Introduction to HIPAA Training

Health Insurance Portability and Accountability Act of 1996

– Data privacy
– Data security
– Data breach notification

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, was introduced to address the problems that can arise with health insurance when someone changes jobs or becomes uninsured for any period of time. The most profound impact to community pharmacies was a requirement that they take steps to ensure the privacy of all patient information, the security of any data stored or transmitted electronically and to notify a patient when there has been a breach so that they might take steps against identify theft.
During a typically busy day at Joe’s Family Pharmacy, Robert, the pharmacist on duty, is asked by one of the pharmacy’s technicians to counsel Mary, an HIV-positive patient who is confused about how often she should be taking one of her new medications, Atripla.

While the pharmacist is on hold waiting for a physician and verifying prescriptions, several patients are waiting impatiently at the counter for their prescriptions. In order to assist Mary quickly, he raises his voice from behind the computer screen to instruct her. He mentions the name of the drug and dosing instructions with other patients within earshot. One of the waiting patients works with Mary and pulled out her smartphone to learn about Atripla. Until now, she was unaware that Mary was HIV-positive.

Ask yourself...have Robert and Joe’s Family Pharmacy just violated HIPAA?
Marie, one of the pharmacy technicians at Joe’s Family Pharmacy, is on the telephone in the prescription department, joking with a friend about Ted, a 76-year-old patient and family friend who had just been prescribed Viagra.

Ted’s neighbor and close friend overheard the technician’s conversation and became highly offended. She plans on telling Ted what she heard as soon as she gets home.

Ask yourself…have Marie and Joe’s Family Pharmacy just violated HIPAA?
A patient’s privacy is violated when pharmacy staff and other health care workers improperly use, disclose or allow unauthorized access to confidential health information. Sometimes this even includes sharing information with a patient’s family.

Violating privacy may lead to not only embarrassment, but financial damage to the patient, and puts you and the pharmacy at risk of stiff penalties. Robert was careless when he decided to provide counseling to an HIV-positive patient by shouting across the counter. Marie violated a patient’s privacy by discussing health matters with someone who is not a health care worker and within earshot of other patients.

Protecting your patients’ privacy must be part of the day-to-day work of the dispensing staff and all employees who have access to patient information to protect against improper disclosure.

The purpose of this program is to make sure you have a good understanding of the HIPAA Privacy Rule, the Breach Notification Rule and the Security Rule and how this affects you as a healthcare professional, your pharmacy, your patients and your customers.
Understanding HIPAA

- A series of fictional scenarios will help you see how HIPAA affects working in a pharmacy.
- Multiple choice questions and explanation of wrong answers will make learning easy.

During this program, you will be presented with case studies and questions about some likely situations pharmacy employees may see to help you understand and retain the information provided. The questions and cases presented during the program are for self-assessment purposes only and will not be graded. Pharmacists and pharmacy technicians who want to earn CE Credit must complete the post-test with a score of 70% or better.

Keep in mind that although the examples use pharmacies as the setting, all health care providers who handle patient information must comply with HIPAA.
This program has been accredited for one hour of ACPE continuing education credit for pharmacists and pharmacy technicians by NCPA.

- Pharmacist ACPE # 207-000-12-048-H04-P
- Technician ACPE # 207-000-12-048-H04-T

This program has been accredited for one hour of ACPE continuing education credit for pharmacists and pharmacy technicians by NCPA.
Learning Objectives

Upon completion of this program, you should be able to:

- Explain what HIPAA is and the effect that HIPAA has on pharmacy operations
- Define Protected Health Information
- List the patient’s rights under HIPAA
- Explain the contents of a Notice of Privacy Practice and understand to whom the notice must be given
- Understand how to maintain privacy when interacting with a patient’s family, friends and caregivers
- List safeguards to maintain patient privacy in day-to-day pharmacy operations

Upon completion of this program, you should be able to:

Explain what HIPAA is and the effect that HIPAA has on pharmacy operations,
Define Protected Health Information,
List the patient’s rights under HIPAA,
Explain the contents of a Notice of Privacy Practice and understand to whom the notice must be given,
Understand how to maintain privacy when interacting with a patient’s family, friends and caregivers, and
List safeguards to maintain patient privacy in day-to-day pharmacy operations.
What is HIPAA?

HIPAA, which stands for the Health Insurance Portability and Accountability Act of 1996, is a federal law created to, among other things, standardize electronic healthcare transactions and to protect a patient’s medical and health information. In 2009, Health Information Technology for Economic and Clinical Health, or HITECH Act modified some parts of HIPAA and added the requirement that patients receive notification if their privacy is breached.
Who needs to comply with HIPAA?

All health care workers, volunteers and interns, paid or unpaid, who have access to patient information must comply with HIPAA.

Not limited to pharmacy staff, all health providers who maintain protected health information must comply with this regulation as of April 14, 2003.

The Privacy Rule is just one part of HIPAA, but a very important part to health care workers such as pharmacy employees. Other rules that affect pharmacy are the Security Rule and the Breach Notification Rule. These two rules will be discussed briefly in the training course.

HIPAA rules are not limited to pharmacy staff, all health care workers, volunteers and interns, paid or unpaid, who have access to patient information must comply with HIPAA.

You have likely already been asked by other health care providers, when you are the patient, to acknowledge that you have received their “Notice of Privacy Practices”
All staff members that have access to the pharmacy’s prescription records or other sets of patient information must complete training for the HIPAA Rules as well as policies and procedures that are specific to the pharmacy. HIPAA requires documentation of follow-up training on these policies and procedures. It is a good practice to review the policies and procedures at your pharmacy on an annual basis. From time to time they may need to be updated.

