HIPAA Training Handbook for the Behavioral Health Staff:

An Introduction to Confidentiality and Privacy under HIPAA

OPUS COMMUNICATIONS
A Division of *hc*Pro

HIPAA Training Handbook for the Behavioral Health Staff: An Introduction to Confidentiality and Privacy under HIPAA is published by Opus Communications, Inc., a subsidiary of HCPro Corp.

ISBN 1-57839-204-7

Opus Communications 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.

Neither HCPro Corp. nor Opus Communications, Inc., is affiliated in any way with the Joint Commission on Accreditation of Healthcare Organizations, which owns the JCAHO trademark.

Lauren McLeod, Senior Managing Editor
Mike Mirabello, Senior Graphic Artist
Jacqueline Singer, Layout Artist
Jean St. Pierre, Creative Director
Kathryn Levesque, Director of Online Education
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:
Opus Communications
P.O. Box 1168
Marblehead, MA 01945
Telephone: 800/650-6787 or 781/639-1872
Fax: 781/639-2982
E-mail: *customerservice@hcpro.com*

Visit Opus Communications at its World Wide Web sites:
www.hcmarketplace.com, www.hcpro.com,
www.hcprofessor.com,* and *www.himinfo.com.

Rev. 08/2002

Contents

HCPro acknowledges the editing contributions of the Missouri Department of Mental Health.

HIPAA Training Handbook for the Behavioral Health Staff:

An Introduction to Confidentiality and Privacy under HIPAA

Intended audience:

- Nurses
- Mental Health Professionals
- Medical records, patient accounting, registration, and back office staff
- Human resources employees
- Dietary services staff
- Nursing assistants
- Housekeeping/facilities staff
- Trainees, students, and volunteers
- All other ancillary staff

Intended for general work force orientation and training, this booklet will acquaint workers in the hospital, patient registration area, lab, and other settings throughout the facility with the requirements for privacy, confidentiality, and information security under HIPAA as well as the potential consequences

of not complying. Case scenarios illustrate situations in which privacy and confidentiality may be breached.

What is HIPAA and what does it govern?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is federal legislation covering three areas:

1. Insurance portability
2. Fraud enforcement (accountability)
3. Administrative simplification (reduction in health care costs)

The first two components of HIPAA, portability and accountability, have been put into effect.

Portability ensures that individuals moving from one health plan to another will have continuity of coverage under pre-existing conditions clauses.

Accountability significantly increases the federal government's fraud enforcement authority in many different areas.

Two of the rules covered under the third component, **administrative simplification,** require administrative, technical, and policy changes to protect patients' privacy and the confidentiality of protected health information (PHI).

HIPAA's privacy and security regulations punish individuals or organizations that fail to keep patient information confidential. Until these regulations were enacted, there was no federal framework to protect patient information from being exploited for personal gain. Now, the Office for Civil Rights in the Department of Health and Human Services has been charged with enforcing the HIPAA privacy rule.

Enforcement

Breaking HIPAA's privacy or security rules can mean either a civil or a criminal sanction. Inadvertent violations, not resulting in personal gain, usually result in fines of up to $100 for each violation of a requirement per individual.

For instance, if the hospital accidentally released 100 patient records, it could be fined $100 for each record, for a total of $10,000. The annual limit for violating each identical requirement is $25,000.

Have you ever gained access to a high-profile patient's medical record to learn why he or she is hospitalized, or looked up a neighbor's medical history out of curiosity? Under HIPAA this could earn you or your organization a civil or criminal sanction and fine.

Criminal penalties for "wrongful disclosure" can include not only large fines, but also jail time. The penalties increase as the seriousness of the offense increases. In other words, selling PHI is more serious than accidentally letting it be released, so it brings stiffer penalties. These penalties can be as high as a $250,000 fine or a prison sentence of up to 10 years. For example:

- Knowingly releasing PHI in violation of HIPAA can result in a one-year jail sentence and $50,000 fine
- Gaining access to PHI under false pretenses can result in a five-year jail sentence and a $100,000 fine
- Releasing PHI with harmful intent or selling the information can lead to a 10-year jail sentence and a $250,000 fine

Your facility is committed to protecting patient privacy and confidentiality. When you fail to protect patient information and patient records by not following your organization's privacy and security policies, it reflects on your job performance. To learn more about the penalties for violating patient privacy and confidentiality, review your organization's privacy policy.

