HIPAA Training Handbook for the Pharmacy Staff

HIPAA Training Handbook for the Pharmacy Staff is published by HCPro, Inc.

ISBN 1-57839-253-5

HCPro provides information resources for the health care industry. A selected listing of other newsletters, videos, and books is found at the end of this book.

HCPro is not affiliated in any way with the Joint Commission on Accreditation of Healthcare Organizations, which owns the JCAHO trademark.

Lauren McLeod, Executive Editor
Jean St. Pierre, Creative Director
Mike Mirabello, Senior Graphic Artist
Paul Singer, Layout Artist
Paul Nash, Group Publisher
Suzanne Perney, Publisher

Advice given is general. Readers should consult professional counsel for specific legal, ethical, or clinical questions. Arrangements can be made for quantity discounts.

For more information, contact:

HCPro
P.O. Box 1168
Marblehead, MA 01945
Telephone: 800/650-6787 or 781/639-1872
Fax: 781/639-2982
E-mail: *customerservice@hcpro.com*

3/2003
16774

Contents

About the Expert

Walter L. Fitzgerald, Jr.

Walter L. Fitzgerald, Jr. received a B.S. degree in pharmacy from Mercer University School of Pharmacy in 1979 and an M.S. degree in pharmacy administration in 1982 from the University of Tennessee College of Graduate Health Sciences. In 1983, he received the Juris Doctor degree from the University of Memphis School of Law. Mr. Fitzgerald is a licensed attorney and pharmacist.

Mr. Fitzgerald serves as Professor of Pharmacy at the University of Tennessee College of Pharmacy. His teaching and research focus is on health care and drug law, health care ethics, and professional liability. In addition to teaching in the professional degree programs, Mr. Fitzgerald teaches research law and ethics for the College of Graduate Health Sciences.

Mr. Fitzgerald's law practice focuses on defense of actions related to malpractice, state and federal licensing and registration of health care professionals, managed care contracting, and health care fraud and abuse. Mr. Fitzgerald's honors and awards include being named Tennessee Pharmacist of the Year in 1996, being appointed to the University of Tennessee Health Science Center Academy of Distinguished Teaching Professors, and most recently in June 2002, receiving the University of Tennessee National Alumni Association Public Service Award.

HIPAA Training Handbook for the Pharmacy Staff

Intended audience

- Pharmacists
- Pharmacy technicians
- Pharmacy students/interns
- Pharmacy cashiers

This handbook, intended for general orientation and training, will acquaint pharmacy staff with the requirements for protecting the privacy of patient information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the potential consequences of not complying. Case scenarios illustrate situations in which the requirements for patient privacy may be breached.

The basics

What is HIPAA?

As part of our pharmacy's promise to give patients quality health care, we keep information about their health and medical treatment confidential. Only pharmacy staff who need the information to do their jobs should use it. They should disclose it to those outside of the pharmacy, such as other health care providers and insurance companies, only in limited circumstances.

Until now, this promise of confidentiality was part of our pharmacy code of ethics and, in some states, a part of the "Pharmacy Practice Act" and/or Board of Pharmacy rules and regulations. But under a federal law effective April 14, 2003, the federal government has, for the first time ever, mandated that we protect the privacy of our patients' health information. Failure to comply with this federal law may result in civil and criminal penalties.

HIPAA includes punishments for anyone violating patient privacy. It also gives patients several rights, including the rights to gain access to our records containing their information, request amendments to their health information, and limit the ways we use and disclose their health information. Our state's laws may already provide some or all of these rights, but HIPAA makes them a federal mandate for the first time.

Those who compromise confidentiality intentionally for financial gain can be fined as much as $250,000 and go to jail for up to 10 years! Even accidentally breaking the rules can result in fines—and tremendous embarrassment—for the pharmacy and its staff.

What brought about this law?

HIPAA is a broad law that covers a variety of issues. One goal was to enable people to easily move from one health insurance plan to another as they change jobs or become unemployed. A second goal was to allow health care providers treating patients to share and transmit information electronically more easily and securely. This law requires all health care providers and payers to use standard formats and code sets for electronic health care transactions, such as eligibility determinations and claims for payment.

Today, with e-mail and Internet access, it is much easier for health care providers, payers, and patients to share records containing health information. However, it is also much easier for people to improperly obtain and use health information transmitted electronically.

