The Health Insurance Portability and Accountability Act

March 2024

Welcome

Welcome to the 2020 training on HIPAA Privacy and Security Training

Learning Objectives

- Employees who come in contact with or may come in contact with “Protected Health Information” are required to complete annual HIPAA training
- This presentation is designed to refresh your knowledge with:
- HIPAA regulations
- Company policies and procedures regarding protected health information (PHI)
- Ensure Federal compliance

Summary of the Law

- To establish basic privacy and security protection of health information
- To guarantee individuals the right to access their health information and learn how it is used and disclosed
- To simplify payment for health care
- Information Protection is not optional, it’s the law.

Who must take this training?

- As someone who provides health or other services to a Medicare or Medicaid beneficiary, you fall into one of the categories listed below and must take this training.
- Any associate or employee of a Medicare contractor or plan sponsor, including 2020.
- Any contractor or contingent workforce member of our company.
- Any First-Tier, Downstream or Related Entity (FDR) that provides services or support to 2020 Medicare/Medicaid members.

What is HIPAA?

- Health Insurance Portability and Accountability Act passed in 1996
- Overseen by: Department of Health & Human Services (HHS)
- Enforced by: Office for Civil Rights (OCR)
- Regulations on:
- Privacy of health information
- Security of health information
- Notification of breaches of confidentiality
- Unauthorized disclosures of protected information
- Penalties for violating HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

Since 1996, the Health Insurance Portability and Accountability Act (HIPAA) has put important safeguards in place for medical providers and health plans to make sure they protect your rights.

If you work for a **health plan** or **medical provider**, the HIPAA law requires you to honor the privacy rights of every patient. The law applies to companies that process claims and patient information (**clearing houses**) and to companies that provide services to health plans, providers or clearing house (**Business Associates**)--people like accountants, records managers, and auditors.

This course will tell you what you must do to protect patient privacy and keep patient information secure. And explain basic Policies and Procedures needed to safeguard the Protected Health Information (PHI) of the members we serve.

The HIPAA Privacy Rule and Security Rules allow us to use peoples information as necessary to do our job. We must be careful how we **USE** and **DISCLOSE** each person's Protected Health Information.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA says that we must have sanctions for staff who violate HIPAA Privacy and Security Rules. You can get reprimanded, suspended, or even fired if you do not keep health information confidential.

There are legal penalties - fines or even jail time - for people who do not follow the HIPAA law. These penalties apply to our organization.

They also apply to staff and contractors (Business Associates) if they ignore the law, especially if they deliberately give someone's private information to another person who is not authorized to see it. That's another reason why this course is so important.

You are probably already doing most of the things that HIPAA requires! HIPAA, however, asks us to make sure, and to write down our policies and procedures.

Health Insurance Portability and Accountability Act (HIPAA)

We are going to use some abbreviations and special terms during the training. In this section you will learn about PHI (Protected Health Information), Use and Disclosure, and TP (Treatment, Payment or Operations).

PHI: HIPAA says that Protected Health Information (PHI) may only be used or disclosed as allowed under the HIPAA law. We will explain what PHI is.

TPO: HIPAA says we can use protected information as we need to for Treatment, Payment or Operations (TPO), so we will learn what TPO means

Use or Disclose: HIPAA says we must be careful how we use protected information.
We must only disclose information as the law allows.
We will explain the difference in **Use and Disclose**.

Health Insurance Portability and Accountability Act (HIPAA)

Protected Health Information (PHI) has two components:

Health Information ... **and**

* Information that **specifically identifies** a certain person

There are rules about how PHI may be used, so it is important to know what it is!