Why are privacy and confidentiality important?

No matter where you work in health care—the hospital, labs, regional centers, nursing homes, business units, or right in a patient home or other supported living situation, it's important to protect privacy and confidentiality as part of providing high-quality care.

Patients have the right to control who will see their PHI. This means that communication with or about patients involving their health information must be private and limited to those who need the information for treatment, payment, and health-care operations. Healthcare operations are activities that don't qualify as treatment or payment, but are closely related and a necessary part of an organization's functions. Examples include training employees, evaluating employee performance, and conducting medical record reviews. Only those people with an authorized need to know will have access to the protected information.

Hospitals and health care organizations have always upheld strict privacy and confidentiality policies. Unless you're new to health care, this idea will be familiar to you.

However, the U.S. government has strengthened the laws protecting privacy and confidentiality in response to situations in which private medical information has ended up in the wrong hands.

In North Carolina, an employer fired a good employee shortly after learning the employee had tested positive for a genetic

illness that could lead to lost work time and increased insurance costs.

In New York, a representative who had battled depression found out her medical history had been released to newspaper reporters.

Not surprisingly, cases of misuse of PHI have also caused lawsuits. A California woman sued a pharmacy that released her medical information to her husband, who used it to damage her reputation in a divorce. In another divorce case, a woman threatened to use information about her husband's health status that she obtained from his health records in custody hearings, forcing him to settle in order to avoid public discussion of his health.

As the number of cases of misuse of PHI rises, Congress has taken action to ensure that hospitals and health care providers protect health information privacy and confidentiality.

With the enactment of HIPAA, a patient's right to have his or her health information kept private and secure became more than just an ethical obligation of physicians and health care facilities—it became the law.

Ways to protect patient privacy

Whether they are in the hospital, physician's office, lab, or other setting, patients receiving medical care expect privacy.

This organization is committed to giving patients privacy. As you work here, you will see many ways we protect patient privacy.

- Patient care or discussion about patient care is kept private by closing room doors or drawing privacy curtains to reduce the likelihood of others overhearing them
- Patient medical records are not left where unauthorized individuals can gain access to them
- Laboratory, radiology, and other ancillary test results are kept private
- When patients are admitted or treated, they discuss their health concerns and treatment with a doctor or staff member privately
- Discussions with patients about their financial information during registration are kept confidential

This feeling of privacy is important to patients—many of whom will be uncomfortable in strange surroundings.

When carrying out your job assignments and meeting deadlines, remember that you don't want to jeopardize the confidentiality of patients' health information in the process.

Much of this is common sense. Knock on a door and ask before entering a room. Keep patient records locked away and out of public areas. If you find records unattended, return them to the appropriate staff.

If you need to page a patient, do not include information that can allow others to identify the patient's condition or reason for being there. Check your organization's policy to understand how to handle this.

If visitors ask you for information about a patient, direct them to the nursing supervisor or information desk for assistance rather than giving out patient names or locations yourself. Always check the facility's directory to ensure the patient has consented to be listed before disclosing any information.

Patients expect privacy when they receive health care. It's up to everyone at this organization to meet their expectations.

Case scenario #1

You are called to work in the psychiatric emergency room. The room has several people waiting for services, but only one male. The physician is discussing the male patient's condition—major depression and HIV—with a nurse. Everyone in the emergency room can overhear the conversation.

What should be done differently?

Mental health professionals should try to find a private area where they cannot be overheard. Even when the patient's name is not used, details about the patient, or in this case the use of the word "he," can identify the patient.

Case scenario #2

Mr. Jones, a patient in a long-term psychiatric facility has had an adverse reaction to his psychiatric medications. The supervising nurse tries several times to reach the patient's physician for instructions, with no success. Finally, she reaches the university where the physician is teaching an adjunct class. She asks the receptionist to tell the physician that Mr. Jones has had an adverse reaction to his psychiatric medications and that she urgently needs a call back.