That's why the law includes a section with requirements for protecting patient privacy and confidentiality and safeguarding health information in all forms and media. A basic premise of HIPAA is that a health care provider cannot use or disclose a patient's health information without authorization from the patient. Fortunately, the law includes several exceptions that

allow for use and disclosure without obtaining a patient's authorization. Most notable among these exceptions is for use and disclosure of patient health information for treatment, payment, and health care operations.

What are the consequences for not complying?

Breaking HIPAA's privacy rules can result in civil or criminal penalties both for businesses, such as pharmacies, and the individuals who break the rules.

Civil monetary penalties are fines of up to $100 for each violation of a privacy rule, up to a limit of $25,000 in a calendar year for all violations of a single privacy rule. However, a single activity may violate multiple privacy rules. For instance, if over the course of a calendar year a pharmacy released 100 medication records in violation of a single privacy rule, it could be fined $100 for each one, for a total of $10,000. But if the release of the records violated two privacy rules, then the fine could rise to $20,000.

Criminal penalties can include not only large fines, but also imprisonment. The penalties increase with the seriousness of the offense. Selling patient information for personal gain is more serious than accidentally disclosing it in violation of the privacy rules, so it brings stiffer penalties. These penalties can be as high as a $250,000 fine and a prison sentence of up to 10 years. For example:

- Knowingly obtaining or disclosing patient information in violation of HIPAA can result in a one-year jail sentence and $50,000 fine
- Obtaining health information under false pretenses can result in a five-year jail sentence and a $100,000 fine
- Obtaining or disclosing patient information with the intent to sell or use the information for commercial advantage, personal gain, or malicious harm can lead to a 10-year jail sentence and a $250,000 fine

The U.S. Department of Health and Human Services (HHS) has indicated that, in determining penalties, it will consider not only the harm done, but the willingness of the organization to achieve voluntary compliance. In addition, whether the organization knew about a violation will be relevant in determining whether civil or criminal penalties apply. However, even accidental violations at an organization making a good faith effort to comply with HIPAA can lead to penalties.

What's considered private and confidential?

The privacy rules require covered entities—organizations covered by HIPAA—to safeguard what is referred to as protected health information (PHI), which is any "individually identifiable health information" maintained in any form or medium or transmitted electronically. Individually identifiable health information is information that relates to past, present, or

future health status, care, or payment and identifies the individual or gives reason to believe it could be used to identify the individual.

Specific examples of PHI include the following:

- Name
- Address
- Age
- Social Security number
- Diagnosis
- Medical history
- Medications
- Observations of health status

Doctors, pharmacists, nurses, therapists, and others use this information about patients to determine how to treat them. Billing department employees use certain confidential information to bill patients, their insurance companies, Medicare, or Medicaid for services. Pharmacy staff use this information to dispense prescriptions, develop patient profiles, conduct prospective drug utilization review, and counsel patients.

HIPAA requires that health care providers use, disclose, or obtain only the "minimum necessary" information needed to accomplish the intended purpose. In fact, pharmacies must develop and implement policies and procedures to carry out this minimum necessary rule. However, the minimum necessary rule does not apply to disclosures or requests by a health care provider for treatment purposes.

Before undertaking any activity that involves PHI, it's helpful to ask yourself **exactly what information do I need to perform this job?** You should not obtain, use, or disclose any information you don't need.

Who is authorized to see information?

All members of the workforce of an organization contribute to the quality of care. But as we know, that doesn't mean everyone needs to see health information about patients.

Many employees have no access to patient information—on computer or on paper—because they don't need it to do their jobs.

When you need to see patient information to do your job, remember that the information is private and you are not allowed to repeat it or share it with other members of our workforce unless they also need the information to do their job.

These rules apply even when you no longer work for this pharmacy.

Who oversees privacy policies?

HIPAA requires each covered entity to appoint a privacy official to make sure no one violates the privacy rules. This person is responsible for developing the covered entity's privacy policies and enforcing them.

Truly protecting confidentiality depends on you. You must not improperly share or use information that you overhear or see in the course of your work. Doing so is a violation of the law.

What if I see someone break the rules?

