

HIPAA Training Handbook for the Nursing/Clinical Staff:

*An Introduction to Confidentiality
and Privacy under HIPAA*



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

Copyright 2002 Opus Communications, Inc., a subsidiary of HCPro Corp.

All rights reserved. Printed in the United States of America. 5 4 3 2 1

ISBN 1-57839-152-0

No part of this publication may be reproduced, in any form or by any means, without prior written consent of Opus Communications or the Copyright Clearance Center (978/750-8400). Please notify us immediately if you have received an unauthorized copy.

Opus Communications provides information resources for the healthcare 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.

Emily Sheahan, Managing Editor
Mike Mirabello, Senior Graphic Artist
Jean St. Pierre, Creative Director
Kathryn Levesque, Director of Online Education
Paul Nash, Executive Editor
Suzanne Perney, Publisher

Special thanks to Kate Borten, CISSP, President of the Marblehead Group, Inc.

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

Intended Audience	1
Overview: What is HIPAA?	2
What is HIPAA and what does it govern?	2
Enforcement	3
Why are privacy and confidentiality important?	5
Protecting privacy	8
The privacy regulation	8
Confidential information	9
What makes information identifiable?	9
Case scenario #1	10
Case scenario #2	11
Case scenario #3	12
Authorization	12
Psychotherapy notes	13
Ways to protect confidentiality	14
The minimum necessary standard	14
Ways to protect patient privacy	15
Maintaining records	16

HIPAA Training Handbook for the Nursing/Clinical Staff

The security regulation and electronic information	17
The security regulation	17
Ways to protect electronic data	17
Passwords	18
Case scenario #4	18
Case scenario #5	19
Faxes	19
Case scenario #6	20
E-mail	21
Exceptions to the rule	23
When reporting is required	24
Case scenario #7	24
Summary	25
Reporting abuses	25
Final exam	27
Answers to final exam	32
Related products	33

HIPAA Training Handbook for the Nursing/Clinical Staff:

*An Introduction to Confidentiality
and Privacy under HIPAA*

Intended Audience:

- Nurses
- Nurse practitioners
- LVNs
- MAs
- Therapists
- Technicians
- Pharmacy staff

Intended for nursing/clinical staff orientation and training, this booklet acquaints staff members with the requirements for confidentiality and information security under HIPAA as well as the potential consequences of noncompliance. The booklet covers workplace practices that may affect privacy and confidentiality. Case scenarios illustrate potential situations in which privacy and confidentiality may be breached.

Overview: What is HIPAA?

What is HIPAA and what does it govern?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a multifaceted piece of 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 and will not be denied coverage under pre-existing-condition clauses.

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



The third component, **administrative simplification**, is arguably the most significant part of the legislation, and is the focus of this booklet.

Administrative simplification received little attention when the law was first enacted because its implementation date

An Introduction to Confidentiality and Privacy under HIPAA

was later than the other two components'. But today, two of its rules, privacy and security, are generating much discussion and debate in the health care community. The debate stems from the administrative, technical, and policy changes that the rules require health care organizations to make to protect their 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.

HIPAA states that "covered entities" must comply with its regulations. Covered entities for HIPAA's privacy and security regulations include most providers, clearinghouses, and health plans. (You can find the definition of covered entity in the Privacy Regulation in section 160.103.)



Enforcement

Breaking HIPAA's privacy or security rules can mean either a civil or a criminal sanction. Civil penalties are fines of up to \$100 for each violation of a requirement per individual. For instance, if the hospital released 100 patient records, it could

HIPAA Training Handbook for the Nursing/Clinical Staff

be fined \$100 for each record, for a total of \$10,000. \$25,000 is the annual limit for violating each identical requirement.

Have you ever looked up a coworker's medical record to learn his or her birthday? Or read a neighbor's medical history out of curiosity? Under HIPAA this could earn your organization a civil penalty and a fine.

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



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

An Introduction to Confidentiality and Privacy under HIPAA

“Egregious violations” such as the sale of a celebrity’s medical record information to a tabloid newspaper or the sale of health information to marketing or pharmaceutical companies for personal profit, could result in criminal penalties.