Health Insurance Portability and Accountability Act (HIPAA)

Here are some examples of Health Information

* Information that describes a medical condition, such as a diagnosis or diagnosis code

* Information that describes a medical procedure or treatment, like a procedure code

* A prescription
* A medical chart
* Vital signs or medical test results
* Information about a doctor appointment or hospital stay
* A medical claim form
* A patient's eligibility information, membership in a health plan or insurance information

Health Insurance Portability and Accountability Act (HIPAA)

Here are some examples of Individual Identifying information

* A person's name
* A social security number
* A patient ID or Insurance ID number
* An address

A zip code, especially a nine-digit zip code

* An email address, Facebook name, or online nickname
* A telephone or fax number

Health Insurance Portability and Accountability Act (HIPAA)

Forms of PHI: PHI can exist in written, electronic or oral format.
All formats of PHI are protected by the HIPAA Privacy Rule!

Written PHI can include claims, forms, letters, notes, reports, lists, and memos.

Electronic PHI can include items stored on computers, cell phones, USB drives, storage devices, laptops, iPads, Blackberries, digital copiers, recorders, electronic medical record systems, voicemail systems, email, databases and many other devices.

We use PHI orally when we talk to doctors and office staff, when we deal with pharmacies or our contractors, when we have to discuss cases with our co-workers, when we talk to the patients themselves, and when we deal with telephone inquiries from government officials.

Health Insurance Portability and Accountability Act (HIPAA)

Examples of PHI:

* The fact that John Doe has a psychiatric condition or that he is receiving mental health counseling.

The information is PHI whether it is a medical record, communicated over the phone, or sent electronically.

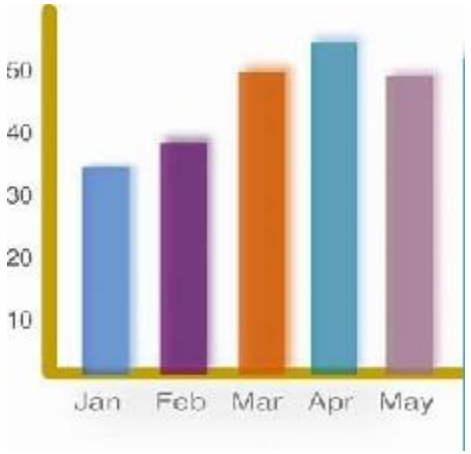
* A health insurance claim form for Jane Doe, because it has both the name of the individual and information about medical services performed. It is PHI whether the claim is a paper form or an electronic record.
* The patient roster for a Primary Care Physician, because it has patient names and IDs and the fact that they are under a particular doctor's care.
* A prescription for patient #112-34-5678, because it has information that identifies the individual and the medication prescribed to him or her.

Health Insurance Portability and Accountability Act (HIPAA)

Examples that are NOT PHI

A statistical report about the drugs that are effective in treating hypertension.
This kind of report is not PHI as long as it does not contain any individual identifying information. It only contains health information.

A notice to providers asking them to update their telephone numbers.
It does not contain any health information about any of our patients.



Health Insurance Portability and Accountability Act (HIPAA)

Treatment, Payment or Operations (TPO)

HIPAA allows us to do routine things with PHI with no special permission from the patient.

These routine things are summarized with the terms **Treatment, Payment and Operations** (TPO). In the rest of this training, we will call it TPO, so let's learn what TPO is.
Treatment includes all the things we do that are part of the patient's medical care.

It includes sending enrollment materials, scheduling appointments, customer service to the patient, coordination of care, and case management.

Examples of treatment include: health care appointments, lab testing, filling prescriptions, referring a patient to a specialist, hospital discharge planning, participating in the prior approval process.

Health Insurance Portability and Accountability Act (HIPAA)

Treatment, Payment or Operations (TPO) (continued)

Payment includes all the activities related to paying for a person's health care.

* Determining if an individual is eligible;

* Coordinating claims with contractors or other payers;

* Reviewing medical records to decide if a procedure should be paid;

* Verifying coverage limits;

* Discussing claims with providers in person, by correspondence or on the phone;

Health Insurance Portability and Accountability Act (HIPAA)

Treatment, Payment or Operations (TPO) (continued)

Operations includes all the activities done for the business of providing health c

Operations includes accounting, auditing, rate-setting, policy determination, fraud and abuse detection and prevention, employee training, legal services, provider contracting.

