walls. It does require that preventable disclosures of information be avoided.

- A patient walking down the hallway accidentally hears part of a loud telephone conversation that takes place while a physician is on the phone with a patient.

The incidental exposure exception does not apply in this instance because there is a failure to follow reasonable safeguards to prevent the occurrence. ***It is unreasonable to discuss patient information in public areas without using discretion.*** The physician must shield the information from disclosure. Speaking loudly is readily preventable.

- A receptionist always uses a sign-in sheet with the patient's name and test to be done. Patients registering for services see the names of other patients that have registered and the test that was requested.

This is not an incidental disclosure because it was foreseeable that others could review protected health information. Sign-in sheets are permissible, but they should only indicate the patient's name and the time of arrival, not the patient's condition or reason for visit.

Minimum Necessary Rule. Under the regulations, any PHI that is shared with persons who are not engaged in active treatment of a patient should be limited to the **minimum necessary**. The receiver of PHI must "need to know" the information. Otherwise, the information should not be given out. For instance, if it is your responsibility to report a suspected case of child abuse to the Department of Youth and Family Services (DYFS), you may not provide DYFS with a complete copy of the medical record. This amount of disclosure is generally not necessary to adequately report child abuse. Only the information that DYFS needs to know should be disclosed, such as the dates the child was admitted or treated at the hospital, the nature of the injuries, and the relevant information as to why the abuse was suspected.

<p>The minimum necessary rule <u>does not apply</u> to the sharing of medical information for treatment purposes. Physicians, nurses, and other health care providers need full access to medical records and medical information regarding their patients in order to provide the best possible care.</p>

Business Associates. Cooper is permitted to disclose PHI to business associates who perform certain key functions for Cooper. Business associates must provide written assurances that they will safeguard and protect PHI. Examples of business associates are: billing companies, accountants, and accreditation agencies.

F. Cooper as an Academic Medical Center

Since Cooper is an academic medical center, many students, residents, and other trainees will spend time at Cooper in the course of their training. While at Cooper, these individuals are

considered members of the Cooper workforce and are permitted to use and disclose PHI to the same extent as any other employee.

G. Penalties

HIPAA is serious about patient privacy. Anyone who obtains or discloses PHI for personal or commercial gain or for malicious purposes is subject to sanctions, and disciplinary action, such as suspension, termination, criminal and civil penalties. The following government fines are applicable when HIPAA is violated:

- Failure to comply with regulations: Where there is failure to follow a procedure or practice designed to protect PHI from unlawful disclosure, complaints may lead to fines. Each violation of a patient's privacy may lead to a fine of \$100.
- Wrongful disclosure of information: If a person gives a patient's information to the media or other parties maliciously, penalties are substantially higher, civil fines up to \$50,000 and/or criminal penalties of up to one (1) year in prison.
- Obtaining patient information under false pretenses: \$100,000 and/or imprisonment for up to five (5) years.
- Intent to sell patient information: \$250,000 and/or up to 10 years in prison.

Under no circumstances should a Cooper associate use sell or otherwise share patient information for purposes unrelated to treatment payment or health care operations. Such unlawful disclosures may lead to personal liability dismissal and prosecution.

Patient Rights

HIPAA creates new rights for patients. As an associate, you must become aware of the patient's rights, as well as your role in the process.

Notice of Privacy Practices and Patient Rights

Patients must be given a clear written explanation of how Cooper uses and discloses health information. This document is referred to as the Notice of Privacy Practices (NPP). The NPP includes a summary of the patient's HIPAA rights.

Cooper's NPP will be presented to the patient at registration or the first time a patient is treated at a Cooper facility or physician office. The patient must sign a NPP acknowledgement. All Cooper associates responsible for registering patients must make a good faith effort to obtain a signed acknowledgment that the patient has received a NPP. The NPP needs to be signed just once, and patients do not have to re-sign an acknowledgment each time they present for treatment.

Example:

- If a patient comes to an appointment with a physician at the Surgery Center, the receptionist would request the patient to read and sign an acknowledgment of having received the NPP. If the patient has previously received a NPP at Cooper and so indicates that fact, there is no need to give the patient another copy of the NPP. Simply note that the patient previously received one.