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 policy, it can have an impact on your ability to do your job, your status with your organization, and your license to practice. You should carefully review your organization’s privacy policy and understand its requirements.

Why are privacy and confidentiality important?

Patients’ expectations of privacy and confidentiality are important to any, hospital, physician practice, lab, nursing home, pharmacy, or other provider organization. Under HIPAA, the hope is that educated patients will be able to trust their providers and the organizations in which they work. To build trust, HIPAA calls on covered entities to learn the rules for privacy and confidentiality and then live by them.

Communications with or about patients involving patient health information should be private and limited to those who need the information for treatment, payment, and health care operations. Health care operations are activities such as conducting medical record reviews, training health care professionals and evaluating staff performance that don’t qualify

HIPAA Training Handbook for the Nursing/Clinical Staff

as treatment or payment but are related to those functions and necessary for the organization operations. Only those 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 will be familiar to you.

But there are changes. The U.S. government has strengthened the laws protecting privacy and confidentiality in response to instances of private medical information getting into the wrong hands.

In North Carolina, an employer fired a good employee shortly after learning that the employee had tested positive for a genetic illness that could lead to lost work time and increased insurance costs.



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

Not surprisingly, cases of misuse of health information 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. And 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.

Protecting privacy

The privacy regulation

The privacy component of HIPAA protects individually identifiable health information that is transmitted or maintained in any form by covered entities. The regulations were published in the *Federal Register* on December 28, 2000.

Individually identifiable information is any information, including demographic information, that identifies an individual and meets any of or all of the following criteria:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse
- Relates to the past, present, or future physical or mental health or condition of an individual
- Describes the past, present, or future payment for the provision of health care to an individual

It's important to note that HIPAA's privacy regulation is not limited to health information maintained or transmitted electronically, but covers information written on paper or spoken.



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 friend about a patient's condition. He explains the condition but omits any identifying information regarding the patient.

Answer: # 1 and # 3

Confidential information

What makes information identifiable?

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

- Names
- Addresses
- Employers
- Relatives' names
- Dates of birth
- Telephone and fax numbers
- E-mail addresses

HIPAA Training Handbook for the Nursing/Clinical Staff

- Social Security numbers
- Medical record 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.

Case scenario #1

Consider the example of a male patient in the waiting room. He's the only male in the room. His physician is discussing his condition—testicular cancer—with a nurse, and everyone in the waiting room can hear the conversation.



What could have been done differently to protect this patient's privacy?



The caregivers should have tried to find a private room or area where details could not be overheard. Even when the patient's name is not specifically used in conversation, remember that details about his

or her case or condition can be identifying factors in certain circumstances.

Case scenario #2

Mr. Olsen, a patient in the facility, has had an adverse reaction to his medications. The nurse tries several times to reach the patient's physician for instructions, with no success. Finally, she reaches the club where the physician is attending a social event. She asks the receptionist to tell the physician that Mr. Olsen has had an adverse reaction to his medications, and she urgently needs a call back.



What should the nurse have done differently?



Leaving a message with someone other than the physician that provides any identifying details about the patient or his condition is a breach of confidentiality. If the person receiving the message knows Mr. Olsen, then information about his presence at the facility and his condition could lead to speculation about the patient. 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. The nurse should have simply requested an immediate call back from the physician about an urgent patient matter.

Case scenario #3

Susan is a nurse in the ER of a city hospital, and she has just heard through the grapevine that a fellow nurse is pregnant. The other staff members would like to give this nurse a baby shower, but nobody knows when the baby is due or whether it is a boy or girl. Susan has access to the records and could easily find the answers to both questions.



Should Susan try to get information about the pregnancy and share it with the staff?



Absolutely not. This is clearly an unauthorized use of medical information. Remember that you should never look at the records of patients you are not helping to care for.

Authorization

Authorization is required for the use and disclosure of health information for purposes other than treatment, payment or health care operations, such as releasing information to financial institutions that offer loans or selling mailing lists to marketing companies. This provision is outlined in section 164.508.

Patients have the right to revoke their authorization at any time. They 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 do so.