Sending information about a payment that was made or denied.

For all TPO, Remember the Minimum Necessary rule.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Privacy Rule has standards for both **use** and **disclosure** of protected health information. They are described as follows:

Use is reading or viewing information, such as looking up patient eligibility, reviewing claims, analyzing reports that contain PHI, reading email with PHI, or in any way accessing PHI electronically, in writing or orally.

Disclosure is giving PHI to anyone outside of our company and contracted Business Associates by any means: electronically, in writing, or orally. It includes all such disclosures, whether purposeful or accidental.

Think of use as internal and disclosure as external communication.

Health Insurance Portability and Accountability Act (HIPAA)

Use and Disclosure of PHI

You may use or disclose information with other authorized staff, such as claims staff, accountants, auditors, provider or member relations, care coordination staff, managers, supervisors, IT staff, our contractors and providers in our network as long as they need the information to do their work on our behalf, and as long as you only use or disclose the minimum necessary PHI to accomplish your job.

Remember that there are penalties if we do not comply with these rules. Our company can be fined. You can be reprimanded or fired if you do not follow our Policies and Procedures.

You can be fined or even jailed for violations of HIPAA, depending on how serious they are.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule

What can you do to safeguard PHI and protect the privacy of our patients?

In this section, we will explain some practical steps that all of us must take. Most are common sense, but we must be careful all the time and not forget them.

For example, we must not leave papers with PHI lying around on our desk. Someone walking by may know a patient on a list we are working or on a claim form we forgot to file.

You may want to keep papers in a folder to make it harder for someone to accidentally see the PHI on papers inside. Keep papers filed away when you are done with them.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

One of the biggest problems protecting privacy comes from unsecured data, things not properly put away, papers left on the copier, faxes sent and not picked up.

It can happen with our conversations, too. People may accidentally overhear a conversation that involves PHI--especially if we talk in the elevator or the break room.

Our work is interesting, sometimes tragic. But we must keep all PHI securely in its place, and not discuss cases at home or anywhere outside our work area.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

Our electronic devices have made it easy to access work information everywhere. We can use our laptop and tablet computers in airports and Internet cafes, and cell phones let people reach us wherever we are.

In general, we should not have any work items that contain PHI on any of these devices, and we should not discuss PHI outside of our protected work environment.

In the rare cases where an email with PHI shows up while we are in a public place or we receive a call involving PHI where we could be overheard, we must be extremely careful.

Remember that without written permission from the patient, you may only disclose PHI: to authorized staff, to do your work, and using the minimum necessary PHI to accomplish the task.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

We must be careful even within our work area to control PHI. Consider the need to send information containing PHI to someone outside of your office.

The quickest way may be to send a fax or an email.
You don't know where the receiving fax machine may be located, or who may be standing by it. So if you must send a fax, make sure you contact the person you are sending to, verify that their fax machine is secure and ready to receive, send the fax, then verify that they have received it and properly stored it away from public view.

Hackers can read emails while they are traveling over the Internet, unless they are sent using a 'private' option that encrypts them. If you must send an email that contains any PHI, it must be encrypted. There are a couple of options for sending PHI by computer that will be discussed later in the course.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

We need access to a wide range of information to do our job. In the office, we must often pull files, review reports, handle patient charts, and look up data for patient appointments. On the computer, we usually have access to look up eligibility information, review claims, and see a wide range of reports.

HIPAA does not allow us to browse through this information except as necessary to do our job. Do not let curiosity lead you to look up friends or family members to see what insurance they have or what their medical test results show.

You may be subject to penalties under HIPAA if you use more than the minimum necessary Protected Health Information to do your job.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

It is best not to take any work that contains PHI out of the office. If you work from home or your supervisor authorizes you to do some work outside the office that involves PHI, you must be very careful to secure that data so it can not be lost or seen by others. The company may do a site visit or audit to make sure that any PHI you keep in a home office is secure.