What should the supervising nurse have done differently?

The nursing supervisor should have simply requested an immediate call back from the physician about an urgent patient matter. Leaving a message that provides any identifying details about the patient or his condition with someone other than the physician is a breach of confidentiality. Whether in person, on the phone, or via voicemail or an answering machine, never leave a message with a third party that contains specific information about a patient that can identify him or her.

Likewise, if a case manager meets a client for a monthly visit at the local coffee shop, and runs into a neighbor who asks what she is doing at the coffee shop, the case manager should not reveal that she is there with a consumer of mental health services.

Any questions?

For more discussion about your organization's privacy policies, refer to your employee handbook or organization policies. If a privacy issue arises and you are unsure about what to do, consult your supervisor or your privacy official.

Which of the following situations describe proper techniques for protecting a patient's privacy and confidentiality?

1. A doctor brings a patient into an unused room to discuss the patient's medical condition.
2. A doctor who is reviewing a patient's record leaves the folder in the doctor's lounge to review later.
3. A doctor e-mails a physician colleague to consult about a patient's condition. He explains the condition but omits any identifying information regarding the patient.

Answers: #1 and #3

What is confidential information?

When patients give information to their providers, they expect that only people involved in their health care will see it.

Confidential information includes the reason a person is sick or in the hospital, the treatments and medications he or she receives, and observations about his or her current or past health conditions.

What makes information identifiable?

Any information that might identify someone is called individually identifiable information under HIPAA. Elements that make information identifiable include the following:

- Names
- Addresses
- Employers
- Relatives' names
- Dates of birth
- Telephone and fax numbers
- E-mail addresses
- Social Security numbers
- Member or account numbers
- Certificate numbers
- Voiceprints
- Fingerprints
- Photos
- Codes
- Any other characteristics, such as occupation, which may identify the individual

Essentially, individually identifiable information is anything that can be used to identify a patient. Releasing any of this information for other than permissible purposes is a violation of the HIPAA privacy regulation.

How is patient information used?

The organization collects this information so that it can take care of patients and perform other related functions.

However, the facility and its work force can use it only in limited ways.

Obviously, doctors, nurses, therapists, dietitians, case managers, and other caregivers use information about patients to determine what services they should receive. In addition, the billing department uses confidential information to bill patients or their insurance companies for the services they receive. Other physicians and quality control directors review confidential information to make sure patients receive good care.

Generally speaking, other uses are not allowed. It's helpful to ask yourself before looking at any patient information: **Do I need this information to do my job and provide good patient care? What is the least amount of information I need to do my job?** This requirement to use or share only the "minimum necessary" is covered in the HIPAA privacy rule, section 164.502(b).

The minimum necessary requirement applies to uses and disclosures for reasons other than treatment. Clinical staff are allowed to look at their patient's entire medical record and share information freely with other clinicians involved in treating that patient.

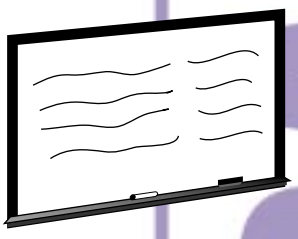
Who is authorized to see information?

All members of the work force at a hospital contribute to the quality of care. But that doesn't mean everyone needs to see patients' PHI.

Many employees have no access to patient information, either in computer or on paper. That's because they don't need to know the information. **"Need to know"** is an important phrase to remember.

If you do not need to know confidential patient information to do your job, you should not look at medical records.

But there still will be occasions when you may see or hear confidential information. For example, if a patient is placed in an isolation room, you may find out why he or she is there or you may suspect you know. This is confidential information about a patient that you should not communicate to anyone else.



The information about a patient's condition that you see written on whiteboards around the hospital is also confidential. It is used for giving care to patients and should only be in places where the public will not see it.

Because this information is confidential, you should not use it or reveal it to anyone, including coworkers, other patients, visitors, or anyone else unless it's part of your job to do so.