All new employees require training. All staff members require training if a new or revised policy or procedure is written.
Penalties

$ $$

- Fines range from $100 - $1.5 million.
- Employers must have a policy on discipline actions for HIPAA violations.

It is very important that all employees take HIPAA and patient privacy seriously. Violations may result in civil fines from $100 for a single violation up to a total of $1.5 million for identical violations in a calendar year.

Employers are required to have a policy regarding discipline for employees who violate HIPAA. Disciplinary measures may range from a verbal warning to dismissal.

The good news is that, as you will see, a little common sense will go a long way in adhering to the HIPAA requirements.
HIPAA is a federal law that regulates how patient health information and records are handled. TRUE or FALSE?
The statement is True.

HIPAA regulates how you and your coworkers handle patient information in pharmacy operations.
Pharmacists are the only health care providers that are affected by HIPAA.

True or False?
The statement is false.

Pharmacists are affected by HIPAA but so are other pharmacy employees as well as hospital, clinic, dentist, health plan and other health care workers. All health care workers who have access to medical records and other health care information are affected by HIPAA.
The Privacy Officer

1. The privacy officer must work with the owner/manager to assess the pharmacy’s current operations and identify areas that need to be addressed in order to comply with HIPAA.

2. The privacy officer will receive and must act upon patient requests for access to and photocopies of pharmacy records, answer patient questions about HIPAA, and respond in a timely fashion to patient complaints.

3. The privacy officer must maintain an efficient filing system for all forms and documents.

4. He or she must assist other staff members with questions for all forms and documents.

5. The privacy officer must monitor any changes in the HIPAA requirements and make any necessary changes accordingly.

In this section, we will explore the selection and role of the privacy officer for your pharmacy and your HIPAA compliance plan.

Each pharmacy owner must appoint a privacy officer. The privacy officer could be anyone on the pharmacy’s staff — it does not have to be the owner, manager, or even a staff pharmacist.

The privacy officer has many responsibilities with regard to the HIPAA regulation. A few of these responsibilities are listed below.

1. The privacy officer must work with the owner/manager to assess the pharmacy’s current operations and identify areas that need to be addressed in order to comply with HIPAA.

2. The privacy officer will receive and must act upon patient requests for access to and photocopies of pharmacy records, answer patient questions about HIPAA, and respond in a timely fashion to patient complaints.

3. The privacy officer must maintain an efficient filing system for all forms and documents.

4. He or she must assist other staff members with questions for all forms and documents.

5. And, the privacy officer must monitor any changes in the HIPAA requirements and make any necessary changes accordingly.
Question

The privacy officer must be the owner or manager of the pharmacy.

True or False?
The statement is false.

The privacy officer may be anyone on the pharmacy’s staff.

The statement is false. The privacy officer may be anyone on the pharmacy’s staff but should be someone capable and willing to take on the responsibility.
What is PHI?

Protected Health Information:

- Name
- Street address and zip code
- Date of birth
- Patient age if over 89
- Telephone number (home, work, mobile)
- Fax number
- E-mail address
- Health Plan, Medicare or Medicaid ID number
- Diagnosis or diagnosis code
- Social Security Number

The common phrase in HIPAA rules for the pieces of information which must be kept confidential is “Protected Health Information” and is abbreviated PHI. The most common protected health information a pharmacy keeps is:

Name
Street address and zip code
Date of birth
Patient age if over 89
Telephone number (home, work, mobile)
Fax number
E-mail address
Health Plan, Medicare or Medicaid ID number
Diagnosis or diagnosis code
Social Security Number
What else is PHI?

- Hospital admission or discharge date
- Date of death
- Charge account numbers
- Certificate or license numbers
- License plate or Vehicle ID Number (VIN)
- Medical device identifier or serial number
- Website URL or IP address
- Biometric identifier (e.g. finger prints)
- Full face photograph or likeness
- Any other unique identifier

Other pieces of protected health information a pharmacy is less likely to keep but must still keep confidential are:

Hospital admission or discharge date,
Date of death,
Charge account numbers,
Certificate or license numbers,
License plate or Vehicle ID number (VIN),
Medical device identifier or serial number,
Website URL or IP address,
Biometric identifier (for example, finger prints),
Full face photograph or likeness, and
Any other unique identifier
Using PHI

• Alone or in combination, pieces of PHI make a patient identifiable.

• Use only for:
  – Treating the patient
  – Requesting or receiving payment
  – Pharmacy operations

• Other uses require written patient permission

Pieces of protected health information, alone or in combination make a patient identifiable. If you write a patient’s date of birth or telephone number on a scrap of paper, you should shred or destroy it. If you photograph a patient for any reason, make sure their face is not in the photograph, or if it is, that you take steps to protect this patient’s privacy.

Pharmacies and other health care providers keep records which contain PHI in order to care for patients, bill for products and services or operate effectively. Your pharmacy computer records, prescription files, dispensing reports and backup files all contain PHI.

Any other use of protected health information requires written patient permission. HIPAA makes exceptions in certain cases for law enforcement, research or detention center inmates.
To help us understand PHI more clearly, let’s take a look at our first case study.

Allison, a cashier at Joe’s Family Pharmacy, performs many tasks, including greeting patients, taking refill requests over the phone and in-person, and ringing up sales for patients.

Mrs. Vinateri calls Allison and inquires whether her doctor’s office has called in a prescription for her yet.

Allison has heard about the HIPAA Rule but is unsure if this is “protected health information” and can be shared with the patient over the phone.

Is Allison allowed to tell the patient if a prescription has been called in for her?

Choose from the following:

A. No, Allison should tell the patient that she cannot provide confidential information over the phone.
B. Yes, Allison can tell the patient but only if she has approval from the privacy officer.
C. Yes, Allison can tell the patient but only if the patient has already signed the acknowledgement that she has received the pharmacy’s notice of privacy practices.
D. Yes, Allison can tell the patient.
D. Yes, Allison can tell the patient.