Don't discuss PHI with others, even your family members. While it may make for good conversation, it is a violation of the HIPAA Privacy Rule for you to disclose PHI to them.

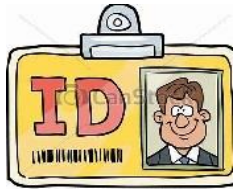
Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

Remember that you may use PHI on the phone with a patient, with other staff, or with other medical offices as long as it is for Treatment, Payment or Operations (TPO). But you must be very careful that you know you are talking to the right person.

You must verify the identity of patients and family members by carefully following our procedures.

These include verifying the name and address of the patient, and using a security question to make sure they are the right person. Do not discuss a patient's PHI with family members unless the family member is the authorized parent or legal guardian of the patient, or if the patient has specifically authorized you to talk with the family member. If you have any question about whether you may discuss PHI with a particular patient or family member, **don't!** Instead, refer the question to your supervisor or to the company Privacy Official and let them make the decision about whether the proper authorization has been received.



Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy Rule continued

The HIPAA Privacy Rule grants our patients certain rights.

First, they have the right to know how we will use their health information. So we prepare and distribute a **Notice of Privacy Practices** (NPP) that explains what health information we keep, how we use it, and what rights they have to see it, amend it, and control how we use or disclose it.

This NPP is given to new patients or health plan members and may be available on our website.

Any patient may ask to receive a printed copy. It may be updated from time to time, and we are bound by what it says.

Health Insurance Portability and Accountability Act (HIPAA)

This does not keep you from being able to use PHI as you have been trained, to do your job as it relates to Treatment, Payment or Operations (TPO).

Most of the HIPAA Patient Rights are related to use and disclosure ***other than*** for TPO.

Other disclosures - for research, for law enforcement purposes, for public health issues, in response to subpoenas--are rare enough that they are handled by our company Privacy Official, a person formally designated to be aware of Privacy Rule requirements and make sure they are followed.

Health Insurance Portability and Accountability Act (HIPAA)

The 2020 **Privacy Official** is Kristen Jimenez.

If you receive any request from a patient to exercise any of the following patient rights, they should be referred to the Privacy Official.

* Right to Review Information. The patient has the right to review PHI that we maintain. The request must be addressed to the Privacy Official in writing.
* Right to Limit Disclosure. The patient has the right to limit certain disclosures of information, but not to control our use of the information for TPO. Any such request must be addressed to the Privacy Official in writing.

* Right to Accounting of Disclosures. The patient has the right to a written accounting of disclosures made for purposes other than TPO. Any such request must be addressed to the Privacy Official in writing.

Health Insurance Portability and Accountability Act (HIPAA)

Also, if you receive any request from a patient to exercise any of the following patient rights, they should be referred to the Privacy Official.

* Right to Request Alternate Communication. The patient may request that we communicate using a different address or communication method. Again, this request must be put in writing and addressed to the Privacy Official.

* Right to Complain. The patient has the right to submit a formal complaint if they believe we have violated or are violating their HIPAA Privacy Rights.

Patients who want to complain should be referred to the Privacy Official. They can complain over the telephone, by email, or in writing.

They also have the right to complain to the Secretary of the US Department of Health and Human Services (HHS).

Health Insurance Portability and Accountability Act (HIPAA)

If you discover that PHI has been or is being used or disclosed in a way that violates the HIPAA Privacy Rule, report it immediately to your supervisor or the HIPAA Privacy Official. Even if you suspect there may have been a violation, report it. If you have accidentally disclosed PHI to someone who should not have seen or heard it--report this incident to the Privacy Official.

Incident reporting is very important, because we may need to take steps to reduce any harm that may have been caused by the incident. We also may need to report the incident to the patient or to authorities.

If you have any questions about HIPAA Privacy or the Privacy portion of this training, you may always contact the Privacy Official.

Health Insurance Portability and Accountability Act (HIPAA)

So far, we have covered requirements of the HIPAA Privacy Rule. That rule explains what kind of data must be protected (PHI), and how we protect conversations and printed materials from unauthorized use and disclosure.