In the course of doing your job, you may also find that patients speak to you about their condition. Although there's nothing wrong with this, you must remember that they trust you to keep that information confidential, and you must not pass it on to the public.

Protecting confidential information is a responsibility that the entire work force shares, including volunteers, regardless of whether they are caring for patients.

Case scenario #3

Two residents receiving mental retardation/developmental disability services reside in the same group home. They do not always get along, and there is an allegation of a physical confrontation. One resident's mother is also her legal guardian. She calls you, the service coordinator, to talk about the situation, and asks specific questions about the other resident's diagnosis and behaviors.

What can you discuss with the resident's guardian?

You can discuss the behaviors exhibited by her ward and plans for addressing the situation from her ward's perspective. However, you cannot discuss anything specific about the other resident without that resident's authorization.

Case scenario #4

A friend is concerned because his girlfriend is in the hospital for an apparent overdose. Your friend calls asking about her. He is sure she is in your facility on a 96-hour commitment and asks you for information about her condition. She was extremely intoxicated when she was brought in and is currently undergoing detox services. He asks you to find out anything you can.

What should you do to protect this patient's privacy?

You should tell your friend that due to federal confidentiality regulations, you can not give him any information.

Do not even acknowledge that the girlfriend is in the hospital. Federal regulations govern the release of any alcohol and drug abuse information, and you are prohibited from giving out that type of information.

Remember that you are not to seek out PHI other than when required by your job. When it is made available to you, you are not to repeat it to anyone. Protecting patient confidentiality isn't just a hospital priority, it's the law.

Any questions?

Remember, if you decide to violate these policies, you can be sanctioned and prosecuted. Violating patient confidentiality is a crime under HIPAA.

For more information about how the hospital will respond to violations of this policy, consult your facility's privacy policies or privacy official.

Confidential information quiz
Circle the correct answer.

1. A patient's confidential information includes his or her

a. Social Security number
b. Address
c. Age
d. Name
e. All of the above

2. Which of the following phrases should you keep in mind when determining whether you should have access to patient information?

a. Disregard all patient information
b. Any information out in the open is public record
c. Need to know
d. All of the above

Answers: **1. e** and **2. c**

Authorization

Your organization must obtain authorization to use or share health information for purposes other than treatment, payment, and health care operations. By way of the authorization, which must be in writing, the patient voluntarily agrees to let your organization use or disclose the information only for a particular request or need. This is covered under HIPAA section 164.508.

Providers may not refuse to treat patients who won't sign authorization forms.

Authorization is also necessary to disclose psychotherapy notes, but it's not needed to disclose information for fundraising as long as the information is limited to individual demographics and dates of service and your organization or fundraising arm performs the fundraising.

Patients have the right to revoke their authorization at any time. They also may ask providers to restrict how their medical information is used to carry out treatment, payment, and health care operations, but providers are not required to agree.

Psychotherapy notes

Not all PHI is treated the same under the privacy rule. Psychotherapy notes have much stronger protections, because the personal notes of the treating psychotherapist can be damaging if they fall into the wrong hands.

The privacy rule defines psychotherapy notes in this way: "Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the individual's medical record.

Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

Helping patients understand their rights

It's important that patients understand how they can protect their own health information and how providers protect their information, so the HIPAA rule requires health care providers to provide notices telling patients how they will use their information.

The notice of privacy practices tells patients about the provider's privacy policies and practices. It also explains patients' right to gain access to their own records and request

amendments to them. HIPAA requires providers to make "good faith efforts" to obtain patients' written acknowledgement that they received a copy of the notice of privacy practices.

These notices must be posted in places where patients can see them. If patients have questions about how the organization uses information, you can direct them to these posted notices, or to the organization's privacy official.

Typical ways to protect confidentiality

Your organization uses many tools and policies to protect confidentiality, including the following:

- Records are kept locked, and only people with a need to see information about patients have access to them.
- Employees who use the computerized patient records must not leave their computers logged in to the patient information system while they are not at their workstations.
- Computer screens containing patient information must be turned away from the view of the public or people passing by.
- Posted or written patient information maintained in work areas such as nurses' stations is kept covered from the public.

