Complying with HIPAA

Lessons covered:

- Introduction
- Using and Disclosing PHI
- Rights of Individuals
- Securing PHI
- Enforcement and Breach Notification

Introduction

Real People, Real Stories

When you visit the doctor’s office, you trust that the information you provide will remain private and secure. You expect that as your medical records pass through the hands of dozens of employees—from registration to clinical staff to billing—only those with a legitimate need to know will access and use your information and that the integrity, availability, and confidentiality is secured at every step.

Our patients and clients trust that we will treat their information with the same care. But sometimes employee carelessness or misguided intentions keep this from happening. Check out what can happen when an individual's health information isn't properly protected:

Medical Identity Theft

Recently, I received an Explanation of Benefits statement containing charges for services I did not receive.

- It turns out that someone had accessed my health information and used my insurance to pay for repeated office visits and treatments. It's going to take months to fix this!

Criminal Snoop

Rumor had it that a celebrity visited the Emergency Room in critical condition! Curiosity got the best of me and I peeked into the ER files to see who it was and what happened. I got excited and spread the gossip around.

- It turns out that snooping can be a criminal offense – shortly after, I was fired, and the hospital was fined $250,000 for violating HIPAA. Even worse, I could go to jail!

Fax Number Mishap

It was a hectic day and I needed to fax some medical billing information to a client. In a rush, I typed in the wrong fax number and sent the information to the wrong recipient.

- Apparently, the fax contained health information and my simple mistake was the cause of a privacy breach and violated HIPAA.

HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) grants individuals the ability to access their Protected Health Information (PHI) along with certain other rights. It also requires our organization to establish policies and processes that ensure patients' PHI is protected and secure.

We follow HIPAA regulations because they're the law, but more so because they protect our patients and customers, giving them legal rights on who can access and use their PHI.

In this course, you'll learn more about how you can protect our patients—and our organization—by following HIPAA regulations.

Course Objectives

Upon completing this course, you will be able to:

- Recognize the importance of HIPAA to individuals and our organization.
- Define the rights of individuals and your responsibility to ensure these rights are granted.
- Identify examples of PHI and how to protect its confidentiality when using and disclosing it.
- Recognize the consequences for non-compliant behaviors.
- Identify your responsibilities for reporting privacy and security incidents.

Protected Health Information (PHI)

Protected Health Information (PHI) is any information that can be used alone or in combination with other information to identify an individual who is receiving healthcare services. HIPAA regulations apply to all PHI, regardless of how it is communicated—whether it is shared verbally, in writing, or through electronic methods.

PHI is data in healthcare records, demographic information, payment information, insurance claims – the list is endless, so you must be careful and mindful when accessing, using or disclosing information.

Help! What is PHI?

- Names of patients and relatives
- Postal addresses
- Dates
- Telephone and fax numbers
- Email addresses
- Social Security Numbers
- Medical Record Numbers
- Account numbers
- Health plan beneficiary numbers
- Certification/license numbers
- Automobile VIN and serial numbers
- Device identifiers and serial numbers
- URLs and IP addresses
- Biometric identifiers
- Photographic images
- Video recordings
- Voice recordings

Your Responsibility

Everyone at our organization must comply with HIPAA regulations. Including our vendors who handle any type of PHI to perform their services for us.

PHI you obtain in the workplace may only be shared with others within the organization when needed for them to perform their duties.

By following HIPAA regulations, you support our organization's commitment to ensuring the security and privacy of PHI. By providing high quality services that safeguard PHI, you also protect our reputation, and help us avoid costly penalties, legal sanctions, and litigation fees for violating the law.

Knowledge Check

Now you'll have a chance to help employees comply with HIPAA in the workplace. Review the following scenarios and determine the best action to take for each situation.

Scenario 1

Employee 1: "I'm worried about being liable for protecting PHI."
Employee 2: "Oh, don't worry! We don't really have to worry about HIPAA compliance, our managers handle that stuff."

Is this accurate information:

- Yes, only those employees who directly handle PHI need to comply with HIPAA.
- No, everyone, regardless of your role, needs to know and comply with HIPAA.

Scenario 2

Employee: "Oh my gosh! You won't believe who just had surgery here!"

Can this employee share this information?

- Yes, this is general information and not PHI.
- No, this is PHI and it is against HIPAA to share.

Scenario 3

Employee: "Hmm, I wonder if I need to keep this patient billing information secure…"

Does the employee need to protect this information?