Psychotherapy notes

Not all protected health information 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. HIPAA requires individual authorization for the release of psychotherapy notes—even for treatment, payment, and health care operations.

The final privacy rule defines psychotherapy notes in this way:

“Notes recorded (in any medium) by a healthcare 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.”

Ways to protect confidentiality

The minimum necessary standard

Health care workers must make a reasonable effort to disclose or use only the minimum necessary amount of protected health information they need to do their jobs. This provision is outlined in the privacy rule in section 164.502(b).

Making minimum necessary determinations is a balancing act. Providers must weigh the need to protect patients' privacy against their reasonable ability to limit the information that is disclosed and deliver quality care.

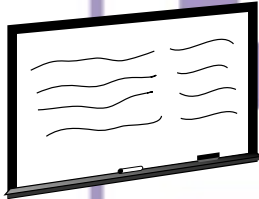
Before looking at patient information staff should ask themselves, "Do I need to know this to do my job?"

However, there is no minimum necessary requirement when it comes to treatment. Clinical staff are allowed to look at their patient's entire record and share information freely with other clinicians directly caring for that patient.

There will also be occasions when you will have access to confidential information that you don't need for your work.

For example, if a patient is placed in an isolation room, you may become aware of why he or she is there, or may suspect you know why. This is confidential information about a patient; do not communicate it to anyone else.

An Introduction to Confidentiality and Privacy under HIPAA



You may also see patient information on whiteboards throughout the facility. They are usually posted where the public cannot see them. In the course of providing patient care, you may work in areas where they are visible.

You must keep this information confidential. Do not disclose it to anyone, including coworkers, other patients, patient visitors, or anyone else who may ask.

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 what they tell you confidential. Do not pass it on.

Ways to protect patient privacy

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 elevators and cafeteria lines.

- Do not leave messages regarding patient conditions or test results on answering machines or with anyone other than the patient.
- Avoid paging patients using information that could reveal their health issues.

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

Maintaining records

When patient information 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.

When you are finished using paper patient information, return it to its appropriate location, i.e., the medical records department or a file at a nursing station. When you are finished looking at 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 or locked in a secure bin to be destroyed later. Leaving paper patient information intact in a wastebasket could lead to a privacy breach. The wastebasket

could get knocked over. The paper information could fall off a recycle truck and blow down the street.

The security regulation and electronic information

The security regulation

HIPAA's security rule sets forth regulations to protect health information 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
- Implement procedures by which it is possible to identify the senders and recipients of data and ensure they are known to each other and are authorized to receive and decrypt the information
- Use passwords or other authentication technologies to protect information from unauthorized users

Ways to protect electronic data

If you have access to electronic medical records, here are some ways to protect patient privacy:

- Use screen savers to block patient information displayed on unattended computer monitors
- Log off the system before you walk away
- Point computer monitors so that visitors or people walking by cannot view information



Passwords

Do not keep your password written down. Never share passwords with anyone. Avoid guessable names for your passwords, such as your last name or the name of your child. Change your password regularly according to your facility's policy.

Case scenario #4

It has been regular practice to leave the records system open and logged on at the nurses' station computer at the end of a shift. This saves time during shift changes for staff who need to retrieve records.



Is this an allowable practice under HIPAA?



No. It may be a timesaver, but this practice is not allowed. It is equivalent to sharing a password.

When many employees gain access to the system under the same password, there is no way to audit who sees

records. Generally, you shouldn't leave the system open when you leave the station.

Case scenario #5

A man tells you that he is here to work on the computers. He wants your password to log on to the electronic medical record system.



What do you do?



The best response is to ask the man who at the organization contacted him. The contact can take him to the appropriate area and give him the information he needs. If the repairman cannot tell you who his contact is, call your supervisor or the privacy official.

Faxes

HIPAA does not address faxing patient information specifically, but protects it under the privacy rule. Keep in mind that faxed patient information can easily fall into the wrong hands, which would be a violation of privacy. Before faxing any patient information, check with your supervisor to see if your facility has a policy that limits its use.

If you do fax patient information, make sure you are faxing it to a dedicated fax machine in a secure location and make certain that the person the information is being faxed to actually receives the fax. If you know you will receive a fax that contains patient information, tell the person faxing the infor-

mation 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 dispose of or file faxed information before others can see it.