- Discussions about patient care are kept private to reduce the likelihood that those who do not need to know will overhear.
- Electronic records are kept secure. The facility will monitor who gains access to records to ensure that they are used appropriately.
- Paper records must always be shredded or placed in closed receptacles for delivery to a company that destroys records for the facility. They must never be left in the garbage.

All of these are basic ways that the institution protects confidentiality. But truly protecting confidentiality depends upon you. You must not share information that you overhear or see in the course of our work. Doing so is a violation of the law.

Here are some common sense ways nurses and other clinical staff members can protect patient privacy:

- Close patient room doors when discussing treatments and administering procedures
- Close curtains and speak softly in semi-private rooms when discussing treatments and administering procedures
- Avoid discussions about patients in public areas such as elevators and cafeteria lines

- Do not leave messages on answering machines regarding patient conditions or test results
- Avoid paging patients using information that could reveal their health problems

The right to privacy is central to the organization's mission, and it's important to patients, many of whom will be uncomfortable in their strange surroundings.

Maintaining records

When PHI is in your possession, you are responsible for safeguarding it. Do not leave it unattended in an area where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic. If you have patient records for home visits, you must secure them when they are not with you.

When you finish using paper patient information, return it to its appropriate location such as the medical records department or the nursing station. When you are finished with electronic patient information, log off the system. Do not leave the information visible on an unattended computer monitor. When discarding paper patient information, make sure the information is shredded and, preferably, locked in a secure bin. Leaving paper patient information intact in a wastebasket or recycling bin can lead to a privacy breach. The wastebasket could get knocked over. The paper could fall off a recycle truck and blow down the street.

Case scenario #5

You are walking by a trash can and notice that a pile of photocopied records has been laid on top of the trash.

How should you handle this? Should you put the records in the shredder or secure disposal container?

The best response is to gather the records and take them to your supervisor. He or she will want to report this to the facility's privacy official so that the facility can try to find out why the records were disposed of improperly.

Case scenario #6

When entering a room containing records, you find that the door is unlocked.

Should you lock the door? How should you respond?

The best response is, again, to contact your supervisor or the security department staff and notify them of the unlocked door. They will follow up with the privacy official to find out why it was left unlocked.

Case scenario #7

You are approached by an individual who tells you he is here to work on the computers and wants you to open a door or point the way to a workstation.

How do you respond to this request?

The best response is to ask this person who his or her contact is at the facility. Often this is the information services director or the facilities manager. That individual can take the repairperson to the appropriate work area. If the repairperson does not know who the contact is, contact security or your supervisor, and he or she will be able to assist the repairperson.

Any questions?

Even if you are not gaining access to records yourself as part of your job, by being on the lookout for potential violations of confidentiality, you help the facility keep its commitment to patient privacy.

You should feel comfortable going to your supervisor or your organization's privacy official with any questions about how to respond in situations in which privacy or confidentiality seem to be at risk.

The security regulation and electronic information

HIPAA's Security and Electronic Signatures Standard rule sets forth regulations to protect health information that is stored or transmitted electronically.

The security regulations call for certain technologies to protect electronic individually identifiable health information. The regulations require organizations to do the following:

- Send and store information on public networks only in encrypted form
- Develop procedures by which it is possible to identify the senders and recipients of electronic data and ensure that they are authorized to receive and decrypt the information
- Use passwords or other authentication technologies to protect information from unauthorized users

Using e-mail on the job

Your organization has developed e-mail policies. Familiarize yourself with them if you use e-mail in your job. These policies will protect both confidentiality of information and the computers from viruses that can harm it.

Remember, work e-mail is not meant for personal use. Sharing or opening attached files from an unknown source 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 e-mail on the receiving end. Never send confidential information about a patient in an e-mail over a public network unless your organization allows it and has mechanisms in place to prevent interception and corruption. 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 systems

Passwords and other security features protect patient information by restricting access to the computer system to authorized users.

If you have password access to your employer's system, never share passwords or log in to the health information system using borrowed credentials. Letting someone else use your password or logging on and letting him or her use the system in your session may seem like a timesaver, but it's a violation of the rules. It's essential that the organization be able to tell who looks at what records. Don't write your password down, post it, or keep it where others can find it. These are all ways to put information at risk.