As an employee in this organization, part of your job is to help maintain privacy for patients as they receive care. This organization's administration expects all employees to adhere to the privacy and confidentiality policies, but knows there may be times when some employees do not follow them. HIPAA requires that we discipline employees who violate the privacy rules. Disciplinary action could include termination for serious or repeated violations.

Employees are encouraged to report violations or suspected abuses to the organization's privacy official. You may report them anonymously, if you wish, by following the procedures given to you by our organization.

However, do not fear any retaliation if you report a privacy violation. The organization does not punish employees for reporting violations. In fact, it is an expectation of your job to report instances where you suspect the privacy or confidentiality policies are being broken.

Case #1

As you are filling a prescription for chemotherapy drugs, you spot the patient's name. She is a good friend of yours, and you weren't aware that she has cancer. Should you call her to offer your support?

No. If you learned of your friend's condition only because you happened to see her name on the prescription, you should not call her, nor should you mention what you found out to anyone else. Your friend may not want anyone to know, and it is her right to keep information about her health private.

If this patient wants you to know that she is battling cancer, she will tell you or ask a friend or family member to contact you.

On the other hand, if in the process of preparing and dispensing the prescription, legitimate questions or concerns arise, such as a drug-related problem, it would be permissible to call her. Even then, the conversation should focus on the reason for the call.

Case #2

Your sister has noticed that her adult son's behavior has changed drastically over the last several weeks. She is concerned that the herbal supplements he is taking could be interacting with his prescribed antidepressant medication. Your sister asks you to look in

the database to find out the type and dosage of antidepressants her son is taking. What should you do?

Because of the pharmacy's responsibility to conduct prospective drug use review, it would be permissible for appropriate pharmacy staff to look at the patient profile to make certain nothing, such as a drug interaction, was overlooked in the review performed when the prescription was dispensed. But it is likely that the herbal supplements are not on the patient profile, so if your sister told you what supplements he is taking, it would also be acceptable to research whether it is appropriate to take the herbal supplement together with the antidepressant.

Certainly, once the pharmacy learns of a potential drug-related problem, it has a duty to resolve or prevent the problem. But whatever information was found reviewing the situation should not be shared with your sister, unless your nephew is given the opportunity to agree or object to the disclosure of the information to her. See p. 20 for more information about disclosures to family and friends.

Looking at PHI for any nonbusiness reason is cause for dismissal and can have possible legal consequences. If you improperly use or disclose PHI that you obtain while working in the pharmacy, either deliberately or by accident, you can lose your job.

Computer systems and electronic transmission of information

Faxes

HIPAA does not address faxing patient information specifically, but does protect faxed documents under the privacy rule like any other form of health information—written, spoken, or electronic. Faxed patient information can easily fall into the wrong hands, which could result in a violation of the privacy rules. Before faxing any patient information, you must check our policies and procedures. If you have any questions, contact the privacy official for guidance and assistance.

Ideally, when you fax patient information, you should send it to a fax machine in a secure location and notify the intended recipient when you are about to send it so he or she can be ready to pick it up.

If you know you will receive a fax that contains patient information, tell the person faxing the information to warn you ahead of time so that you can be present to receive it.

Do not let faxed patient information lie around a fax machine unattended. Immediately take it off of the machine before others can see it.

E-mail on the job

Our pharmacy has policies about the use of e-mail. Be sure to familiarize yourself with these if you use e-mail to transmit patients' PHI. Remember that work e-mail accounts are not meant for personal use. Sharing or opening attached files from unknown sources can open the door to viruses and hackers.

It's also important to keep in mind that you can never be sure who will have access to your message on the receiving end. Never send confidential information about a patient in an e-mail over a public network without first checking with the privacy official.

When you send e-mail, always double-check the address line just before sending the message to be sure that your e-mail doesn't go to the wrong person or list by mistake.

Passwords and computer equipment

Passwords and other security features help protect patient information by preventing unauthorized access to the computer system.

If you have password access to a computer system that contains patients' PHI, never give your password to another employee or log in using someone else's password—even if it

Helpful hints to use when working with computers

- Review our organization's policies on using computers
- Never use our e-mail system for personal purposes
- Never share or open attached files from an unknown source
- Always double-check the address line of an e-mail before you send it
- Don't share your password or log in to the computer system with someone else's password
- Always keep computer screens pointed away from the public
- Choose a password that contains a combination of letters and numbers

seems like a timesaver. HIPAA requires organizations to be able to tell who looks at PHI so they can make sure all uses of it are necessary and appropriate.