Treatment should never be withheld if the patient refuses to sign the NPP. However, you should document the patient's refusal as evidence of your good faith attempt to obtain a signature.

In emergency situations, the patient may sign the NPP after the emergency is addressed and the patient is stable.

Facility Directory Rights

A. Hospital Directories

Any time a patient enters a Cooper facility, information about that patient can be retrieved from Cooper's computer system for directory purposes to determine whether a patient is in the hospital and where the patient is located. HIPAA includes new rules affecting directories:

- Every patient will be given notice that his/her name and location will be listed in the hospital's directory. Every patient is also given the right to opt-out of being listed in the directory.
- Every patient must also be given the opportunity to have his/her name excluded from the list of people given to the clergy.
- *If the patient opts out of the hospital's directory, anyone inquiring about the patient on the unit, at the visitor's desk, or when calling must be told that the facility does not have information on that patient.* It is not permissible to disclose that a person is in the hospital when the patient has requested that information not be disclosed.
- For patients who have not opted-out of the directory, the patient's location in the hospital may be given to a caller who asks for that patient by name.
- When a patient is unable to express a preference regarding the directory, their name generally will be included in the directory, unless professional judgment dictates that a person's identity be kept confidential. For example, it would be prudent to protect the identity of a gun-related shooting victim who is unconscious. Because of the nature of the injury, this patient may attract greater media attention.
- Exception: Patient identities can be disclosed to entities providing relief in disasters, such as the Red Cross, during fires, floods, or terrorist attacks.

B. Sign-in Sheets

When dealing with sign-in sheets, it is a Cooper requirement that only the patient's name and time of arrival or appointment is requested. Private medical information, such as the reason for the visit, may not be listed where other patients can review it. If clinical information is needed, replace sign-in sheets with cards or forms that are filled out by the patient and removed from view of the public after they are completed.

C. Clergy/Other Religious Personnel

Clergy have a right to obtain the list of patients with the same religious affiliation so long as that list does not include patients who requested that their names not be provided to clergy. If a patient wants visitation, clergy may receive the patients' name and location. Please note that associates are not permitted to discuss a patient's condition with clergy without first obtaining permission from the patient.

Sharing Information with Caregivers and Family

Patients have a right under HIPAA to control who will get their information. Each associate must exercise great discretion in disclosing information to family members, relatives and close friends assisting with the care of the individual. Associates must know the patient's wishes *prior to sharing PHI with other persons*. If you don't know the patient's wishes, *only general information regarding the condition of a patient may be disclosed*.

General information may be given to persons who ask using the patient's name. However, in response to those requests, associates may only give the general condition (*e.g.*, good, fair, serious, critical) and location in the facility (*e.g.*, North 1015 Door).

HIPAA puts patients in control of their health information. HIPAA requires that PHI be shielded from inappropriate use and disclosure. Aside from being used for TPO, health information may be given only to persons identified by the patient or by the patient's guardian as appropriate recipients, or as otherwise authorized by the patient. Thus, Cooper associates need to know the patient's individual preferences before information is shared.

Example:

- A caller asks, "My mother is having a test at 2 p.m. What is that test?" This question could not be answered without first obtaining the patient's permission to discuss the information requested.
- A visitor states that his wife, Sally Smith, is in bed 715W and asks, "How is she doing?" Unless you know the identity of the visitor *and* also that the patient has given permission for the visitor to receive PHI, only the patient's general condition (good, fair, serious, critical) may be disclosed to the visitor.
- A caller calls to get an update regarding his brother. He does not have a password.

The associate could obtain the caller's telephone number and provide it to the patient. Alternately, the patient's permission to speak with the caller could be obtained.

Discretion should be exercised here. It is always better to verify the number of the caller with the patient and return the call or have the patient verify the identity of the caller's voice. This assures that information is not given to the wrong person.

- An unconscious patient is admitted to the ICU. No one is able to reach family members. You learn that the police have been notified and they are seeking relatives. A caller telephones indicating he is a relative.