It is okay to answer the patient’s questions about the status of her prescription. She does not need the permission of the privacy officer. However, care should be taken so that other patients can’t overhear any information that would identify the patient and her individually identifiable health information.

The correct answer is D. It is okay to answer the patient’s questions about the status of her prescription. However, care should be taken so that other patients can’t overhear any information that would identify the patient and her individually identifiable health information. For example, if Allison answered the telephone and said, “Hi, Mrs. Vinateri. Yes your prescription for acyclovir is ready,” within earshot of other patients, they would know the patient’s name and the name of the medication that she was taking. The privacy rule may have been violated. As an alternative, she may want to avoid saying the medication’s name along with the patient’s name if other patients are present and can overhear.”
Question

Which of the following is protected health information that should not have been discussed at the deli:

A. The patient’s age
B. The OTC drug purchased
C. The patient’s relationship status
D. A and B
E. None of the above since the patient name was not spoken

Let’s look at another case study.

Marie and Rachel, the two technicians at Joe’s Family Pharmacy, are chatting in line at the deli, waiting to order sandwiches for lunch. Mayor Williams overhears their conversation about the 97-year old man who buys two bottles of gingko biloba every month, one for himself and one for his lady friend. Mayor Williams knows his father is 97 and a customer of the pharmacy but is upset to learn his widower father may have a girlfriend.

Which of the following is protected health information that should not have been discussed at the deli:

A. The patient’s age
B. The OTC drug purchased
C. The patient’s relationship status
D. A and B
E. None of the above since the patient name was not spoken
Answer

D. A and B

The patient’s age and drug purchase are protected health information.

The relative few number of patients over age 89 makes very old age a piece of information that may allow patient identification. Purchase of gingko biloba indicates the patient and his lady friend may suffer from memory loss, a condition they may prefer to discuss privately.

The correct answer is D, both A and B. The patient’s age and drug purchase are protected health information.

The relative few number of patients over age 89 makes very old age a piece of information that may allow patient identification. Purchase of gingko biloba indicates the patient and his lady friend may suffer from memory loss, a condition they may prefer to discuss privately.

Also, the patient’s relationship status, while it may be a private matter, is not considered protected health information.
Question

HIPAA prohibits sending a fax to the doctor’s office with a refill request since the request contains the patient’s name and the name, strength, quantity and last fill date of the drug.

True or False?

Time to answer one last question about protected health information.

True or False – HIPAA prohibits sending a fax to the doctor’s office with a refill request since the request contains the patient’s name and the name, strength, quantity and last fill date of the drug?
The statement is false. The pharmacy may fax information to the physician’s (or other health care provider’s) office for treatment purposes. The HIPAA privacy standards allow pharmacies and other health providers to use and disclose protected health information, without authorization from the patient or the patient’s personal representative, for purposes of “treatment, payment and health care operations.

That being said, reasonable safeguards must be in place to protect the privacy of the information. Safeguards might include: confirming refill fax number, requesting refills via a secure e-prescribing network or locating the fax machine in a secure place in the pharmacy to prevent unauthorized access to faxes.
• **Privacy** has to do with patient rights to control sharing of their PHI.

• **Security** of PHI has to do with the safeguards a pharmacy or other health care facility uses to keep patient information confidential.

The Sometimes it can be hard to understand the difference between privacy and security.

Privacy has to do with patient rights to control sharing of their PHI. It does not matter if that limits sharing of paper and electronic data or verbal sharing. If one of your patients – or you, yourself - do not want PHI shared with anyone except those directly involved in their health care, they have that right.

Security of PHI has to do with the safeguards a pharmacy or other health care facility uses to keep patient information confidential. Examples of safeguards include shredding waste, using privacy filters on computer screens visible to customers, limiting the number of employees who have full access to patient records, encrypting computer files that contain PHI and using a secure e-prescribing network to receive new prescriptions or request and receive refill authorization.
HIPAA Security rules require health care workers to shred all waste paper that contains PHI.

True or False?
The statement is false. The HIPAA Security Rules give health care facilities the flexibility to determine the best security measures for their company.

HIPAA doesn’t require you do anything specific to secure PHI.

It is wise to determine proper security measures and ensure all pharmacy staff members comply.
In this section of the program, we will learn about offering the notice of privacy practices and collecting written patient acknowledgement and what it means to have a notice of privacy practices.

You will be presented with a series of case studies to help you better understand the key areas covered under this topic.
The HIPAA Privacy Rule requires all health care businesses to write down their privacy practices and share them with patients.

Some parts of the Notice will be the same no matter where you go.

Other parts will be specific for the health care business

After the phone call with Mrs. Vinateri, Allison wants to learn more about HIPAA.

She knows that her employer, Joe’s Family Pharmacy, has developed its own “notice of privacy practices,” much like the notice she received from her bank and family doctor during the last year.

During your HIPAA Training, take out a copy of your pharmacy’s Notice of Privacy Practices flier, or ask where they are filed. Look it over. The HIPAA Privacy Rule requires all health care businesses to write down their privacy practices and share them with patients. Some parts of the Notice will be the same no matter where you go. Other parts will be specific for the health care business.
To prove that you have provided the *Notice* to your patients, you ask them to sign a paper or electronic form acknowledging they have received the *Notice*.

HIPAA requires that you provide this Notice to all patients and that you provide notice again if anything in the Notice changes.

To prove that you have provided the Notice, you ask patients to sign a paper or electronic form acknowledging they have received the Notice.

If a patient refuses to provide written acknowledgement, the pharmacy will have a procedure to document refusal.
Here’s a case question about the Notice of Privacy Practices.