Avoid passwords that can be easily guessed, such as your child's or pet's name, your birth date, and any word that could be found in the dictionary. Use a combination of letters and numbers and, if the software system allows, use a combination of uppercase and lowercase letters. This makes your password more difficult to crack.

Case #3

A woman arrives at the pharmacy and tells you she is there to work on the computers. She asks you where the computer system is located. How do you respond?

The first and most important question to ask her is whether she needs access to patients' PHI to perform her work. If not, you can allow the work to proceed under the supervision of a pharmacy employee, preferably the privacy official. If it is necessary for her to have access to patients' PHI to perform the work, then the woman, or the company for which she works, may be a business associate. The privacy official will need to become involved if access to PHI is necessary.

Case #4

The container or receptacle in the prescription department of the pharmacy where you normally dispose of documents that contain patient information is nearly overflowing. You need to dispose of some materials.

Can you toss the materials into a garbage can outside the pharmacy for pick up by the local trash service?

No. Although HIPAA does not specifically address the disposal of individually identifiable health information in a pharmacy, any documents that contain PHI must be shredded or otherwise destroyed so that the information is obliterated. This also applies to used prescription vials returned to the pharmacy. Simply throwing these vials with labels containing patient and medication names into the trash is not acceptable. If the pharmacy does not have the capability to destroy such materials, it will arrange for an acceptable waste disposal service to shred the materials.

Case #5

A physician calls the pharmacy and asks you to fax a patient's medication record to his office. It is evening, his office is closed, and no one will be able to pick up the fax until morning.

What should you do?

Don't send the fax to an unattended machine unless the doctor assures you that the machine is in a locked room or has a locked cover. If the fax machine is out in the open, arrange to fax the report to the office during regular business hours when a staff member at the office can wait for the fax and pick it up immediately.

Case #6

A fellow pharmacy technician is having trouble logging in to the pharmacy's prescription dispensing computer system. She asks for your login name and password. Should you share them with her?

No. HIPAA requires the use of individual passwords for each employee with access to PHI stored in the computer system. Our organization keeps track of the records you view based on the login name and password you use to enter the system. If you let others use your name and password, you are breaking HIPAA rules, and you may be held responsible if inappropriate access to patient information occurs.

Staff members must keep the system secure by using only their own login name and password to gain access to the computer system. Employees cannot share passwords and should change them regularly based on the pharmacy's policy and procedure.

Case #7

Because the pharmacy's policies and procedures require that you change your password for the computerized record system often, you have a hard time remembering it. Should you jot it down on a piece of paper and stick it in your desk drawer?

No. Even if your desk drawer remains locked, every time you open it, there will be an opportunity for others to see your password. Do not write down your password.

If you have a hard time remembering your password, ask your privacy official or information systems department staff for tips for coming up with a password that meets your organization's criteria, but is easy for you to remember.

Patient rights

Notice of privacy practices

It's important that patients understand how they can protect their own health information and how health care providers protect their information. For this purpose, HIPAA requires health care organizations to prepare and provide a "notice of privacy practices" that informs patients about the ways it will use and disclose PHI and the legal duties of the organization to protect PHI.

This notice of privacy practices also tells patients about rights they have, including the right to review and obtain copies of the pharmacy's records containing their PHI, request amendments to their PHI, request limitations on the use and disclosure of their PHI, and file complaints about the pharmacy's compliance with HIPAA. All patients must be given a notice upon the first provision of pharmacy services on or after April 14, 2003. If the patient is not present in the pharmacy at the first delivery of service, the notice may be delivered to the patient as soon as possible.

For example, if the pharmacy mails a prescription to a patient, it should mail the notice to the patient on the same day, or the next day at the latest. Delivering the notice to a patient by e-mail is acceptable, but the pharmacy must confirm that delivery was successful. If your pharmacy is within a hospital setting filling medication orders for inpatients, the notice will already have been provided to the patient upon admission.