Case scenario #6

You are just coming off of a double shift at the hospital, and a physician has asked you to fax her patient's lab test results to her office fax. The results are ready, but it's after hours in her office, and none of her office staff are available to receive the fax.



What do you do?



Don't send the fax to an unattended machine unless you have been assured that it is in a locked room or has a locked cover. You have no way to ensure that someone will not see the fax besides the physician or his staff. Talk with the incoming shift about handling the fax during office hours, and leave a message with the physician's office asking them to call for a fax of the results that were requested. Make sure not to leave the patient's name or other identifying information on the message.

E-mail

HIPAA does not ban the use of e-mail for sending patient information, but the security regulation does require organizations to put security mechanisms in place, including the use of password protection, encryption over the Internet, and technology that authenticates both the sender and receiver.

Check with your supervisor to see whether your facility has a policy for sending and receiving e-mail. Be sure to familiarize yourself with this policy if you use e-mail in your job. This policy will protect both confidentiality of information and the computers from viruses that can harm it.

Remember that 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 remember that you can never be sure who will have access to your e-mail on the receiving end. So never send confidential information about a patient in an e-mail unless it is permitted under your hospital's e-mail policy.

When you send e-mails, 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.

As with faxes, do not let printed e-mails lie around. Immediately dispose of printed e-mails after use or file them in the medical record, as appropriate.

Helpful Hints to Use When Working with Computers

- Review your organization's policies on using computers.
- Do not use work e-mail for personal messages.
- Never share or open attached files from an unknown source.
- Never send confidential patient information in an e-mail unless your facility has a policy that allows it and mechanisms in place to protect the information.
- Always double-check the address line of an e-mail before you send it.
- Never share your password or log on 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 rule

There are exceptional cases in which providers are required to release patient information regardless of whether the patient agrees, and the law allows that.

The following list gives the circumstances in which an organization may release information:

- There are laws that require providers to report certain communicable diseases to state health agencies. The provider must report when patients have these diseases, even if the patient doesn't want the information reported.
- The Food and Drug Administration requires providers to report certain information about medical devices that break or malfunction.
- Some states require physicians and other caregivers who suspect child abuse or domestic violence to report it to the police.
- Police have the right to request certain information about patients when conducting a criminal investigation.
- Certain courts have the rights, in some cases, to order providers to release patient information.

- Providers must report cases of suspicious deaths or certain injuries, such as gunshot wounds.
- Providers report information about patients' deaths to coroners and funeral directors.

When reporting is required

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

The organization complies with the law and makes reports when necessary. Unless reporting this information is part of your job, you should not report it yourself. Check with your supervisor when you have questions about whether a report is necessary.

If you are interested in more information about what your state requires, you might find it useful to contact the department of public health, attorney general, or your organization's privacy official.

Case scenario #7

You are a technician in the emergency room. A child is brought in with suspicious bruises and other injuries. You suspect that the child is being abused, but her mother insists she is not and begs you not to report the incident.



What should you do?



It's important to know your own state laws in this case. Check with your supervisor or your organization's privacy official, and that person can, if needed, check with legal counsel or the attorney general. If your state requires it, you should report cases of suspected abuse to the police. You should ensure, however, that the information goes only to the authorities necessary under the law. This exceptional need to report does not provide an open door to share the patient's information with others.

Summary

HIPAA requires organizations to have detailed policies and procedures in place that dictate how employees can use patient information, when they can disclose it, and how they should dispose of it. Be sure to read these carefully. If you have questions, see your supervisor or consult your organization's privacy official.

Reporting abuses

If a patient, a member of the public, or an employee suspect your organization is not complying with HIPAA, he or she may file a complaint with the Office for Civil Rights (OCR) in the U.S. Department of Health and Human Services. This provision is outlined in section 160.306(a).

A complaint must be filed in writing (either on paper or electronically) within 180 days of the date the complainant knew about the violation of privacy.

HIPAA Training Handbook for the Nursing/Clinical Staff

The OCR has the authority to audit an organization's privacy practices for HIPAA compliance, and will likely do so by reviewing your organization's policies and procedures and interviewing staff.