Allison, the clerk at Joe’s Family Pharmacy, is often the staff member who asks patients to sign the electronic signature pad or paper log acknowledging they have been provided with Joe’s Family Pharmacy’s Notice of Privacy Practices.

Mr. Henry is a patient at Joe’s Family Pharmacy who has come in to pick up a prescription. He asks Allison why he should sign the acknowledgement document. She correctly and politely explains why but he refuses to sign the document. What should Allison do now?

A. Sign his name for him after he leaves the pharmacy.
B. Refuse to give him his prescription until he signs.
C. Give him his prescription and do nothing else.
D. Allow him to pick up his prescription but make a note to the pharmacist or privacy officer that he refused to acknowledge receipt of the privacy notice.
D. Allow him to pick up his prescription but make a note to the pharmacist or privacy officer that he refused to acknowledge receipt of the Notice.

The pharmacy must make a “good faith effort” to deliver its notice of privacy practices and obtain the patient’s written acknowledgement of receipt of the Notice.

The correct answer is D.

HIPAA does not force patients to sign acknowledgement of the pharmacy’s notice of privacy practices in order to receive their prescriptions. Never sign a name that is not your own.

It is important to note, though, that the pharmacy must make a “good faith effort” to deliver its notice of privacy practices and obtain the patient’s written acknowledgement. The HIPAA privacy standards do not define what constitutes a “good faith effort,” however, it’s important that the attempts to acquire the patient’s written acknowledgement are documented by a staff person at the pharmacy. In this case, it should be documented that Mr. Henry refused to sign the acknowledgment document stating that he received the pharmacy’s privacy notice. Many pharmacies will choose to document this in the “pharmacist’s comments” section of the patient profile in the computer prescription processing system. Others may choose alternative ways to note the refusal.
Documenting Refusal of Notice

- Know your pharmacy’s guidelines for “good faith effort”

- Document every attempt and each result:
  - Refusal
  - Acknowledgement

The pharmacy owner, manager, or privacy officer should determine, document, and communicate to the staff guidelines on what constitutes a “good faith effort.”

For example, pharmacies decide that a good faith effort is asking the patient to sign the acknowledgment document, but after three refusals to sign, a copy of the notice is then mailed to the patient. The notice mailing is documented in the pharmacy’s records on the patient. A pharmacy may opt to use certified mail or delivery confirmation to document delivery.

Other owners or managers may use different criteria to represent their good faith efforts to obtain the patient’s written acknowledgement. Regardless of what the owner or manager decides, it is essential that each attempt is recorded.
Dave, the staff pharmacist, was recently designated the Privacy Officer, prompting a revision of the Notice.

Mr. Henry is back for another refill but wants to know why Allison wants a signature for HIPAA. What should she say?

A. I think we lost track of who already signed – we just started making everyone re-do it.
B. Protecting your private health information has always been a priority at Joe’s Family Pharmacy. Dave is the new HIPAA Privacy Officer after Jake, the technician, and his family moved away. If you have questions or complaints about the privacy of your health information talk to Dave, his contact information is on the back of this notice.
C. So we can start selling our patient lists.
D. Just sign it!
Answer

B. Protecting your private health information has always been a priority; talk to Dave, his contact information is on the back of this notice.

The **Notice** was updated with contact information for Dave, the new Privacy Officer and all patients need to be provided a new **Notice** with contact information for the Privacy Officer.

The correct answer is B.

Since the **Notice** was updated with contact information for Dave, the new Privacy Officer, all patients need to be provided a new **Notice** with contact information for the Privacy Officer.

Though it is not illegal to sell patient lists, answer choice 3 is not correct. A patient must be allowed to decide if they want their PHI to be sold for a specific marketing activity.
Many community pharmacies offer convenient delivery services. The delivery of medications to the patient’s home, however, creates situations in which the capture of the patient’s written acknowledgement becomes more difficult.
Case Study

Sam has two places to go on his deliveries.

Sam asks the privacy officer, “Pearl doesn’t always come to the door when I take the delivery to her house. How am I supposed to get her to sign the acknowledgement document? And, what about all the patients at the nursing home?”

Let’s review a common delivery case study to see how to best manage this scenario.

The Privacy Officer at Joe’s Family Pharmacy explains the HIPAA privacy standards and the pharmacy’s policy on capturing patient written acknowledgment to Sam, the pharmacy’s employee who makes deliveries.

Sam has two places to go on his deliveries – one to the residence of Pearl Shepard and one for the Heritage Village Nursing Home. After giving some thought to how the HIPAA policy will impact his delivery routine, Sam asks the privacy officer, “Pearl doesn’t always come to the door when I take the delivery to her house. How am I supposed to get her to sign the acknowledgement document? And, what about all the patients at the nursing home?”
How do you think the privacy officer should appropriately respond to Sam?

A. Ring the doorbell and if Pearl Shepard comes to the door, hand her the Notice of Privacy Practices and the logbook or other document to collect her signature acknowledging receipt of the pharmacy’s privacy notice and ask her to sign it.

B. Go to the rooms of the patients he has deliveries for at Heritage Village and hand each patient the Notice of Privacy Practices and request the patient to sign the logbook or other document used to collect patient signatures.

C. The privacy officer should arrange in advance for Heritage Village to distribute the pharmacy’s notice along with its own privacy notice.

D. A & B only

E. A & C only
In the case of delivering a prescription to a patient’s residence, the pharmacy must make a “good faith effort” to obtain the patient’s signature regardless of whether the prescription is delivered to the patient in-person, picked up by someone else or delivered.

In the case with the nursing home, the pharmacy should coordinate the signing of its acknowledgement document with the nursing home.

The correct answer is E: A and C only.