Several other rules are associated with the notice requirement for retail pharmacies:

1. Anyone, regardless of whether he or she is an existing patient, may request a copy of the notice at any time.

2. The notice must be posted in the pharmacy in a location where it can be easily read.

3. If the pharmacy has a Web site, it must post the notice on the Web site.

The pharmacy must also make a good faith effort to obtain a patient's written acknowledgement of receipt of the notice. For pharmacies, the most recognized method for obtaining the written acknowledgement is use of a signature log, similar to the one used for third-party prescription programs. If the patient is not present in the pharmacy or refuses to give written acknowledgement, pharmacy staff must document that. The pharmacist comments section of the patient profile may be a good place to document a failed attempt to obtain acknowledgement.

Authorization

A basic premise of HIPAA is that a health care provider cannot use or disclose a patient's PHI without authorization from the patient except for purposes of treatment, payment, and health care operations, and for other purposes permitted by HIPAA as described in the next section.

If the pharmacy wants to use patient information for purposes other than treatment, payment, operations, or other permitted purposes, it must obtain written authorization from the patient. For example, authorization from every patient on a mailing list may be required to sell the list to drug companies or to mail advertisements to customers based on addresses taken from patient profiles. By way of the authorization—which must be in writing—the patient voluntarily agrees to let your organization use the information only for a particular purpose.

In order to be valid, the authorization must describe specifically the use or disclosure to be made. The authorization must be signed by the patient and include a date after which it will no longer be effective. A copy of the signed authorization must be provided to the patient.

Patients are permitted to revoke authorizations at any time. After an authorization has been revoked, the pharmacy is no longer allowed to use or disclose the information for the purpose documented in the authorization. However, uses or disclosures made before the patient revoked the authorization are not affected.

HIPAA prohibits organizations from requiring patients to sign authorizations. You must serve the patient regardless of whether he or she agrees to allow you to disclose his or her health information beyond the scope of treatment, payment, routine operations, or other disclosures permitted by HIPAA.

Authorization exceptions

HIPAA recognizes the need to use and disclose information without authorization for specific activities and functions. The pharmacy may use and disclose to a family member, other relative, or a close personal friend identified by the patient, PHI directly relevant to the person's involvement with the patient's care or payment. The pharmacy may also use or disclose PHI to notify, or assist in notifying, a family member, personal representative, or another person responsible for the care of the

patient of the patient's location, general condition, or death. In both cases, one of the following requirements must be fulfilled:

- If the patient is available, the pharmacy must obtain the patient's agreement, provide the patient with the opportunity to object, or reasonably infer from the circumstances that the individual does not object.
- If the patient is not available, the pharmacy staff may exercise professional judgment to determine that the use or disclosure is in the best interests of the patient, and use and disclose only the PHI relevant to the person's involvement with the patient's care.

Finally, HIPAA establishes uses and disclosures for which neither an authorization nor an opportunity to agree or object is required, including the following:

- To authorities for public health activities
- To law enforcement officials for investigations or reports of suspected abuse
- To appropriate authorities for health oversight activities authorized by law
- For judicial and administrative proceedings in response to a court order, subpoena, or other lawful process
- To a coroner or medical examiner

- To organ procurement organizations for facilitating organ, eye, or tissue donation and transplantation
- For research approved by either an institutional review board or a privacy board
- To avert a serious threat to health or safety of a patient or the public
- For specialized government functions, such as for military activities, national security, intelligence activities, and protective services of the President
- Authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs

It is very difficult to determine whether patient authorization is required for a use and disclosure outside of the normal course of pharmacy practice. If you are not certain, consult with the privacy official.

Right to access

HIPAA gives patients the right to inspect and obtain a copy of the PHI the pharmacy keeps about them in the "designated record set." In a pharmacy, the designated record set will typically include, but is not limited to, prescriptions, patient profiles, billing records, and forms patients fill out to provide information for the patient profile. Our policy may require

patients to write a letter of request or fill out a form before seeing or obtaining a copy of their PHI.

HIPAA allows the pharmacy to charge a reasonable, cost-based fee for copies of PHI, including the cost of mailing the copies if the patient requests the copies to be mailed.

When a patient requests a copy of his or her PHI, it's up to the pharmacy to verify his or her identity. Our pharmacy's policy will specify the types of identification you can accept, but if you are uncertain, always consult the privacy official.

In many cases, the pharmacy's records may include documentation from other providers who treated the patient. In responding to requests for access to PHI, you should include this additional documentation only if it has become part of the pharmacy's designated record set.