Most of the Protected Health Information we have is stored electronically. HIPAA calls this electronic Protected Health Information, or **ePHI**.

The HIPAA Security Rule tells us what we must do to protect ePHI. There are three basic requirements:

* Use **Physical Safeguards** to protect ePHI.
* Use **Technical Safeguards** to protect ePHI.
* Use **Administrative Safeguards** to protect ePHI.

Health Insurance Portability and Accountability Act (HIPAA)

We work behind locked doors in a secure environment.
We must take the steps necessary to keep our work area secure. Think of it like a military base or a walled city or a bank vault. We have to guard the perimeter and control the access points.

Every staff member must keep the entry doors secure.

* Do not prop doors open.
* Do not leave doors unlocked.
* Do not allow others to use your keys or key cards.

* If you have been issued a badge, wear it at all times.

* Visitors must sign in and be escorted or monitored while they are in the building. They are not allowed in immediate areas where PHI is being used, unless they have proper authorization.

* If you see a person you do not know without a badge or an unescorted visitor, politely escort the person to the sign-in station or to your supervisor.

Health Insurance Portability and Accountability Act (HIPAA)

It becomes more difficult when you leave the building and take your laptop, iPhone, or tablet computer (or any device that can access ePHI). It is also harder for people who must travel for their work or who work from home.

A common HIPAA Security violation is for a mobile devices to be lost or stolen. If the device has data files that contain ePHI, thousands of records could be compromised, and HIPAA fines can be high. You are responsible for the devices and the data, to make sure they are kept secure at all times.

Don't leave your mobile devices anywhere--lock them up when not in use. Make sure you use the password-protection feature on your device. Don't leave the device in a shared hotel room or in the car where people can see it. Don't download any unencrypted data containing ePHI to the device. If the data is not physically on the device, or if data is properly encrypted, technical controls will still be in place to provide some protection to the data.

Health Insurance Portability and Accountability Act (HIPAA)

If you must copy data to a CD, DVD, USB drive (thumb drive), portable hard drive, or any other external device you must make sure the device or data are password encrypted.

If you work from home or in a shared office, follow the same kind of security routines we do at the main offices:

Keep doors locked. Visitors must be escorted and kept away from areas where you use PHI. Make sure your doors, windows, and locks are sufficient to protect against invasion and theft.

You may be visited at any time by our staff to monitor or audit the security of your at-home work area.

Health Insurance Portability and Accountability Act (HIPAA)

We put **Technical Safeguards** in place to further protect electronic Protected Health Information (ePHI).

The safeguard you are probably most familiar with is the requirement that all system access be controlled with unique user IDs and passwords. At times this will feel like a nuisance, especially when you have multiple passwords for multiple systems, and they must be changed regularly. But it is an important tool to protect data and the law requires it.

* You may not share user IDs and passwords with anyone else to access systems where PHI is stored.
* You must keep your passwords secret. Don't write them down where others can see.
* You must change your password when the system requires.
* When you walk away from your computer, lock the screen so it cannot be accessed without re-entry of your password.

Health Insurance Portability and Accountability Act (HIPAA)

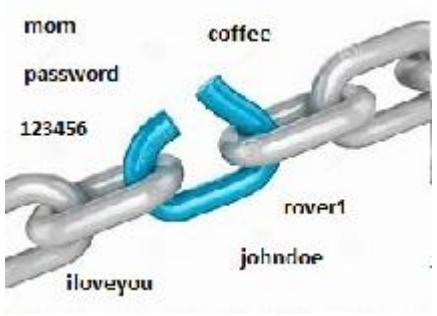
What makes a good password?

When selecting a good password, use different types of characters: lower case letters, upper case letters, numbers, and special characters. Often the system will require you to use three different character types in your password. Usually they must be at least six or seven characters long.

Avoid using simple passwords like: 12345 or abcde.

Avoid using passwords that contain: your birthdate; the name of your child, spouse, or pet; a sports team.