In the case of delivering a prescription to a patient’s residence, the pharmacy must make a “good faith effort” to obtain the patient’s written acknowledgement of receipt of its Notice of Privacy Practices regardless of whether the prescription is delivered to the patient in-person, picked up by someone else or delivered. The pharmacy should attempt to include the Notice of Privacy Practices with the patient’s prescription when delivered and obtain the patient’s signature. If Pearl Shepherd is not home, Sam should leave the pharmacy’s Notice of Privacy Practices with the delivery and upon returning to the pharmacy inform the privacy officer so that an appropriate note documenting the attempt can be recorded.

In the case with the nursing home, it’s impractical and, in many facilities, a violation of their policies for Sam to drop off the pharmacy’s Notice of Privacy Practices in each of the patient’s rooms. Since the nursing home must also comply with HIPAA, the pharmacy should coordinate the signing of its acknowledgement document with the nursing home.

If the patient has a responsible party and/or caregiver, the pharmacy should attempt to acquire their written acknowledgement. In both cases, it’s essential that the pharmacy document its “good faith effort” to acquire the written acknowledgement if unsuccessful in obtaining the patient’s signature.
Finally, let’s review a case that explores what constitutes the patient’s rights with regard to protected health information.

Mr. Henry returns to the pharmacy later that day, obviously upset. He tells Allison that he demands to speak to the manager because his empty prescription bottles were not returned to him, a request he has made at the pharmacy for years.

After consoling Mr. Henry, pharmacist Robert makes a note on Mr. Henry’s computer patient profile that reads: “That old geezer ALWAYS wants his bottles back – give them to him!!!”

A few weeks later, Mr. Henry comes back to the pharmacy. He says he saw on the news something about HIPAA and that one of his patient rights is to receive a copy of the pharmacy’s records containing his PHI, including the patient profile.

True or False – The inappropriate comment is part of Mr. Henry’s protected health information?
The statement is true.

Since the pharmacy uses Mr. Henry’s patient profile in his treatment, it became part of what HIPAA refers to as the “designated record set”.

Since a patient has a right to request access to their PHI, it’s a good idea to avoid entering negative, unprofessional comments in a patient profile.

Technically, the statement is true. All records containing PHI used for treatment, payment or health care operations are subject to access by the patient. Since the pharmacy uses Mr. Henry’s patient profile in his treatment, it became part of what HIPAA refers to as the “designated record set”.

Since a patient has a right to request access to their PHI, it’s a good idea to avoid entering negative, unprofessional comments in a patient profile.
Patient Rights Under HIPAA

• Patients may request a copy of their protected health information. The pharmacy has the option to accept or deny the patient’s request. In either case, the pharmacy must respond to the patient within 30 days. It’s important to document such patient requests and respond to them.

• Patients have a right to request amendments to their PHI contained in the pharmacy’s records if they believe that the PHI is incorrect or inaccurate. The pharmacy must respond to the patient’s request within 60 days.

Patients are afforded several rights under the HIPAA privacy standards, and it is important that each staff member understand and respond in a timely fashion to patient requests.

• Patients may request a copy of their protected health information that is maintained by the pharmacy. Although, it’s likely that most pharmacies will accommodate the patient’s request for a copy of their records, the pharmacy has the option to accept or deny the patient’s request. In either case, the pharmacy must respond one way or the other to the patient within 30 days. It’s important that the pharmacy document such patient requests and respond to them.

• Patients also have a right to request amendments to their PHI contained in the pharmacy’s records if they believe that the PHI is incorrect or inaccurate. Again, the pharmacy can accept or deny the request for amending the patient’s records but it must respond to the patient’s request within 60 days.

• It is possible for the pharmacy to request a 30-day extension in either of these situations by sending a letter to the patient informing the patient of the need for the additional 30 days.
Patient Rights Under HIPAA

• Patients may request an accounting of all disclosures of their PHI made by the pharmacy. Fortunately, for the pharmacy staff, in the vast majority of pharmacies, virtually all of the disclosures typically made are exempt from the accounting requirement because they are for treatment, payment or health care operations.

• Finally, patients have a right to place limitations on the pharmacy’s disclosure of their PHI and request that the pharmacy communicate with them in a confidential manner.

Patients may request an accounting of all disclosures of their PHI made by the pharmacy. In other words, patients may request a list of all of the disclosures the pharmacy has made of the patient’s PHI – unless the disclosure was for purposes of treatment, payment or health care operations, or for other purposes that are specifically exempt from the accounting by HIPAA. Fortunately, for the pharmacy staff, in the vast majority of pharmacies, virtually all of the disclosures typically made are exempt from the accounting requirement because they are for treatment, payment or health care operations.

Finally, patients have a right to place limitations on the pharmacy’s disclosure of their PHI and request that the pharmacy communicate with them in a confidential manner.

For example, if a husband and wife separate pending divorce, one or both of them may request that the pharmacy use a specified personal mailing address, telephone number or email address if it becomes necessary to contact them.
Patient Rights Under HIPAA

• Patients also have a right to file a complaint if they believe their PHI has not been protected by the pharmacy, the pharmacy has denied the patient the exercise of their rights under HIPAA.

• Patients may file a complaint with the pharmacy’s privacy officer.

• Patients may file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, in Washington, D.C.

Patients also have a right to file a complaint if they believe their PHI has not been protected by the pharmacy, the pharmacy has denied the patient the right to exercise a right under HIPAA or the pharmacy has otherwise failed to comply with the HIPAA privacy standards.

Patients may file complaints with the pharmacy’s privacy officer or they may file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, in Washington, D.C.
It is critical that each member of the pharmacy staff understands just how much, or how little, information should be provided to a patient’s family member or caregiver under HIPAA. The complete health record, or data set, is a combination of information from the patient, from pharmacy records and from the records of other healthcare providers or family and caretakers. The pharmacy rarely needs to share the whole patient record for a prescriber to provide proper care or for a third party to help process a claim.