Except in an emergency, only general information should be disclosed to the caller. Only the information necessary to identify guardians should be disclosed. Patient information may be disclosed in order to verify the caller's relationship with the patient and to obtain emergency information.

Remember that as a health care associate, anytime you share information with those involved in the patient's care, you still need to be sure that the disclosure follows the wishes of the patient, and that the information you disclose is relevant to the person to whom you are disclosing. ***If ever in doubt, always ask the patient for permission to discuss their medical care with others, especially sensitive information.***

Example:

- A patient's lab test comes back positive for a sexually transmitted disease. You are about to administer an antibiotic shot for this. When you go to administer the shot, his spouse and children are present in the room.

It would be best to first discuss this treatment with only the patient in the room. The patient may have questions you may need to discuss.

The Press

Calls from members of the press regarding a particular patient's condition will be handled like any other call. Only information about the patient's general condition (good, fair, serious, critical) may be released – as long as the patient has not requested that his/her name not be listed in the patient directory.

Requests for Restrictions on the Use and Disclosure of their PHI

Patients may request that Cooper restrict the use and disclosure of their PHI regarding TPO to certain people and may request that certain people do not receive any information about their TPO. Patients may also request that any communications from Cooper be made to them at a specific location (at work rather than at home, for example). Members of the Cooper workforce must honor any requests to which Cooper has agreed.

Example:

- A patient requests that Cooper not disclose any information about the current hospitalization to his/her adult children.

Assuming that Cooper has agreed to this request, if the patient's children ask about their mother's condition, no information about the mother's condition may be given.

Preventing Disclosure and Safeguarding PHI

Outside of Work – Zip it! The patient information you learn as a Cooper associate is confidential and should never be discussed outside of work.

Conversations – Whisper it! Patient information should be shielded from disclosure. With conversations, often whispering in treatment areas is enough.

Viewing Records – Cover it! Protecting bedside chart information, supervising medical charts, protecting x-rays, protecting computer screen information, etc.; the responsibility lies with each associate to shield this information from unnecessary disclosure. Specific procedures for how Cooper expects these safeguards to be implemented will be communicated by your supervisor.

Disposal of Records – Secure it! All PHI trash is to be disposed of in the locked trashcans or shredded. If your work location is not the hospital, check with your manager regarding how trash should be disposed of or shredded so that PHI is kept confidential.

Giving PHI on the Telephone or Via Fax – Verify it! Before providing PHI to a physician or other caregiver by fax or on the telephone, make reasonable efforts to verify the identity of the person requesting the PHI.

Access to Records

Patients have the right to access their medical records in order to view and copy information that is used to make decisions about them. Cooper will follow its present policy regarding hospital chart access. Hospitals can deny access to the records if the access would endanger the life or safety of the patient or

another person; if access could lead to domestic violence or abuse; or if the information was obtained under a promise of confidentiality.

Amendment Rights

Patients have the right to request an amendment of information in their medical records. These requests may arise when the patient believes that the medical record is incorrect. However, if Cooper believes the information is correct, the organization can deny the patient's request. **All medical information amendment requests must be made in writing to the Director of Health Information Management at Cooper. No employee or physician should alter the record following a patient's request.**

Authorization Rights

Patients most give Cooper written authorization before certain information is released. An authorization form is required before Cooper may release medical information for most non-health care purposes. Examples of these releases include responding to school requests, responding to inquiries from a patient's employer, and responding to life insurance claim reviewers.

NOTE: There is a difference between an authorization and a consent to receive treatment (*e.g.* surgical consent). Under HIPAA an authorization is required when patient information is disclosed for purposes unrelated to providing treatment payment or health care operations. For instance the release of medical records to an attorney requires an authorization. The attorney is not involved in treatment, payment, or health care operations.