- Yes, these records contain PHI.
- Yes, but only from people outside of their workplace.
- No, the information in these records is not confidential.

Knowledge Check Answer Key

Scenario 1: No is Correct. All employees are obligated to comply with HIPAA and our organization's Information Security and Privacy policies and procedures.

Scenario 2: No is Correct. Any information pertaining to the healthcare of an individual is PHI and cannot be shared or accessed unless there is an authorized business need to know.

Scenario 3: Yes, these records contain PHI is Correct. Medical claim forms, patient contact information, healthcare billing statements and explanation of benefits forms all contain PHI and need to be safeguarded from anyone who does not need them to perform their duties.

Summary

You have completed this lesson providing an overview of HIPAA. Here are the key points covered:

- HIPAA requires us to keep patients' information secure and private.
- PHI is information that can be used alone or in combination with other information to identify an individual.
- HIPAA regulations apply to all PHI, regardless of the method in which it is stored or communicated.
- Everyone is responsible for complying with HIPAA regulations and our organization's Information Security and Privacy policies and procedures—even if your job duties do not directly include working with PHI.

Using and Disclosing PHI

HIPAA Privacy Rule

HIPAA defines the permitted uses and disclosures of PHI. The HIPAA Privacy Rule states that PHI can only be used and disclosed to the minimum necessary for Treatment, Payment, and Healthcare Operations purposes. The minimum necessary standard requires us to evaluate our practices and enhance safeguards as necessary to:

- Limit unauthorized or inappropriate access to PHI.
- Limit unauthorized disclosures of PHI.

Take a moment to learn more about the allowable purposes for sharing PHI in Treatment, Payment, and Healthcare Operations purposes.

Treatment

Treatment activities include:

- The provision, coordination, or management of healthcare and related services among healthcare providers or by a healthcare provider and a third party.
- Consultation between healthcare providers regarding a patient.
- Referral of a patient from one healthcare provider to another.

Payment

Payment activities include:

- Determining eligibility or coverage under a healthcare plan and adjudication claims.
- Risk adjustments.
- Billing and collection activities.
- Reviewing healthcare services for medical necessity, coverage, justification of charges, etc.
- Utilization review activities.

Healthcare Operations

Healthcare Operations activities include:

- Quality assessment and improvement activities.
- Underwriting and other activities related to creating, renewing, and replacing health insurance or benefits contracts.
- Medical review, legal, and auditing services.
- Business planning and development.
- Business management and general administrative activities.

Use, Disclosure, and Request

The HIPAA Privacy Rule also regulates the use, disclosure, and request of PHI. Take a moment to learn more about how these terms apply to your job functions.

Use Refers to activities conducted in routine business activities. Only those involved in the treatment, payment, or operations may share, apply, utilize, examine or analyze PHI.

Disclosure Refers to how PHI is shared between departments or outside of our organization. It includes the release, transfer, access, or divulgence of PHI. Disclosing PHI may be necessary for operational purposes but is subject to certain limitations.

Request Refers to any situation where an individual of our organization requests and/or is requested to disclose PHI to an outside entity. Requests for PHI may be necessary for operational purposes, but are subject to certain limitations.

Types of Disclosures

It is critical to understand the limitations around disclosing PHI. Most disclosures fall into the following categories:

- Permitted disclosures for Treatment, Payment, and Healthcare Operations.
- Disclosures following an “Opportunity to Object.”
- Disclosures required by law.
- Disclosures requiring authorization.

Take a moment to learn more about these types of disclosures by reviewing the examples provided.

Permitted Disclosure for Treatment

"Another healthcare provider's office called and wanted a patient's PHI for an upcoming appointment. Is this OK?"

- You can share information with other healthcare providers, pharmacies, labs, etc who are involved in the patient's care.

Permitted Disclosure for Payment

"I need to share a patient's PHI with their insurance company for billing purposes. Is this OK?"

- You can share information with the patient's health plan in order to obtain payment for the services provided.

Permitted Disclosure for Healthcare Operations

"The Quality Management department is requesting PHI to followup on a complaint. Is this OK?"

- You can share information internally for healthcare operations without any additional authorization.

Disclosures Following an Opportunity to Object

"A family member is requesting information on a patient. Since they're family, I can go ahead and share this."

- Sharing information with a patient's family and friends—or including a patient in the facility directory—can occur only after the patient has been given an opportunity to object or "opt-out" of these types of disclosures.