The following two case studies will assist you in understanding this important issue and developing this portion of your policy.
Question

Can Marie tell Mr. Thatcher’s daughter that his prescription is ready?

A. Yes, Marie should tell the daughter that Mr. Thatcher’s prescription is ready
B. No, Marie should hang up the phone as soon as she finds out Mr. Thatcher is not home
C. No, Marie should ask when Mr. Thatcher will be home and call back then
D. Marie should not have called in the first place. She should wait until Mr. Thatcher calls the pharmacy to ask about the status of his prescription.

One of our technicians, Marie, faxes a prescription refill request for patient Tom Thatcher’s digoxin prescription. Later that day, the prescription is approved by the physician’s office.

Marie calls Mr. Thatcher’s home to let him know that his prescription is ready, but his daughter answers the phone and tells Marie that Mr. Thatcher is not home. Marie has heard about the HIPAA requirement to protect an individual patient’s health information and is unsure what she should do.

Can Marie tell Mr. Thatcher’s daughter that his prescription is ready?

A. Yes, Marie should tell the daughter that Mr. Thatcher’s prescription is ready
B. No, Marie should hang up the phone as soon as she finds out Mr. Thatcher is not home
C. No, Marie should ask when Mr. Thatcher will be home and call back then
D. Marie should not have called in the first place. She should wait until Mr. Thatcher calls the pharmacy to ask about the status of his prescription.
A. Marie should tell the daughter a prescription is ready.

Marie should use good judgment in leaving messages with a family member, she could also simply request that Mr. Thatcher return her call.

The “minimum necessary” information doesn’t include the name of the drug and might not even require saying a refill is ready.

The correct answer is A. Marie should tell the daughter that Mr. Thatcher’s prescription is ready.

However, Marie should use good judgment in leaving messages with a family member. A pharmacy staff person may leave a message with a family member if the patient is not home.

Another example of a purpose for such a call would be a refill reminder to the patient. When making such calls, the pharmacy should take care to disclose only the minimum amount of information necessary to achieve the purpose of the call. This “minimum necessary rule” is a key requirement of the HIPAA privacy standards and applies to all uses and disclosures of PHI. For this example, Marie should only tell Mr. Thatcher’s daughter that the prescription is ready. In most cases, however, it would not be necessary for Marie to tell the daughter the name of the medication, the doctor, or a use for the medication.

Furthermore, Marie may leave messages on an answering machine or by email, but again, great care should be taken not to disclose any more information than is necessary. When leaving a message on voicemail or sending e-mail, the minimum information necessary might be the name of the pharmacy, the pharmacy’s phone number and a request for a return call – without stating the name of the medicine or other information.
Question

Our sales associate Allison is unsure whether or not HIPAA allows someone other than the patient to pick up the prescription for the patient. What should Allison do?

A. Tell Mrs. Thatcher that she will need to bring in a letter granting Mr. Thatcher’s permission for her to pick up his prescription.

B. If Mrs. Thatcher has not already signed the acknowledgement of receiving the pharmacy’s Notice of Privacy Practices, she should include it in the prescription bag and ask Mrs. Thatcher to sign the document used to collect written acknowledgements of receipt of the Notice.

C. Allow Mrs. Thatcher to pick up Mr. Thatcher’s prescription.

D. Both B and C.

This next scenario involves the case where a family member or caregiver is picking up a prescription for the patient.

The next day Tom Thatcher’s wife, Regina Thatcher, comes into the pharmacy to pick up his prescription. Our sales associate Allison is unsure whether or not HIPAA allows someone other than the patient to pick up the prescription for the patient. What should Allison do?

A. Tell Mrs. Thatcher that she will need to bring in a letter granting Mr. Thatcher’s permission for her to pick up his prescription.

B. If Mrs. Thatcher has not already signed the acknowledgement of receiving the pharmacy’s notice of privacy practices, she should include it in the prescription bag and ask Mrs. Thatcher to sign the document used to collect written acknowledgements of receipt of the notice.

C. Allow Mrs. Thatcher to pick up Mr. Thatcher’s prescription.

D. Both B and C.
D. Both B and C

The fact that a relative or friend arrives at the pharmacy and asks to pick up a specific prescription for the patient effectively verifies that he or she is involved in the patient’s care.

The patient does not need to provide the pharmacy with the names of friends or family members in advance.

The next time Mr. Thatcher visits the pharmacy, he should be given the Notice and asked to sign acknowledgment.

The correct answer is D; Both B and C.

The pharmacist may use professional judgment and professional experience to make a reasonable decision if it is in the patient’s best interest to allow a person other than the patient to pick up the prescription.

According to the Department of Health and Human Services, “The fact that a relative or friend arrives at the pharmacy and asks to pick up a specific prescription for the patient effectively verifies that he or she is involved in the patient’s care. The patient does not need to provide the pharmacy with the names of friends or family members in advance.”

But with this example, one other point should be made. While Mrs. Thatcher has now provided written acknowledgement of her receipt of the notice, the next time Mr. Thatcher visits the pharmacy, he should be given a notice and asked to sign the document used to collect written acknowledgement of receipt of the notice.
The Pharmacy must now be careful about how it uses and shares patient information for marketing purposes.

Under HIPAA, the pharmacy must now be careful about how it uses and shares patient information for marketing purposes.
Question

Fran, the pharmacist manager, receives a phone call from a company requesting to purchase a list of all of the pharmacy’s diabetes patients. The company plans to contact all of the patients to tell them about their new medication and to send them a $5 coupon for use in purchasing the new medication.