Make sure computer screens are pointed away from the public and that computers are not connected to the patient information system when they are not in use. If you notice screens and information that appear easy for passersby to see or read,

let the user or someone in the department know about the problem so that it can be corrected right away.

Never remove computer equipment, disks, or software from the facility even if you think they are no longer used, unless you have permission from your supervisor. Special processing is required to remove all patient information from computer equipment before it is discarded.

Case scenario #8

You enter an unattended work area and notice a password for the computer system is posted on the wall.

What should you do?

Notify your supervisor that a password appears to be publicly available. Mention that you are concerned this might allow unauthorized access to the computerized health records of patients. You or your supervisor should also notify your organization's security official.

Case scenario #9

You find a laptop computer in an unlocked facility vehicle parked on your facility's grounds.

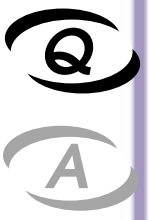
Should you remove the computer, lock the doors, or take some other action?

The best thing to do is to notify your supervisor immediately. Any unauthorized removal of facility

property may be considered theft, so under no circumstances should you take the computer out of the car without approval.

Case scenario #10

A contractor providing service coordination wants to be sure that its list of patients is consistent with the "official" list from your agency. The company's right to know this information has been verified. You are asked to run a computer report and then e-mail or fax the report to the contractor.



What should you do?

Since you've confirmed that they have a legitimate right to the information, providing the report is not a problem. However, sending it by e-mail or fax could pose a problem. If you send it by e-mail, it must be encrypted. If that is not possible, send a diskette or hard copy. If you use a fax, make sure you can send it to a particular person at a secure fax machine.

Helpful Hints to Use When Working with Computers

- Review your organization's policies on using computers.
- Don't use e-mail for personal matters.
- Never share or open attached files from an unknown source.
- Never send confidential patient information in an e-mail unless it is encrypted.
- Always double-check the address line of an e-mail before you send it.
- Never share your password or log in to the system under someone else's password.
- Always keep computer screens pointed away from the public.
- Never remove computer equipment, disks, or software from the facility unless you have permission.

Exceptions to the rules

You must be sure you know your organization's policies before releasing information. There are some cases in which patients do not have the right to keep their information private.

In some cases, your organization has a legal responsibility to release information regardless of the patient's wishes.

Seven reasons for releasing confidential patient information

1. Providers are required to report certain communicable diseases to state health agencies. The facility must report when patients have these diseases, even if the patients don't want the information reported.

2. The Food and Drug Administration (FDA) requires providers to report certain information about medical devices that break or malfunction.

3. Some states require physicians and other caregivers who suspect child abuse or domestic violence to report it to the police.

4. Police have the right to request certain information about patients to determine whether they are suspects in a criminal investigation.

5. The courts have the right to order providers to release patient information.

6. Providers must report cases of suspicious deaths or certain suspected crime victims, such as people with gunshot wounds.

7. The hospital or provider must report information to coroners and funeral directors in cases where patients die.

Understanding your role

In most cases, patients are informed when their health information is reported to police or others outside the facility, but these are cases in which they do not have the right to control their information.

In all of these cases, the facility complies with the law and reports information when necessary. Unless reporting this information is part of your job, you should not report this information yourself. Refer the request to your facility's medical records department or the privacy official.

If you are interested in more information about what your state requires, you may find it useful to contact your facility's privacy or security officer. That person can, if needed, check with legal counsel.

Summary

As an employee in this organization, one of your jobs is to help maintain privacy for patients as they receive care and help protect the confidentiality of the information patients give to their providers.

You are expected to not seek out information about patients unless you need it to do your job. There will be times when you will hear or see patient information in the course of doing your job. Remember that the information is confidential and you are not allowed to repeat it or share it with others. This applies even when you no longer work at this facility.

Reporting abuses

The organization expects all employees to adhere to the privacy and confidentiality policies, but it recognizes there may be times when the staff do not follow the policy.