The pharmacy must take action on a request for access to PHI within 30 days. If the PHI is not maintained or accessible at the pharmacy, the pharmacy has 60 days to act. If unable to do so, the pharmacy may request a one-time extension of not more than 30 days, as long as it notifies the patient in writing of the reasons for the delay and the date by which the pharmacy will respond to the request.

HIPAA establishes two sets of grounds for denial of access—one that is "unreviewable" and one that is "reviewable." There

are several grounds listed in each set; those of interest to pharmacy are the following:

Unreviewable grounds for denial of access

A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances:

- The individual agreed to the denial of access when consenting to participate in research that includes treatment, and the right of access will be reinstated upon completion of the research
- The PHI was obtained from someone other than a health care provider under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source of the information

Reviewable grounds for denial of access

A covered entity may deny an individual access, as long as it gives the individual the right to have such denials reviewed, in the following circumstances:

- A licensed health care professional exercises professional judgment to determine that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person

- The PHI makes reference to another person (other than a health care provider) and a licensed health care professional exercises professional judgment to determine that the access requested is reasonably likely to cause substantial harm to that other person

- A licensed health care professional exercises professional judgment to determine that providing access to a personal representative is reasonably likely to cause substantial harm to the individual or another person

If access is denied on one of the above reviewable grounds, the individual has the right to have the denial reviewed by a licensed health care professional designated by the covered entity to act as a reviewing official. That official must not have participated in the original decision to deny. The pharmacy must abide by the decision of the reviewing official.

If it decides to deny access, the pharmacy must provide the denial to the patient in writing within the applicable 30-day or 60-day time frame. The written denial must include the following:

- The basis for the denial

- A statement of the patient's review rights

- A description of how the patient may complain to the pharmacy or HHS

Requests for amendments

HIPAA allows patients to request amendments to their PHI contained in the pharmacy's designated record set. Facilities are not required to automatically make any change a patient requests, but they must allow patients to make the requests and follow this specific process for handling them:

1. **Respond by either accepting or denying the amendment within 60 days of receiving the request.** As with requests for access, if the pharmacy cannot take action within the 60-day period, an extension of 30 days is permitted if the patient is notified.

2. **Inform the patient in writing whether it has accepted or denied the request.** Providers are permitted to deny requests for the following reasons:

   - The PHI is not part of the designated record set.
   - The PHI is not available for access to the individual according to the HIPAA rules governing access.
   - The PHI that the patient wants to amend is accurate and complete.
   - The pharmacy did not originally create the PHI the patient wants amended. However, if the patient provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested

amendment, the pharmacy must respond as though it had created it.

Accounting of disclosures

Even when our organization follows HIPAA's privacy rules to the letter, we still have to be able to produce an accounting of disclosures of a patient's PHI if requested by the patient. The accounting of disclosures lists all parties outside the pharmacy who have received the patient's PHI.

However, the accounting of disclosures doesn't have to include everything. Disclosures to carry out treatment, payment, and health care operations do not need to be included. The accounting also doesn't have to include the following disclosures:

- Directly to the patient and to individuals involved in the patient's care
- Authorized by the patient
- Incidental to a permitted use and disclosure
- To correctional or law enforcement officials
- Of limited data set information
- For national security or intelligence purposes
- Prior to the compliance date of April 14, 2003

Patients have the right to request an accounting of disclosures of their PHI as far back as six years from the date of the request. Facilities must produce the accounting within 60 days of receiving the request, with a possible 30-day extension. Patients have the right to receive one accounting without charge every 12 months. The pharmacy may charge a reasonable, cost-based fee for additional accountings during the same 12-month period.

Right to complain

HIPAA calls for facilities to designate a contact person or office for receiving complaints of privacy violations. In most pharmacies, this person will be the privacy official. The name or title of a contact person or office must be included in the pharmacy's notice of privacy practices.

If a patient or other member of the community wants to file a complaint or register a concern about a privacy violation, be sure to send him or her to the appropriate person or office.

HIPAA also allows people to file complaints with the HHS Office for Civil Rights (OCR). Persons wishing to file complaints should be encouraged to file the complaint with the pharmacy so that we may attempt local resolution. But if this is not possible, then we must assist the person in filing the complaint with OCR.

Final exam

True or false?

1. The criminal penalties for improperly disclosing protected health information (PHI) can include fines of up to $250,000 and prison sentences of up to 10 years.