Does HIPAA address this situation?  
Yes or No.
The answer is yes, HIPAA has rules about selling patient data for marketing.
Question

What should Fran do about the company’s request for a list of diabetes patients to purchase?

A. Ask the company representative if he wants a list of all patients from this year or from previous years.
B. Ask the representative, “How much per patient record?”
C. Advise the representative that the information is protected health information under HIPAA and cannot be used in this way unless the pharmacist has acquired the patient’s written authorization for this use and disclosure.
D. Let the representative have the information as long as the patient has received the pharmacy’s Notice of Privacy Practices.

What should Fran do?

A. Ask the company representative if he wants a list of all patients from this year or from previous years.
B. Ask the representative, “How much per patient record?”
C. Advise the representative that the information is protected health information under HIPAA and cannot be used in this way unless the pharmacist has acquired the patient’s written authorization for this use and disclosure.
D. Let the representative have the information as long as the patient has received the pharmacy’s notice of privacy practices.
Answer

C. Fran should advise the representative that the information is protected health information and patient’s written authorization is required.

Any patient authorization must be specific stating the use and data disclosure planned and include a date or event upon which the authorization will no longer be effective.

The correct answer is C. Fran should advise the representative that the information is protected health information under HIPAA and cannot be used in this way without the patient’s written authorization for this use and disclosure.

The pharmacy may not provide a list of its patients to a third party for its use unless the patient has given written authorization.
Consent for Marketing

• Any patient authorization must be specific stating the use and data disclosure planned and include a date or event upon which the authorization will no longer be effective.

• Written consent for marketing in addition to acknowledgement for Notice.

Furthermore, the written patient authorization must be specific as to the use and data disclosure planned and include a date or event upon which the authorization will no longer be effective. In this case the authorization might request authorization to share patient name, address and diabetes diagnosis for product marketing that will occur during the month of November or a specific year.

Note that the patient’s written authorization for marketing activities would need to be acquired in addition to the patient’s signature acknowledging receipt of the pharmacy’s notice of privacy practices.
**Question**

Jeanie has heard about HIPAA and is reluctant to give the employee’s information to Acme. What should she do?

A. Jeanie should tell Acme that Joe’s Family Pharmacy can no longer do business with them because of HIPAA.

B. Jeanie should secretly give the requested information to the HR coordinator but tell her not to tell anyone that she told.

C. Jeanie should give the HR coordinator the minimum information necessary that is required.

D. Jeanie should ask the patient to pay cash and to get reimbursed by Acme Construction.

The next area that we will cover in this program relates to billing workers’ compensation claims.

Jeanie does the pharmacy’s billing. As part of her job, she bills all workers’ compensation claims. Acme Construction sends all of its employees to Joe’s Family Pharmacy in the event of an injury to one of their employees. Before the prescription is filled, Jeanie must call the Human Resource coordinator at Acme to get a pre-approval for the claim. When Jeanie calls, the HR coordinator asks for the injured employee’s name, the name of the medication, the doctor’s names, and the probable use of the drug. Jeanie has heard about HIPAA and is reluctant to give the information to Acme. What should she do?

A. Jeanie should tell Acme that Joe’s Family Pharmacy can no longer do business with them because of HIPAA.

B. Jeanie should secretly give the requested information to the HR coordinator but tell her not to tell anyone that she told.

C. Jeanie should give the HR coordinator the minimum information necessary that is required.

D. Jeanie should ask the patient to pay cash and to get reimbursed by Acme Construction.
C. Jeanie should give the HR coordinator the minimum information necessary that is required.

The correct answer is C. Jeanie should give the HR coordinator the minimum information necessary that is required.

Workers’ compensation insurance, because it is established under state law and for other reasons, is exempt from much of the HIPAA privacy standards. A worker does not have a right under HIPAA to request the pharmacy restrict its disclosures when that disclosure is authorized by, and necessary to comply with, a workers’ compensation or similar law. Even so, Jeanie should only give the HR coordinator the minimum necessary information to process the prescription claim.

Furthermore, HIPAA permits the use of protected health information for purposes of billing for payment. When billing, keep in mind the minimum necessary requirement described earlier.
Breach Notification

- Pharmacies and other health care companies are required to notify patients if there is a breach of protected health information privacy.

- Notification is only required when PHI is unsecured.

The final topic we will cover in this training program is the Breach Notification Rule.

Beginning in September 2009, pharmacies and other health care companies are required to notify patients if there is a breach of protected health information privacy.

It is important to know the difference between “secured” and “unsecured” PHI with respect to breach notification. Notification is only required when PHI is unsecured.
### Breach Notification

<table>
<thead>
<tr>
<th>Secured PHI</th>
<th>Unsecured PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format that cannot be read, used, deciphered or accessed by unauthorized individuals:</td>
<td>PHI in a form that could be read, used, deciphered or accessed by unauthorized individuals:</td>
</tr>
<tr>
<td>- Shredded</td>
<td>- Whole pieces of paper</td>
</tr>
<tr>
<td>- Incinerated (burned)</td>
<td>- Torn pieces of paper</td>
</tr>
<tr>
<td>- encrypted</td>
<td>- Unencrypted files</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- email</td>
</tr>
<tr>
<td></td>
<td>- Hard drive</td>
</tr>
<tr>
<td></td>
<td>- Flash drive</td>
</tr>
<tr>
<td></td>
<td>- Tapes</td>
</tr>
<tr>
<td></td>
<td>- Disks, CD/DVD-ROM</td>
</tr>
</tbody>
</table>

**Secured PHI:** is protected health information in some format that cannot be read, used, deciphered or accessed by unauthorized individuals. Cross-cut shredded paper, incinerated waste and encrypted electronic records are examples of secured PHI. Note: encryption must meet the specifications in the HIPAA Security Rule.