Disclosures Required by Law

"I received a subpoena for PHI provided by our customer, so I can disclose this information."

- We are legally required to disclose information in certain situations, being subpoenaed is one of them. Always follow our organization's policies for handling this type of disclosure.

Disclosures Requiring Authorization

"One of our employees was admitted to your facility this morning. How is he doing?"

- Disclosing PHI to a patient's employer without proper authorization is illegal. All disclosures not related to the patient's treatment, payment for the treatment, and healthcare operations require authorization—except for requests required by law.

Knowledge Check

Now you'll have a chance to help employees properly use and disclose PHI. Review the following scenarios and determine the best action to take for each situation.

Scenario 1

Manager: "I heard a rumor that one of my employees was hospitalized for substance abuse, which may affect his work eligibility. What was he admitted for?"

Nurse: "Hmm…let me check."

Does releasing patient information to an employer without authorization violate HIPAA?

- Yes, authorization is required before disclosing PHI to a patient's employer.
- No, releasing PHI to a patient's employer is permitted if it could affect his workplace status.

Scenario 2

Patient: "Do I need to call the insurance company myself to provide my information? It would be great if you would call them for me!"

Employee: "No, Mrs. Jenkins. Our staff will take care of that for you."

Is this correct?

Scenario 3

Front desk receptionist: "Eww. What a gnarly fracture!"

Is this employee violating HIPAA by viewing the x-ray?

- Yes, they have no business need to view a patient's x-ray.
- No, viewing an x-ray does not violate HIPAA.

Knowledge Check Answer Key

Scenario 1: Yes is Correct. Disclosing PHI to a patient's employer—or even looking at the patient's file—is not permitted without proper authorization.

Scenario 2: No is Correct. A covered entity can share information with other providers, pharmacies, labs, etc., involved in the patient's care or to the patient's health plan to obtain payment.

Scenario 3: Yes is Correct. The receptionist does not have a business need to view this PHI. Accessing, using, or disclosing PHI without authorization from the patient violates HIPAA regulations.

Summary

You have completed this lesson on using and disclosing PHI. Here are the key points covered:

- PHI can be used or disclosed to the minimum necessary for treatment, payment, and operations purposes.
- Only those involved in the treatment, payment, or operations may share, apply, utilize, examine, or analyze PHI.
- Most disclosures require authorization.

Rights of Individuals

Notice of Privacy Practices

HIPAA regulations are based on requirements and standards concerning individuals' rights to their PHI. That's why our organization provides every patient with a Notice of Privacy Practices.

This notice must be provided to patients the first time they present for service, whether it is in person, over the phone, or through electronic means. A copy of this notice must also be available at every service location for patients to review.

The Notice of Privacy Practices describes how a patient's PHI may be used or disclosed, as well as the rights the patient has regarding that information. You have an ethical and legal responsibility to ensure individual's rights to their PHI are granted as outlined in the Notice of Privacy Practices. Let's take a closer look at these rights.

Rights of Individuals

Individuals have a right to:

- Inspect and request a copy of their PHI.
- Amend their PHI.
- Request an accounting of all PHI disclosures—note that some exceptions apply.
- Request confidential communications of their PHI by alternative means.
- Request restrictions on uses and disclosures of their PHI.
- Obtain a paper copy of the Notice of Privacy Practices.
- File a complaint regarding the privacy and security of their PHI.

Handling Requests

You protect individuals' rights by handling requests appropriately, obtaining authorization for use and disclosure when necessary, and processing complaints in accordance with our policies. In general, all requests should be referred to the appropriate person within our organization.

Take a moment to explore examples of requests and the procedures for handling these requests at EvergreenHealth.

Right to File a Complaint

"I think my PHI has been disclosed illegally."

Your Responsibilities

In this situation, you should:

- Inform the individual of his right to file a compliant if he suspects his privacy rights have been violated.
- Refer the complaint to the Privacy Officer.

Request to Amend Record

"The information in my health record is not correct."

Your Responsibilities

In this situation, you should:

- Explain that the patient has a right to request an amendment, and it's the provider's decision whether to accommodate the request.
- Refer the request to the HIM Operations Manager.

Written Authorization
"I need some patient information for marketing purposes."

Your Responsibilities
In this situation, you should:

- Explain that using or disclosing PHI for marketing purposes is not allowed under HIPAA without patient authorization.
- Explain that we would need to obtain written authorization from the patient to use or disclose their information before fulfilling this request.