Employees are encouraged to report violations or suspected abuses to the facility's privacy official. You may report violations anonymously, if you wish, by following the procedures in your privacy policy. 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 considered part of your job to report instances where you suspect the privacy or confidentiality policies are being broken.

Final exam

1. The criminal penalties for improperly disclosing protected health information can be as high as fines of $250,000 and prison sentences of 10 years.

True or false?

2. Why are confidentiality and privacy important concepts in health care?

a. They help protect hospitals from lawsuits.
b. They allow patients to feel comfortable sharing information with their doctors.
c. They avoid the confusion of having people other than a physician distributing information about a patient.
d. Both a and b

3. Which of the following are common ways employees protect patient privacy?

a. Closing patient doors
b. Knocking before entering a patient room
c. Using curtains to shield patients during treatment
d. All of the above

4. Sally is a long-term resident of a group home and has been receiving mental health services for many years. As her case manager, you have been concerned about some recent side effects of Sally's medication and you need to consult her doctor. What should you do?

a. Fax your concerns about Sally to the doctor's office.
b. Send the doctor an e-mail about Sally through the office receptionist.
c. Call the receptionist and ask that the doctor return your call as soon as possible.
d. Call the receptionist and leave a detailed message about Sally.

5. Confidentiality protections cover not just patients' health-related information, such as why they are being treated, but also information such as address, age, Social Security numbers, and phone number.

True or false?

6. You are approached by an individual who tells you that he is here to work on the computers and wants you to open a door for him or point the way to a workstation. How do you respond to this request?

a. Provide him with the information or access he needs.
b. Ask him who at the hospital has hired him and refer him to that person for assistance.
c. Call the police.
d. None of the above

7. Any employee or physician who violates the hospital privacy policy is subject to punishments up to and including firing or termination of work privileges.

True or false?

8. Which of the examples below is NOT a common work practice that protects the confidentiality of patient information?

a. Keeping computers logged out of the patient information system when not in use
b. Keeping records locked when not in use
c. Limiting the number of visitors who can see a patient
d. Limiting the people who can look at electronic patient records

9. Privacy laws have exceptions that allow physicians to report suspected cases of child abuse to the police when they are required to do so by other laws.

True or false?

10. 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 hospital
b. After a patient dies
c. Only if you believe the patient won't mind
d. When authorized for business purposes

11. 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.

12. Which of the following are common features designed to protect the confidentiality of health information contained in patient medical records?

a. Locks on medical records rooms
b. Password access to computerized records
c. Rules that prohibit employees from looking at records unless they have a need to know
d. All of the above

13. Computer equipment that has been used to store PHI must undergo special processing to remove all traces of the information before it can be discarded.

True or false?

14. Why do providers have a special concern now for protecting patient privacy?

a. Patients are suing more often when their information is released without their knowledge.
b. A new law makes it a criminal offense not to protect patient health information.

c. Health care workers have gotten sloppier than they were in the past about protecting privacy.
d. Both a and b

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

True or false?

Answers to the final exam

1. True
2. d
3. d
4. c
5. True
6. b
7. True
8. c
9. True
10. d
11. c
12. d
13. True
14. d
15. False

Related products from HCPro

Books

HIPAA Made Simple: A Practical Guide to Compliance

Learn how to implement a comprehensive and ongoing HIPAA compliance program in your organization! The goal of this book is to provide you with a practical guide to implementing the administrative simplifications regulations under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. It's geared toward helping to ease your workload in these demanding days of preparing for HIPAA compliance on top of all of your other responsibilities.

HIPAA Guidelines Policy and Procedure Manual

The compliance deadline for HHS' HIPAA privacy regulations is April 14, 2003. Are you ready to comply? You are with this 150-page, three-ring binder of charts, forms, logs, lists, policies, and procedures for your health care organization to document functional compliance with HIPAA's privacy standards, as well as other HIPAA regulations.