**Unsecured PHI:** is protected health information in a form that could be read, used, deciphered or accessed by unauthorized individuals. Torn or shredded paper with patient information that can be readily pieced together is unsecured PHI. Unencrypted files of patient information in emails or on a computer hard drive or storage device are unsecured PHI.”
Let’s review a case study to help us understand secured PHI.

Jeanie has had a busy month of billing at Joe’s Family Pharmacy. In order to get caught up, she saves her work in and spreadsheet on a USB storage device to bring home with her. After finishing her work on her home computer, she emails a number of documents to be mailed in the morning to her work email. Which of the following is true?

A. The PHI on the USB storage device is unsecured PHI.
B. The PHI attached to the email message is unsecured PHI.
C. Jeanie is only working with secure PHI since she is not transporting unshredded paper records.
D. Both A and B are true.
D. Both A and B are true

Unless Jeanie applies a special encryption program to the files she saves on the USB drive or attaches to her emails, Jeanie is putting unsecured PHI at risk for breach.

The correct answer is D, both A and B are true.

While unsredded paper records are considered unsecured PHI, so are unencrypted electronic files. Unless Jeanie applies a special encryption program to the files she saves on the USB drive or attaches to her emails, Jeanie is putting unsecured PHI at risk for breach.
Breach Notification

• In all cases of breach, provide written breach notice to each affected patient within 60 days.
  – Type of breach
  – List of information involved
• If more than 10 patients can’t be reached, notice must be posted on your website or published in the newspaper.
• If 500 or more patients are affected, notice must be provided in major media.

In all cases, your pharmacy is required to provide written notice to each affected patient within 60 days. The letter should describe the breach (such as stolen laptop, unshredded PHI in the trash) and list the pieces of information involved.

If your pharmacy is missing, or had out-of-date contact information for more than 10 affected patients, the pharmacy is required to post notice of the breach on its website or in the local newspaper. It is important to keep patient records up-to-date and secure to avoid this.

Finally, if the breach affects 500 or more patients the pharmacy also must notify a major media outlet in the state or other jurisdiction.
Breach Log

- A breach log is required.
- Any logged breaches must be reported to the Secretary of Health and Human Services annually by March 1st.
- If 500 or more patients are affected, notify the Secretary within 60 days.
  – Posted on www.hhs.gov/ocr/privacy

Your pharmacy is required to keep a log of breaches of unsecured PHI. This log is to be reported to the Secretary of Health and Human Services at the end of every year by the first of March. If 500 or more patients are affected, notify the Secretary within 60 days. After breaches affecting 500 or more patients are reported to the Secretary, they are posted online at www.hhs.gov/ocr/privacy.
Business Associates

• A business associate provides a service to the pharmacy that may require access to PHI
  – Attorney
  – DME billing service
  – Contract shredding company
  – Non-employee delivery courier
  – Others
• Business associates must agree to keep PHI secure and assist the pharmacy with breach

Some pharmacies and other companies regulated by HIPAA have business associates who, because they have access to protected health information, are also regulated by HIPAA.

Examples of business associates a pharmacy may have include an attorney, a durable medical equipment billing service, a contract shredding company, a contract prescription delivery courier, and etc.

A formal agreement should exist with any of these companies outlining their responsibility to keep PHI secure and private and to report a breach to the pharmacy immediately.
Question

Jeanie loses the USB drive with patient billing information. Which of the following is true?

A. The pharmacy must immediately call each of the 24 patients who had PHI on the lost USB drive.
B. The pharmacy must notify each of the 24 patients who had PHI on the lost USB drive in writing within 60 days.
C. The pharmacy must place a notice in the local newspaper since PHI of more than 10 patients was affected.
D. The pharmacy must immediately notify the Secretary of the U.S. Department of Health and Human Services.

Let’s use a case study to learn about breach notification.

Jeanie walks to the coffee shop on her way to the pharmacy the morning after bringing the spreadsheet with billing information home on a USB drive. She accidentally leaves the USB drive attached to her keychain at the coffee shop and there is no sign of her keys or the USB drive when she returns. Which of the following is true:

A. The pharmacy must immediately call each of the 24 patients who had protected health information on the lost USB drive.
B. The pharmacy must notify each of the 24 patients who had protected health information on the lost USB drive in writing within 60 days.
C. The pharmacy must place a notice in the local newspaper since protected health information of more than 10 patients was affected.
D. The pharmacy must immediately notify the Secretary of the U.S. Department of Health and Human Services.
**Answer**

B. The pharmacy must notify each of the 24 patients who had PHI on the lost USB drive in writing within 60 days.

The breach should be recorded on the breach log and reported to the Secretary by March 1\textsuperscript{st} of the following year.

The correct answer is B. The pharmacy must notify each of the 24 patients who had protected health information on the lost USB drive in writing within 60 days.

Notice in the local paper or on the pharmacy’s website is only required when the pharmacy does not have current contact information for 10 or more patients. And since the number of affected patients is fewer than 500 the breach should be recorded on the breach log and reported to the Secretary by March 1\textsuperscript{st} of the following year.
Conclusion

- Patient privacy and data security, whether paper or electronic, is a top priority for pharmacy staff.
- Protected Health Information (PHI) is any piece of information that alone or in combination identifies an individual patient.
- Patients have a right to review and request amendments to their PHI.

To wrap things up, remember that patient privacy and data security, whether paper or electronic, is a top priority for pharmacy staff.

Protected Health Information refers to the data you must keep private and secure because alone or in combination, it identifies and individual patient.

Patients, including you when you are a patient, have a number of rights with respect to protected health information. Patients may request copies, file a complaint, or request amendments or changes to the record.

Think back over the questions and case studies and recall how often the answer could be chosen using common sense. HIPAA has many rules, but most are pretty easy to follow.