All organizations must also designate an individual who handles complaints. This person may or may not be the organization's privacy official.

You should feel free to contact this person if you think there are privacy violations occurring regularly in your organization. Ask your supervisor, or consult your organization's privacy policy, to find out who handles complaints in your organization.

SAFE
SAVING

Final Exam

1. Which area is not addressed by HIPAA?

- a. Insurance portability
- b. Hospital accreditation
- c. Fraud enforcement
- d. Administrative simplification

2. What are considered “covered entities” under HIPAA?

- a. Hospitals only
- b. Hospitals and payers only
- c. Most providers, clearinghouses, and health plans
- d. Accredited nursing homes, home health agencies, and hospitals only

3. What are the two kinds of sanctions under HIPAA?

- a. Egregious and inadvertent
- b. Criminal and civil
- c. Warranted and unwarranted
- d. Security and privacy

4. Which organization has been charged with enforcing HIPAA's privacy regulation?

- a. The Joint Commission on Accreditation of Healthcare Organizations
- b. The Office for Civil Rights
- c. The Centers for Medicare and Medicaid Services
- d. The Federal Bureau of Investigation

5. What kind of personally identifiable health information is protected by HIPAA's privacy rule?

- a. Written
- b. Electronic
- c. Spoken
- d. All of the above

6. Authorization is required to release psychotherapy notes for any reason including treatment.

True or False?

7. What does HIPAA say about faxing patient information?

- a. It can be done only among providers.
- b. All patient information must be de-identified.
- c. It is not allowed.
- d. None of the above

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

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

9. In which case is it acceptable for a hospital to release information without a patient's permission?

- a. When the patient is under 16 years old
- b. When the person requesting the information is a spouse, parent, or sibling
- c. When a provider suspects child abuse and state laws require providers to report suspected abuse
- d. None of the above

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

- a. In most cases when patient information is going to be shared with anyone for reasons other than treatment, payment, or health care operations
- b. Upon admission to a hospital

- c. When patient information is to be shared among two or more clinicians
- d. When patient information is used for billing a private insurer

11. You are working elsewhere in the hospital when you hear that a neighbor has just arrived in the ER for treatment after a car crash. What should you do?

- a. Contact the neighbor's spouse to alert him or her about the accident
- b. Tell the charge nurse in the ER that you know how to reach the patient's spouse and offer the information if it's needed.

12. Confidentiality protections cover not just a patient's health-related information, such as his or her diagnosis, but also other identifying information such as Social Security number and telephone number.

True or false?

13. If you suspect someone is violating the organization's privacy policy, what should you do?

- a. Confront the individual involved and remind him or her of the rules
- b. Watch the individual involved until you have gathered evidence against him or her.
- c. Report your suspicions to the organization's privacy or complaint officer, as outlined in your organization policy.

14. Computer equipment that has been used to store patient health information must undergo special processing to remove all traces of information before it can be disposed of.

True or false?

15. The minimum necessary rule applies to all uses and disclosures including those for treatment.

True or false?

Answers to the final exam

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



Related Products from HCPro

Books

The Long-Term Care HIPAA Lifeline: A Practical Guide on How to Comply

This book gives you HIPAA information the easy way—boiled down to the basics and written in plain English, making compliance as simple as possible. This book is one of the few HIPAA products available on the market that is geared specifically to long-term care facilities. A bonus CD-ROM has all of the forms and checklists you'll find in the book, making it easier to adapt them to your facility's needs.

This book was written by an attorney and reviewed by a long-term care professional. Reviewer Laurie A. Miller, CCS-P, is the privacy officer, medical records director, and head of HIPAA implementation and training at Columbia Basin Care Facility in The Dalles, OR. Her input helped the author ensure that the material is not only practical, but also easy to understand and implement. Author Kathy J. S. Fritz, RN, is a HIPAA specialist with 15 years of experience as a registered nurse and adult nurse practitioner, including roles as a direct-care provider and department manager.