2. Only employees who need access to patient records have to worry about protecting patient privacy and confidentiality.

3. Confidentiality protections cover not only a patient's health-related information, such as current medications, but also information such as address, age, Social Security number, and phone number.

4. Any employee who violates the pharmacy privacy policy is subject to punishments up to and including termination.

5. Pharmacies must obtain authorization from patients before selling their names and addresses to a drug company.

Multiple choice

6. How long does a pharmacy have to respond to a patient's request for an amendment to PHI?

a. 15 days
b. 60 days, with a possible 30-day extension
c. seven days
d. 120 days

7. Your brother is worried about a friend's health. He asks you to find out whether the friend is taking any medications. What should you do?

a. ask the rest of the pharmacy staff whether they know anything about your brother's friend's health
b. log in to the computerized record system and read the patient's medication record to find information for your brother
c. explain that it's a violation of the patient's privacy for you to look up his record, and suggest that he call one of his friend's family members
d. none of the above

8. Under what circumstances are you free to repeat to others PHI that you hear on the job?

a. after you no longer work at the pharmacy
b. after a patient dies
c. only if you know the patient won't mind
d. when your job requires it

9. What should you do if you suspect someone is violating the facility's privacy policy?

a. nothing, it's none of your business
b. watch the individual involved until you have gathered solid evidence against him or her
c. report your suspicions to the privacy official or your supervisor, as outlined in the facility privacy policy
d. tell your coworkers so that they can keep an eye on the employee

10. When is the patient's authorization to release information required?

a. in most cases in which patient information is going to be shared with anyone for reasons other than treatment, payment, health care operations, or other disclosures permitted by HIPAA
b. at the patient's first visit to the pharmacy
c. when patient information is to be shared among two pharmacists
d. when patient information is used for billing a private insurer

11. Which of the following is PHI protected under HIPAA?

a. the patient's medical conditions and disease states
b. the patient's allergies
c. the patient's medication list
d. all of the above

12. Which of the following types of individually identifiable health information does HIPAA's privacy rule protect?

a. patient information in electronic form
b. patient information communicated orally
c. patient information in paper form
d. all of the above

13. Who should receive a copy of your pharmacy's notice of privacy practices?

a. all customers
b. anyone who requests a copy
c. both a and b
d. none of the above

14. What is the effective date of the HIPAA privacy rule?

a. April 14, 2003
b. April 14, 2004
c. January 1, 2004
d. August 1, 2003

15. Which of the following is a method for protecting patients' privacy?

a. turning computer screens away from public view
b. lowering your voice when discussing the details of a prescription
c. shredding paper that contains patient information
d. all of the above

16. What is the maximum penalty for selling patient information in violation of HIPAA?

a. one year in prison and a $1,000 fine
b. 10 years in prison and a $250,000 fine
c. a $100 fine
d. five years in prison

17. Which of the following is an acceptable reason to deny a patient's request to amend his or her PHI?

a. The PHI is not part of the designated record set.
b. The PHI is accurate and complete.
c. The pharmacy did not originally create the PHI, and the provider organization that did create it is available to respond to the request.
d. all of the above

18. How often does HIPAA allow a patient to receive an accounting of disclosures free of charge?

a. every 12 months
b. every six months
c. every two years
d. as often as the patient wants

19. Which of the following disclosures of PHI requires an authorization?

a. to a coroner or medical examiner
b. to an organ procurement organization to facilitate organ or tissue donation
c. to a pharmaceutical company for marketing
d. to law enforcement official for reports of suspected abuse

20. When should you share your password?

a. when your coworker forgets his or her password
b. never
c. when you know you can trust the person
d. when it will save time

_____

(Sign your name on the above line if you have completed this quiz.)

Answers to final exam

1. T
2. F
3. T
4. T
5. T
6. b
7. c
8. d
9. c
10. a
11. d
12. d
13. c
14. a
15. d
16. b
17. d
18. a
19. c
20. b

Related products

Books

HIPAA Compliance Handbook for Community Pharmacy

From the National Community Pharmacists Association. Written by Walter L. Fitzgerald Jr., BS, Pharm, MS, JD. To order, go to *www.ncpanet.org* or call 800/544-7447.