Request to Limit Access
"I'd like to limit who has access to my medical information."

Your Responsibilities
In this situation, you should:

- Inform the individual that he has a right to request a restriction or limitation on the PHI we use or disclose for certain specified reasons.
- Refer the request to the HIM Operations Manager. Note that our organization is not required to agree to the restriction request in most instances.

Knowledge Check

Now you'll have a chance to help employees ensure that individual's rights are respected. Review the following scenarios and determine the best action to take for each situation.

Scenario 1

Voice on telephone: "… and I know that I did not authorize you to share my information! I can't believe this is happening to me …"

What should this employee do to process this patient complaint?

- Reassure the patient that her situation will be resolved immediately.
- Transfer the call to his manager.
- Refer the complaint to the appropriate person within our organization.

Scenario 2

Employee: “I need medical information on the following patients in order to process insurance claims.”

Does this request for information comply with HIPAA regulations?

- Yes, requesting information associated with the payment for healthcare is allowed.
- No, only medical and legal requests for PHI are compliant with HIPAA regulations.

Answer Key

Scenario 1: Refer the complaint is Correct. All complaints of this nature should be referred to the appropriate person within our organization. In most situations, this will be our Privacy Officer.

Scenario 2: Yes is Correct. Requests made for PHI that deal with obtaining payment comply with HIPAA regulations.

Summary

You have completed this lesson on individuals' rights to their PHI. Here are the key points covered:

- The Notice of Privacy Practices describes how patients' PHI may be used or disclosed, as well as the rights patients have regarding that information.
- It’s your responsibility to ensure individuals’ rights to their PHI are granted as outlined in the Notice of Privacy Practices.
- Individuals have a right to make requests and file complaints regarding the use of their PHI, and you must ensure requests and complaints are directed to the appropriate person.

Securing PHI

HIPAA regulations define the standards required for securing PHI.

Our organization must maintain reasonable administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI. All employees are required to adhere to these safeguards to ensure that all PHI, regardless of its form (e.g., paper, electronic, spoken, etc.), is secure.

Securing PHI not only ensures we keep our customers' trust, but also reduces the risk of incidents—and severe legal consequences.

Physical Safeguards

You can minimize the risk of unauthorized access to PHI by following physical security practices in your workplace. Review some of our organization's policies for physical security by reviewing the security controls below.

Secure Storage and Disposal

- Keep PHI out of clear view from the public (desks, copiers/fax machines) and stored in secure areas.
- Dispose of documents and electronic media containing PHI in secured containers.

Access Control

- Do not allow anyone to follow you into a secure location. Ensure that anyone who enters swipes his or her badge.
- Always follow our organization’s policies for accessing PHI.
- Only discuss PHI in private settings to avoid eavesdropping.

Technical Safeguards

When accessing, storing, and/or transmitting PHI on computers, smart phones and other electronic devices, be sure that you follow our organization's procedures related to:

- Accessing networks.
- Encrypting e-mail and files containing PHI.
- Using passwords.
- Installing and modifying software.

Did You Know

There are over 370 passwords that have been identified as the most commonly used and "hackable" passwords. Do your research, and be sure you aren't using one of them!

Technical Safeguards

- Use passwords that consist of a combination of characters, such as upper and lowercase letters, numbers, and special characters.
- Set your laptop or mobile device's screensaver to require a password and appear automatically when the device is not in use.
- Never share your password with anyone, including family, friends, or coworkers.
- Encrypt emails containing PHI.
- Only connect to approved and secure networks when accessing PHI.

Knowledge Check

Now you'll have a chance to help employees secure PHI in the workplace. Review the following scenarios and determine the best action to take for each situation.

Scenario 1

Employee 1: ""I can't access this system with my password. I was just in the system yesterday!"

Employee 2: "Hmm…They must be in the middle of a system update. Here, go ahead and login as me."

Does sharing your login credentials violate our organization's security policy?

- Yes, you should never share your login or password with anyone.
- No, as long as you change your password immediately afterwards.
- No, you can share passwords with managers or the IT department.

Scenario 2
Employee: “Hold the door! I forgot my badge.”

Should this employee hold the door open for another employee when entering a secured area?

- Yes, if the person is in the building, he must be a valid employee.
- Yes, but only if the employee has valid ID.
- No, all employees need to scan their badges to enter the secured area.

Answer Key
Scenario 1: Yes is Correct. It is against our security policy to share your password with anyone, regardless of their position in our organization. Sharing passwords allows unauthorized people to access information, which violates HIPAA regulations.