There are strict rules related to obtaining authorizations from patients:

- ✓ **Authorization forms must be completed in full.** Every line must be completed.
- ✓ **Authorizations allow patients to request reasonable restrictions** on the disclosures of their information. A patient may request that only portions of the record be disclosed. For example, a woman may not want a pregnancy test result released to her employer.
- ✓ **Cooper may choose whether or not to agree with requested restrictions.** All such restrictions must be carefully documented in the authorization.
- ✓ **Care or payment cannot be denied to a patient who refuses to sign an authorization form.** Authorization is voluntary, and patients can revoke an authorization at any time. A patient cannot be forced to sign an authorization as a condition of receiving required treatment.
- ✓ **No authorization is needed where the release of information is needed for public policy purposes** such as releasing the patient's information for public health care activities; law enforcement purposes, to report health care fraud; laws requiring the production of information; or the donation of organs and tissue.
- ✓ **A copy of the signed authorization form must be given to the patient** if the covered entity seeks an authorization from an individual for the use or disclosure of protected health information.

Highly Confidential Information. Some health information is considered highly confidential and is specially protected under Federal and/or New Jersey law. Cooper is generally not permitted to disclose this highly confidential information without a patient's authorization.

Highly confidential information includes the following:

- (a) HIV-related information

- (b) Behavioral or mental health treatment
- (c) Substance abuse treatment
- (d) Genetic information
- (e) Tuberculosis information

In these circumstances, contact medical records or your manager before information is released.

Accounting For Disclosures

As noted above, a health care worker can disclose information to persons who need to know the information for purposes of TPO. By contrast, there are other situations that require the reporting of PHI to third parties. Because state and/or federal law mandate these reports, the patient's permission is not necessary. Examples include reporting communicable diseases, reporting child abuse, reporting gun shot wounds, and reporting elder abuse or neglect. These reports are not for TPO, but they are required by law and are permitted disclosures.

The state and other regulatory bodies require the release of PHI in the course of audits, investigations, facility inspections, civil or criminal investigations, and investigation of civil rights violations. Again, law or regulations require participation in these programs.

Because these disclosures are not related to TPO and because they are made without patient authorization, the release of this information must be logged in an accounting of disclosure form. Cooper associates must record every instance of disclosure of PHI when it is not related to the treatment of the patient processing a claim for payment or health care operations. An online database is being prepared at Cooper to make this process easier.

Example:

- Although reporting the names of patients newly diagnosed with HIV diagnoses is a mandated public health requirement, providing PHI to the state health department is not related to treating the patient, processing the patient's insurance claim, or internal Cooper operations. Consequently, this disclosure must be recorded in an accounting of disclosures.

Examples of disclosures that **Do** and **Do Not** need to be recorded are listed in separate tables below:

DO RECORD These Disclosures

- | | |
|---|--|
| <ul style="list-style-type: none"> • To public health authorities; i.e., NJDHSS • Birth and death reporting • To law enforcement regarding crime on premises • To law enforcement in emergencies where crime is suspected • For cadaveric organ, eye, tissue donation purposes • For judicial and administrative proceedings • For research with an IRB waiver • To military command authorities • Tumor Registry reports • For workers compensation reports • To correctional institutions • About decedents to medical examiners, funeral directors, coroners • For public health activities • About victims of abuse • Implantable device registrations sent to manufacturers | <ul style="list-style-type: none"> • Regarding child abuse or neglect • To the FDA (adverse events) • To the FDA (product defects or biological product deviations) • To the FDA (for product recalls, or lookback studies) • To the FDA (for post marketing surveillance) • To a person who may have been exposed to a communicable disease • To health oversight agencies for audits, civil or criminal investigations, inspections, licensure or disciplinary actions • In response to a court order • In response to a subpoena or discovery request • As required by law for wound or injury reporting • For identification & locating a suspect or fugitive |
|---|--|

Disclosures That DO NOT Need To Be Logged

- | |
|--|
| <ul style="list-style-type: none"> ➤ Disclosures for treatment, payment, or health care operations ➤ Disclosures that have been authorized by the patient in a written authorization form ➤ Disclosures made directly to the patient ➤ Incidental disclosures ➤ Disclosures as part of a limited data set ➤ Limited disclosures to/from patient directory ➤ Disclosures made to individuals involved in patient's care (family, friends) ➤ Disclosures for national security purposes; i.e., counter-intelligence ➤ Disclosures for protective services of the President, or for security clearance ➤ Disclosures to correctional institution or law enforcement, if patient is in custody |
|--|

Complaint Rights

Patients have recourse if their rights are violated. If a patient feels his information was shared inappropriately, he has the right to file a formal complaint with either one of the following:

- The Chief Privacy Officer, One Cooper Plaza, Camden, NJ 08103-1489, or with
- The U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C. 20201

A complaint must be filed within 180 days of the patient knowing of the act, and a record must be kept of the complaint and how it is resolved.