Handbooks

Train clinical staff and employees for the bargain rate of only $3.00 per person! (Minimum order: 100 handbooks)

HIPAA Training Handbook for Nurses/Clinical Staff: An Introduction to Confidentiality and Privacy under HIPAA

HIPAA's requirement for staff training and documentation of training can now be easily fulfilled with these convenient, pocket-sized handbooks! Staff trainers, privacy officials, compliance officers, and supervisors can easily teach and test nurses and clinical staff on HIPAA compliance by using *HIPAA Training Handbook for Nurses/Clinical Staff: An Introduction to Confidentiality and Privacy under HIPAA*.

HIPAA Training Handbook for the Health Care Staff: An Introduction to Confidentiality and Privacy under HIPAA

Staff trainers, privacy officials, compliance officers, and supervisors can easily teach and test general health care, administrative, and ancillary staff on HIPAA compliance by using the *HIPAA Training Handbook for the Health Care Staff: An Introduction to Confidentiality and Privacy under HIPAA*.

HIPAA Training Handbook for the Medical Staff: An Overview of HIPAA

Staff trainers, privacy officials, compliance officers, and supervisors can easily teach and test physicians, medical staff, and licensed independent practitioners on HIPAA compliance by using the *HIPAA Training Handbook for the Medical Staff: An Overview of HIPAA*. An examination found inside each of the handbooks (answer key included) can be kept on file to fulfill HIPAA's regulations.

Newsletters

Briefings on HIPAA: Analysis and advice about the privacy and security rules

From the publishers of *Medical Records Briefing*

Are you ready for the new rules under HIPAA that put strict controls on patient information? You will be with *Briefings on HIPAA: Analysis and advice about the privacy and security rules*.

Created exclusively for health care professionals who are in charge of information security or sit on information security

task forces, this newsletter will help you comply with the new law, including:

- Rewriting contracts with business associates, including attorneys, auditors, and consultants to make sure that they adhere to privacy rules.
- Telling patients about how their information is being used and whom it is being disclosed to.
- Restricting the amount of information used or disclosed to the minimum necessary to achieve the purpose of the use or disclosure.
- Establish privacy-conscious business practices.

Videos

Keep it to Yourself! Protecting Patient Confidentiality

Customize your own video!

Since the advent of the computerized patient record, the task of maintaining patient confidentiality has become more challenging than ever!

That's why The Greeley Company and Harvard Vanguard Medical Associates have collaborated to bring you *Keep It To Yourself! Protecting Patient Confidentiality,* a new 14-minute video training tool designed to orient all staff members to the importance of maintaining patient confidentiality.

Keep It To Yourself! Protecting Patient Confidentiality educates the entire staff about the importance of safeguarding the privacy of patient records.

The video also teaches how to identify and avoid common breaches of confidentiality. This new training resource provides real-life situations and techniques for ensuring that confidential records remain confidential.

This video is ideal for

- human resources directors
- medical records directors

Physician Compliance: It's Not an Option

Customize your own video!

An addition to the *Spotlight Series on Corporate Compliance*

Compliance isn't just a trend. It's here to stay. And it's not an option. Introducing a new video training tool to convey that message to the medical staff . . .

Truth be told, physicians look upon compliance efforts as an additional burden. But compliance is a necessary consideration for everyone working within a health care organization. Just look at the evening news or read the latest headlines. This new video is just the thing to bolster physician support for your corporate compliance program, in light of increased attention.

Physician Compliance: It's Not an Option takes a look at

- the physician's place in compliance efforts
- better documentation of care
- the role of the corporate compliance officer
- site-specific services
- proper coding and how to avoid upcoding

The medical staff is the first line of defense against fraud and abuse. Arm physicians with information on their role in compliance and their responsibility to report incidents of noncompliance.

To obtain additional information, to order any of the above products, or to comment on *HIPAA Training Handbook for the Pharmacy Staff*, please contact us at:

HCPro
P.O. Box 1168
Marblehead, MA 01945

Toll-free telephone: 800/650-6787
Toll-free fax: 800/639-8511
E-mail: *customerservice@hcpro.com*
Internet: *www.hcmarketplace.com*

Notes

Certificate of Completion

This is to certify that

_____

has read and successfully passed the final exam of

HIPAA Training Handbook for the Pharmacy Staff

Suzanne Perney
Vice President/Publisher