Use an acronym to help you remember your password. (Example, to remember **Jce36w!** you might think: John can eat 36 waffles !)



Health Insurance Portability and Accountability Act (HIPAA)

What makes a good password?

All computers and devices you use to access PHI should be approved and set up by the company or an IT professional.
Verify that password controls are in place and the applications you need to use are secure. Make sure any required standard virus-control software is functioning, and check the computer regularly for malicious software and viruses.

Do not download or install any software that has not been approved on any company equipment.

If you have questions or need help, contact IT staff or your supervisor for support.

Health Insurance Portability and Accountability Act (HIPAA)

BEWARE OF MALICIOUS SOFTWARE (VIRUSES, BOTs, SPYWARE)

The Internet and email systems are dangerous places! Without your knowledge, hackers can plant software on your system that allows them to access any data you can. They can even control your computer without your knowledge. To guard against this kind of attack, don't open email (especially attachments) from people you do not know well. Don't send or open forwarded post cards, jokes, inspirational messages, or photographs.

Don't visit unauthorized or questionable web sites.
Some sites are absolutely off limits: pornographic sites, gambling sites, sites that promote violence or hate groups.

But you must even be careful about sites with general information or news. Pop-up ads may contain the seeds of a virus that can still do damage. Viruses sometimes cause erratic behavior or extreme system slowness--as if the computer is always *doing something in the background*. If you believe you may have picked up a virus, contact IT staff or your supervisor for help.

Health Insurance Portability and Accountability Act (HIPAA)

Many companies store their ePHI on a secure server, with access via a secure network. The secure server sits behind a **firewall** that protects it from hackers and intruders.
Make sure your supervisor gives you clear instructions about where secure data is supposed to be kept.

Do not place unencrypted data containing PHI into an unsecured folder or onto an unencrypted device.

Health Insurance Portability and Accountability Act (HIPAA)

Email systems are not very secure.

Any email sent to people outside of the company must be encrypted if it contains any PHI. There are three ways to do this:

1. Before you start the email, put all of the data into Excel or a WinZip file, and use the Excel or WinZip tools to encrypt the data file itself.
Include the encrypted file as an attachment to your email. Send the password for removing the encryption in a separate message.

2. Post the data to a **secure FTP** (sFTP) site or secure Internet site (**https**) or through a Virtual Private Network (VPN) set up by an IT professional, and send only the notification by email.

3. Some email systems provide an Encrypt Message option on the email Send screen. If it is available, you may use it to meet the encryption requirement.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Security is a serious matter.

Finally, we put **Administrative Safeguards** in place to further protect electronic Protected Health Information (ePHI).

Our HIPAA Privacy and Security Policies and Procedures are part of those safeguards. So is this training. HIPAA requires us to develop rules and methods to make sure we abide by the law, to teach all of our staff and Business Associates about our Policies and Procedures, and to document what we do to enforce HIPAA.

We must sanction employees who violate the HIPAA Privacy and Security Rules. Remember that you can be reprimanded or even fired if you are responsible for a security breach. If the breach is negligent or intentional, there can be further legal consequences.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Security is a serious matter.

The HIPAA Security Official for 2020 is Robert Copola. The Security Official is responsible for making sure the HIPAA Security Policies and Procedures are implemented.

If you become aware of any possible threat to security or breach in security, you must report it to the Security Official. The earlier we are aware of potential issues, the better we can limit any possible damage, and the quicker we can put controls in place to limit further problems.

If you have any HIPAA Security questions, please send them to the Security Official.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Security is a serious matter.

Remember that the main reason we are painstaking about enforcement of HIPAA is to protect the people we serve. Yes, there are rules and procedures and forms and penalties. But most important: people's lives and their good health are at stake.

We appreciate your diligence and expect your full cooperation in giving them the respect and confidential treatment they deserve. Thank you for your participation in taking this course.

Assessment.

Assessment.

HIPAA is ...