Scenario 2: No is Correct. It is a security violation to allow anyone to follow you into a secure location. Ensure that anyone who enters scans his or her badge.

Summary

You have completed this lesson on securing PHI. Here are the key points covered:

- All employees are responsible for protecting PHI.
- Always follow our organization’s procedures for accessing, transmitting, storing, securing, and disposing of PHI.

Enforcement and Breach Notification

HIPAA Enforcement and Penalties

In addition to specifying the ways that PHI must be protected, HIPAA regulations also contain specific penalties for failing to protect PHI. Any improper release, acquisition, use, or disclosure of PHI may be a violation of HIPAA regulations.

These types of incidents not only violate individuals' privacy rights—and their trust in our organization—but also may have severe consequences ranging from significant fines to criminal penalties. Monetary penalties and legal sanctions exist to prevent incidents from occurring and also provide consequences for those who violate HIPAA rules and regulations.

Everyone in our organization is legally obligated and accountable for following HIPAA regulations as well as our organization's Information Security and Privacy policies and procedures.

Types of Violations

The biggest risks to maintaining the privacy and security of PHI usually occur from within our organization. We must protect against violations, whether caused by a lack of someone following the appropriate procedures, or by a malicious attempt to steal information.

HIPAA legislation increases the penalty amounts based on the level and intent of a breach of information.

All incidents are classified and penalized according to their type. Examples include:

- Faxing a document containing PHI to the wrong number.
- Sending lab results to the wrong patient.
- Giving discharge instructions to the wrong patient.
- Leaving a computer logged on and unattended.
- Leaving passwords in plain view of others.
- Using electronic PHI without the proper security controls.

Social Media

EvergreenHealth recognizes the value of social media, and also the added risks of HIPAA violations that it can cause. Multiple facilities have terminated employees after pictures or stories of patients were posted to social media sites.

Staff should at all times use social networking in a manner consistent with the EvergreenHealth Code of Conduct, as well as policies, laws and privacy regulations in order to minimize risk. Let's look at some best practices:

Social Media

What to avoid:

Posting pictures of patients

Complaining about patients while complaining about your job

Blowing off steam after a hard day, such as posting an experience with a difficult patient

Commenting on new stories about patients who are being treated

Letting people know who you are caring for Adding information to threads others have started

Best practices:

Do not list our organization in your employment section

Do not reference events that happen at work

Keep social media conversations with co-workers limited to personal, non-work events

Do not send pictures of patients to your friends, or post them

Do not add of follow any patients you met through work

Report inappropriate use to privacy@evergreenhealth.com or your supervisor.

Breach Notification

To comply with HIPAA, our organization must investigate all incidents in which PHI has been improperly accessed, acquired, used, or disclosed. This requirement applies to all forms of PHI and includes all unauthorized types of access and disclosures— inside and outside of our organization.

In many cases we must also notify individuals of the incident.

To ensure we fulfill these requirements, you are responsible for promptly reporting suspect actions – no matter how minor they may appear – through our incident reporting process.

Did You Know?
If an incident affects more than 500 people, our organization must notify the media.

Knowledge Check

Now you'll have a chance to help employees report incidents in the workplace. Review the following scenarios and determine the best action to take for each situation.

Scenario 1

Employee: "Uh oh. I just e-mailed a patient's contact information to the wrong address…"

What should this employee do?

- Wait to see if the e-mail bounces back before doing anything.
- Nothing. Mistakes like this happen all the time.
- Consider this to be an incident and report it.

Scenario 2

Employee: “Who threw this patient’s contact information away in the regular garbage? I wonder who saw this…”

What should this employee do?

- Nothing. No one will ever see it beyond the facility.
- Remove the record from the trash can and report the incident.
- Notify the patient immediately.

Answer Key

Scenario 1: Report this incident is Correct. Although mistakes do happen, sending PHI to an unauthorized party is an incident and, by law, must be reported.

Scenario 2: Remove and report is Correct. Finding unsecured PHI is a violation. The PHI needs to be secured and the incident needs to be reported immediately.

Summary

You have completed this lesson on HIPAA enforcement and notification. Here are the key points covered:

- An incident is defined as the suspected or known improper access, acquisition, use, or disclosure of PHI.
- Everyone in our organization is responsible and accountable for following our organization's procedures for safeguarding PHI and promptly reporting incidents.
- To comply with HIPAA, our organization must investigate all suspected or known privacy incidents in which PHI may have been improperly accessed, acquired, used, or disclosed.