All complaints will be handled confidentially.

HIPAA Self Learning Module Post Test

1. T/F. A receptionist always leaves the window open to the waiting room while she converses with patients on the phone. Patients in the waiting room overhear these conversations. This is an example of Incidental Disclosure.
2. T/F. Providing the “minimum necessary” information does not apply to the sharing of medical records amongst physicians, nurses, and other health care providers for treatment purposes.
3. The following can be said about authorizations:
 - A. Patients must give authorization before certain information is released
 - B. A health care facility can deny treatment to a patient that does not sign an authorization form
 - C. Authorization is needed to release information for public policy purposes such as public health care activities or law enforcement purposes
 - D. All of the above
4. Which one of the following would **NOT** be considered a covered entity under HIPAA?
 - A. Hospital information desk personnel
 - B. Clergy visiting patients in the hospital
 - C. Doctor’s office staff
 - D. Health insurance companies
5. T/F. At Cooper Hospital, PHI that must be disposed of may be placed in regular trash receptacles.
6. T/F. Contacting the Sharing Network program about a potential organ donor would need to be recorded on an “accounting of disclosure” form.
7. You are the Unit Clerk on a busy hospital unit. Someone calls and says, “Hi! I’m John Smith and I work with your patient, Susan Jones. I need to know when she will be discharged so we can arrange for temporary help at the office until her return.” You know that Ms. Jones is listed in the patient directory. Which one of the following responses by you would **NOT** be appropriate?
 - A. “Let me check her chart. Oh. I see that the doctor plans for her discharge on Friday.”
 - B. “I do not have that information. Let me transfer your call to Ms. Jones’ phone so you can speak directly to her.”
 - C. “I am sorry, but in order to protect her privacy, I am not authorized to provide that information.”
 - D. “If I can have your name and number, I would be happy to let Ms. Jones know you called so that she can return your call.”
8. All of the following would be considered Protected Health Information (PHI) **EXCEPT**:
 - A. X-ray films
 - B. Telling an unknown visitor to wait until the patient finishes his respiratory treatment
 - C. Looking up an employee’s birthday on the information system
 - D. The patient’s name on a sign-in sheet for outpatient testing
9. One nurse asks her co-worker to see one of her assigned patients to confirm the presence of a heart murmur. This would be considered:
 - A. No violation of HIPAA regulations
 - B. An incidental disclosure
 - C. An impermissible disclosure

PLEASE COMPLETE – TRAINING CERTIFICATE

HIPAA Privacy Training Certificate

This certifies that I have completed the Cooper Health System (CHS) compliance training for associates to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

I understand and agree that it is my responsibility to maintain confidentiality for all patients using services at CHS. I understand that protecting the confidentiality of patient information includes protecting both the patient's personal identity and the patient's health related information.

I understand that any use, sale, barter, or disclosure of confidential patient information for purposes outside of the scope of my employment at CHS is prohibited, and that such disclosures may also be in violation of state and/or federal law. Violating confidentiality outside of the scope of my employment may lead to loss of employment and potential personal liability for civil or criminal penalties.

I further understand that disclosure of patient information necessary for purposes of treatment, payment for services, or health care operations is permissible. When making. Such disclosures of patient information, I must limit disclosure to the minimum necessary information to accomplish the task required.

Print Associate Name

Dept.

Campus/Location

Associate Signature

/ /
Date

Return completed form to:

Rose M. Rossiter

Office of the Registrar

UMDNJ/Robert Wood Johnson Medical School

401 Haddon Avenue, Suite 154

Camden, NJ 08103