Newsletters

Briefings on HIPAA

Are you ready for the new rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that put strict controls on patient information? You will be with **Briefings on HIPAA.**

Created exclusively for health care professionals who are in charge of HIPAA this newsletter will help you comply with the new law, including

- rewriting contracts with business partners, 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
- establishing privacy-conscious business practices

Briefings on HIPAA will also provide practical information, such as how to monitor audit trails of patient records, manage security incidents, and conduct educational awareness programs.

Software

h-Mail: HIPAA Training E-Mails for the Whole Staff

An easy-to-use CD-ROM containing an entire year's worth of e-mails on HIPAA privacy compliance. The e-mails feature HIPAA Q&A's, quizzes, tips, training games, and contests that you can send to your entire health care facility.

HIPAA Privacy Self Assessment Tool for Hospitals Software

A software gap analysis tool that offers an easy way to find out what your hospital and individual departments need to do to meet the many HIPAA privacy regulations in the areas of treatment, billing, research, auditing, data collection, marketing, and more.

HIPAA Privacy Self Assessment 1-2-3 for Physician Practices

Use this CD-ROM software to easily find out what your physician practice needs to do to meet the many HIPAA patient privacy regulations. Start your HIPAA compliance now, before the April 2003 compliance deadline!

HIPAA Online Learning Courses, Quizzes, and E-books from *www.hcprofessor.com*

An Introduction to HIPAA Privacy and Security (3 RHIA/RHIT and CPHQ credit hours)

Effective April 14, 2001, organizations that deal with patient medical records will have to comply with the privacy and

security standards of HIPAA (compliance must be completed by 2003). Learn about the HIPAA regulations, policies and procedures, compliance dates and penalties, tips on how to work Medicare compliance hand-in-hand with HIPAA compliance, steps to preparing for the requirements in the areas of staff education, risk assessment, auditing, monitoring, and more. This course has been officially approved by AHIMA for RHIA/RHIT recertification!

Confidentiality and Privacy under HIPAA for Nurses/Clinical Staff

For nursing/clinical staff, this course teaches HIPAA privacy compliance; protecting patient confidentiality; recordkeeping and files; maintaining, viewing, sharing, and discarding records; methods for protecting electronic information; and more. Covers electronic, paper, and verbal disclosures.

Overview of HIPAA for the Medical Staff

For the medical staff, this course teaches HIPAA regulations, compliance and protection from liability, the AMA's stance on privacy, exceptions to confidentiality, rules for who is authorized to see information and how, protecting confidentiality electronically and through organizational policies, electronic signatures, business associates, and more.

Confidentiality and Privacy under HIPAA for Health Care Staff

For general and ancillary staff, this course teaches why privacy and confidentiality are important, what HIPAA is, who is

authorized to see confidential information, how to protect confidentiality, and more.

HIPAA Self-Assessment and Planning E-Book and CE Quiz (3 RHIA/RHIT and CPHQ credit hours)

Receive a detailed electronic book and CE quiz on the HIPAA legislation, including use, disclosure, consent; de-identified information; applications to business partners; authorization and identity verification; compliance assessment; and preparation for security and electronic signature standards, including technical security and confidentiality. The quiz in this e-book has been officially approved by AHIMA for RHIA/RHIT recertification.

HIPAA Self Assessment and Planning CE Quiz (3 RHIA/RHIT and CPHQ credit hours)

Receive the CE quiz to the e-book (see "HIPAA Self Assessment and Planning E-Book and CE Quiz").

HIPAA Training Compliance Package (6 RHIA/RHIT and CPHQ credit hours)

Three HIPAA training/education products for one low price: "An Introduction to HIPAA Privacy and Security" online course (see description on p. 40),"HIPAA Self-Assessment and Planning E-Book and CE Quiz" (see description above), and Keep It to Yourself video, which shows real-life situations and techniques for ensuring that confidential records remain confidential.

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 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.

To obtain additional information, to order any of the above products, or to comment on *HIPAA Training Handbook for the Behavioral Health Staff: An Introduction to Confidentiality and Privacy under HIPAA*, please contact us at:

Opus Communications, 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*

Certificate of Completion

This is to certify that

_____

has read and successfully passed the final exam of

HIPAA Training Handbook for the Behavioral Health Staff

Suzanne Perney
Vice President/Publisher