Congratulations! You've completed this training on HIPAA regulations and compliance.

Summary of the key points

- HIPAA requires us to keep patients' information secure and private.
- You must follow our organization's policies and procedures when using, disclosing, transmitting, storing, or requesting PHI to ensure that individuals' rights are respected.
- PHI may be used and disclosed to the minimum necessary for treatment, payment, and healthcare operations purposes.
- Unauthorized access of PHI has severe consequences to our patients and our organization, and you are obligated to comply with HIPAA standards to ensure PHI remains secure.
- You have a responsibility to identify and promptly report privacy and security incidents using our organization's reporting policies and procedures.

Resources

Privacy questions, complaints, requests and incidents should be reported to our Privacy Officer. Our Information Security and Privacy policies are located in Lucidoc.

Privacy Officer: Richard A Meeks, CHC, CCEP
Compliance Hotline: 425-899-5599
Email: Privacy@evergreenhealthcare.org

Remember, HIPAA compliance begins with you!

HIPAA Assessment

1. When you comply with HIPAA standards, what are you ensuring?
    a. Patients have unlimited access and control over their health information.
    b. Patients have legal rights regarding who can access and use their PHI.
    c. Our organization has implemented the proper security controls required by law.
    d. Our organization has the final say on who can access our patients and/or customers' PHI.

2. You attempt to log in to an unattended computer but notice one of your coworkers is still logged in with their credentials. What should you do?
    a. Log out of the computer and log back in with your credentials.
    b. Stay logged in as your coworker—you will only be using the computer for a minute.
    c. Ask around to see if anyone else has used the computer.
    d. Log out and report the situation to the Privacy Officer.

3. You are eating lunch in a public place with a coworker who begins to tell you details about a patient's condition. Is this permitted?
    a. Yes, if you have an authorized need to know.
    b. Yes, as long as she doesn't disclose the patient's name.
    c. No, only your coworker and her patient are legally allowed to discuss the patient's condition.
    d. No, even if you have an authorized need to know, you should never discuss PHI in a public place where others may hear.

4. You receive a medical file containing a patient name, address, e-mail address, injury report, and automobile VIN number. Which of the information is PHI?
    a. The patient name
    b. The patient name, address, and e-mail address
    c. All of the information is PHI
    d. None of the information is PHI

5. What's your responsibility in protecting PHI?
    a. To know and follow our organization's HIPAA security and privacy policies and procedures for safeguarding PHI.
    b. Limited, the person who gave me the PHI is responsible for its protection.
    c. To know what it is and report violations as needed.
    d. None, I don't ever work with PHI.

6. True or False: You are only liable for securing physical or electronic forms of PHI.
    a. True—having conversations about PHI is just part of our business and requires no security controls.
    b. False—reasonable safeguards need to be taken to secure all PHI, regardless of its form.

7. To what extent can you access, use or disclose PHI?
    a. To the minimum degree necessary required for treatment, payment, and health care operations.
    b. To the minimum degree necessary to ensure a profit for the organization.
    c. To the extent necessary to fulfill authorizations allowed by the patient.
    d. Generally, if you can access PHI, you can use it.

8. You just learned from Facebook that your friend had an accident and they may be in the hospital. You're concerned about them and want to know if they are OK. What can you do (select all that apply)?
    a. Contact a mutual friend to find out what they might know.
    b. Call the Operators to inquire of their presence.
    c. Contact Health Information Management (HIM) to get a copy of information.
    d. Look them up in the system to see what happened.

9. You receive a patient complaint that their privacy has been violated. What should you do?
    a. Try to resolve the situation.
    b. Direct the complaint to the appropriate person in the organization (the Privacy Officer).
    c. Determine if it is a valid complaint and then report it as necessary.
    d. Nothing—complaints are a natural part of business operations.

10. A coworker asks you to provide him with PHI for one of his employees. He isn't authorized to access the information himself, but assures you he has no malicious intent. Should you do this?
    a. Yes, because he is a coworker, he has a business need.
    b. Yes, if he has no malicious intent, there's no harm in doing a favor.
    c. No, you can't be sure he won't use this information illegally.
    d. No, providing this information—regardless of intent—is against the law and could result in massive legal repercussions.

Note: 80% correct is required to pass this assessment.

Name (Please Print):_____

Signature:_____ Date:_____

Score: _____