- A. a voluntary program undertaken by the health care industry to protect the privacy of our patients.
- B. a set of laws we follow because of the associated penalties.
- C. the Health Insurance Patient Protection Act.
- D. an important federal law enacted, in part, to safeguard and secure patient health information.
- E. a law that can impose penalties on Covered Entities, but not on individual staff members.

Assessment.

Which of the following would NOT be considered Protected Health Information (PHI)?

- ❑ A prescription called in from the doctor to the pharmacy.
- ❑ A report showing the number of HIV/AIDS patients in each county.
- ❑ A medical claim form with the name covered up.
- ❑ A hospital medical chart by the patient's bed.
- ❑ A report of patients who are due for a diabetic screening.

Assessment.

Treatment, Payment, and Operations (TPO) includes?

- ❑ giving PHI over the phone to a specialist's office so they can see one of our patients.
- ❑ research to find a cure for cancer.
- ❑ fundraising for neighborhood Health Centers.
- ❑ advertising our patients' success to attract new members.
- ❑ collecting donations from staff for a patient who cannot afford a medical procedure.

Assessment.

You could face HIPAA penalties ...

- ❑ if you email one of our contractors to explain why a medical claim was denied.
- ❑ if you talk to one of our providers on the telephone, and use PHI to discuss a patient's upcoming treatment.
- ❑ if you maintain a list of HIV patients who need intensive case management.
- ❑ if you use or disclose more than the minimum necessary PHI to do your job.
- ❑ if you allow the accounting department to see your paid claim reports.

Assessment.

Our staff is not allowed to ...

- ❑ discuss PHI with the patient or any family member.
- ❑ send a fax with PHI to a consulting doctor's office.
- ❑ store PHI in an unsecured location.
- ❑ look up eligibility information on the computer for a patient who has an appointment tomorrow.
- ❑ send PHI on the computer using secure, encrypted email.

Assessment.

Under HIPAA, we may always ...

- ❑ talk about cases as much as we want to with our co-workers.
- ❑ send PHI to a doctor we know who is researching the cause of Alzheimer's.
- ❑ mail the patient's medical claim to a collection agency to secure payment.
- ❑ tell a policeman whether a patient tested positive for alcohol intoxication.
- ❑ use PHI as necessary to do our job.

Assessment.

If a Patient calls to complain about a possible violation of their privacy rights under HIPAA, you should ...

- ❑ explain our Policy and assure them that we do not violate patient rights.
- ❑ tell them the complaint has to be put in writing and sent to the Privacy Official.
- ❑ tell them to contact the Secretary of the Department of Health and Human Services.
- ❑ refer them to the Privacy Official by phone, email or regular mail, and notify the Privacy Official yourself.
- ❑ investigate further to see if there is any truth to the allegation.

Assessment.

If you see an unknown person in the secure area of the building who is not wearing a badge, you should ...

- ❑ politely escort them to the visitor check-in station or to your supervisor so they can be issued a badge.
- ❑ escort them off the premises immediately.
- ❑ ask one of your co-workers who they are and why they are here.
- ❑ notify the Privacy Official.
- ❑ not worry. It is the responsibility of someone else to monitor visitors coming and going.

Assessment.

To protect against malicious software, you are not allowed to ...

- ❑ visit web sites to research health policy questions.
- ❑ download unauthorized applications onto your company-issued computer.
- ❑ save files containing PHI onto a secure network folder.
- ❑ email encrypted data containing PHI.
- ❑ open email from trusted sources.

Assessment

The most important focus of HIPAA Privacy and Security Training is ...

- ❑ to meet the legal requirements of the HIPAA Rules.
- ❑ to make sure staff members are not reprimanded, fired, fined or imprisoned.
- ❑ to make sure the company does not have to pay major fines or penalties for non-compliance.
- ❑ to prove we have good administrators and record-keepers.
- ❑ to protect the privacy of the people we serve.

Assessment End.

Congratulations!!! You have completed the HIPAA Privacy and Security Training

You must score at least 80% in order to pass

Thank you