HIPAA Training Handbook for the Nursing/Clinical Staff

This book will answer your urgent HIPAA questions, such as:

- How will HIPAA affect the MDS and billing?
- How will resident interactions change under HIPAA?
- How can I establish new HIPAA-compliant contracts?
- How can I write resident waivers to legally address long-term care privacy issues?

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

Created exclusively for health care professionals who are in charge of HIPAA compliance or sit on HIPAA task forces, this newsletter will help you comply with HIPAA, including

- rewriting contracts with business partners, including attorneys, auditors, and consultants to make sure that they adhere to privacy rules

An Introduction to Confidentiality and Privacy under HIPAA

- telling patients about how their information is being used and to whom it is being disclosed
- 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

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&As, 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!

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 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 training resource provides real-life situations and techniques for ensuring that confidential records remain confidential.

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

Long-Term Care Privacy for Beginners

Long-term care clinical, frontline, ancillary, and administrative staff who need only a basic understanding of the HIPAA regulations can get easy, accurate training with the online course **Long-Term Care Privacy for Beginners**, which covers the fundamentals of the HIPAA regulations, case examples, and a final exam that can help your facility meet HIPAA's training requirement.

Confidentiality and Privacy for Long-Term Care Managers and Licensed Staff

Long-term care administrators, managers, and licensed clinical care staff who need to understand the HIPAA regulations can get convenient, accurate training with this online course, which covers the most important aspects of the HIPAA regulations, including:

- What is HIPAA and what does it govern?
- What makes information "identifiable" under HIPAA?
- The minimum necessary standard
- Ways to protect resident privacy
- Maintaining records
- Ways to protect electronic data

***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. 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 on 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; record-keeping 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, who is authorized to see information and how, protecting confidentiality electronically and through organizational policies, electronic signatures, business associates, and more.

An Introduction to Confidentiality and Privacy under HIPAA

Confidentiality and Privacy under HIPAA for Health Care Staff

For general and ancillary staff, this course teaches why privacy and confidentiality are important, what is HIPAA, who is authorized to see confidential information, ways to protect confidentiality, and more.

Confidentiality and Privacy under HIPAA for Medical Records Staff

Train medical records, administrative, customer service, and ancillary personnel, as well as others who have substantial interaction with the medical record with this online course. The course will acquaint workers with the requirements for HIPAA privacy, confidentiality, and information security. The course covers the patient's rights granted by the HIPAA privacy rule. Thirteen case scenarios illustrate day-to-day issues related to HIPAA privacy compliance.

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 who and what is covered under the privacy and security standards; use, disclosure, consent; de-identified information; applications to business partners, authorization and identity verification, and administration; 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)***

Just get the CE quiz to the e-book (see “HIPAA Self Assessment and Planning E-Book and CE Quiz” on the previous page).

***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 above), “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.

Long-Term Care HIPAA Package

The Long-Term Care HIPAA Trainer’s Toolkit

This kit makes training staff on the HIPAA privacy and security regulations easy. In this comprehensive, yet easy-to-understand group of resources, you’ll get:

- *The Long-Term Care HIPAA Trainer’s Playbook*
- 20 copies of *HIPAA Training Handbook for Long-Term Care: Privacy for Frontline Staff*

An Introduction to Confidentiality and Privacy under HIPAA

- 20 copies of *HIPAA Training Handbook for Long-Term Care Managers and Licensed Staff: An Introduction to Confidentiality and Privacy under HIPAA*
- Ten copies of *HIPAA Daily Do's and Don'ts*, a 5" x 7" laminated cheat sheet to remind staff what they're allowed to do under HIPAA

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

**Opus Communications
P.O. Box 1168
Marblehead, MA 01945**

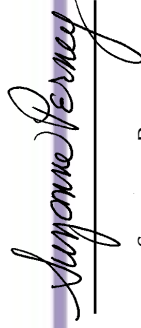
**Toll-free telephone: 800/650-6787
Toll-free fax: 800/639-8511
E-mail: customerservice@hcpro.com
Internet: www.hcmarketplace.com**

CERTIFICATE OF COMPLETION

This is to certify that

_____ has read and successfully passed the final exam of

HIPAA Training Handbook for the Nursing/Clinical Staff



Suzanne Perney
Vice President/Publisher

