HIPAA Training Handbook for Long-Term Care Managers and Licensed Staff:

An Introduction to Confidentiality and Privacy under HIPAA

OPUS COMMUNICATIONS
A Division of *hc*Pro

HIPAA Training Handbook for Long-Term Care Managers and Licensed Staff: An Introduction to Confidentiality and Privacy under HIPAA is published by Opus Communications, Inc., a subsidiary of HCPro Corp.

ISBN 1-57839-189-X

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.

Deborah L. Brown, RN, LNHA, Author
Christine Seymour, Senior Managing Editor
Mike Mirabello, Senior Graphic Artist
Jean St. Pierre, Creative Director
Kathryn Levesque, Director of Online Education
Kelly Wallask, 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.snfinfo.com.

Rev. 08/2002

Contents

About the Expert

Deborah L. Brown, RN, LNHA

Deborah Brown is a healthcare manager in the PostAcute Healthcare Advisory Services Group at American Express Tax & Business Services. She specializes in healthcare reimbursement and consulting. Ms. Brown's areas of expertise include regulatory compliance, implementation of the prospective payment system and the Minimum Data Set, and survey preparation.

Prior to her experience with American Express, Ms. Brown was director of nursing at Addolorata Villa in Wheeling, IL. While there, she managed all PPS, managed care, Medicaid, and private-pay insurance. She also developed a restorative rehabilitation program; created a plan to make the facility restraint-free; managed the physical therapy department; trained staff on coding and clinical computer programs; and developed a "Unit Coordinators" program.

Ms. Brown has also worked as an emergency room nurse, cardiac nurse, financial director, assistant administrator, business manager, and assistant comptroller at various health care organizations in the Chicago area.

HIPAA Training Handbook for Long-Term Care Managers and Licensed Staff:

An Introduction to Confidentiality and Privacy under HIPAA

Intended Audience:

- Owners
- Administrators
- All department heads
- Nurses
- LVNs/LPNs
- Therapists
- Directors of nursing
- Nursing management

Intended for nursing/clinical staff orientation and any managers conducting this training, this booklet will acquaint licensed staff and department heads with the requirements for confidentiality and information security under HIPAA as well as the common consequences of noncompliance. The

course covers workplace practices that may affect privacy and confidentiality, and the risks of breaching confidentiality. Case scenarios will 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 healthcare 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 will be the focus of this course.

Administrative simplification received little attention when the law was first enacted because its implementation date was later than the other two components. But today, two of its rules, privacy (which is finalized) and security (which is proposed), are generating much discussion and debate in the healthcare community. The debate stems from the administrative, technical, and policy changes that the rules require healthcare organizations to make in order to protect their residents' privacy and the confidentiality of protected health information (PHI).

Parts of HIPAA May Sound Familiar

You'll be happy to know that your facility is probably already meeting some of the HIPAA regulations for other reasons. After all, nursing homes must follow strict federal guidelines regarding confidentiality and privacy. Under the Code of Federal Regulations (CFR), facilities must meet the following conditions:

- **Resident rights (CFR section 483.10).** Residents must have access to all their records within 24 hours of oral or written request. They also have the right to personal privacy and confidentiality of their records. (Residents can refuse to allow the facility to release their records in most instances.)

  If you violate a resident's privacy or the confidentiality of his or her records, surveyors can cite you under Tag #F164.

- **Resident assessment (CFR section 483.20).** Automated resident assessments must be encoded within seven days of completion. Also, facilities can't release resident information to the public that would allow someone to identify the resident.

  As you probably know, surveyors can cite your facility under Tag #F516 if you do release resident-identifiable information.

- **Clinical records (CFR section 483.75).** The facility must protect clinical records from loss, destruction, or unauthorized use. All information in the records must be kept confidential.

And if your facility has a compliance plan, there's a good chance that it addresses resident privacy and records confidentiality. The Office of Inspector General guidelines for nursing homes establishing a compliance plan addresses resident confidentiality in its list of potential risk factors.

In addition, HIPAA's privacy and security regulations punish individuals or organizations that fail to keep resident information confidential. The Office for Civil Rights (OCR), in the Department of Health and Human Services (HHS) 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 are 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 usually fines from HHS/OCR (42USC & 1320d-5) . These are the result of "inadvertent violation," not necessarily resulting in personal gain. These penalties can result in fines of up to $100 for each violation of a requirement per individual. For instance, if the health facility released 100 resident records, it could be fined $100 for each record, for a total of $10,000. $25,000 is the annual limit for violating each identical requirement or prohibition.

Have you ever accessed a coworker's medical record to learn his or her date of birth? Or looked up a neighbor's medical history out of curiosity? Under HIPAA this could earn your organization a civil sanction and a fine. In some specific cases, even "inadvertent violations" can result in criminal sanctions.

Criminal penalties for "wrongful disclosure" can include not only large fines, but also jail time. (42USC & 1320D-6) – DOJ/U.S.) The criminal penalties increase as the seriousness of the offense increases. In other words, selling resident 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 resident 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 resident information with harmful intent or selling the information can lead to a 10-year jail sentence and a $250,000 fine

For instance, criminal penalties for "egregious violations" could result from 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.

Your facility is committed to protecting resident privacy and confidentiality. When you fail to protect resident information and resident 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 to be clear about its requirements.

Why are privacy and confidentiality important?

Residents' expectations of privacy and confidentiality are central to any provider organization that has access to resident-identifiable information, be it a hospital, physician practice, lab, nursing home, pharmacy, or other provider service or organization. Under HIPAA, the hope is that educated residents 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.

Confidentiality and privacy means that residents have the right to control who will see their protected, identifiable health information. This means that communications with or about residents involving resident health information will be private and limited to those who need the information in order to provide treatment, payment, and healthcare operations. Such communications may involve verbal discussions, written communications, or electronic communications. Only those people and computer processors with an authorized need to know will have access to the protected information. Nursing homes and other healthcare organizations have always upheld strict privacy and confidentiality policies. And unless you're new to healthcare, this idea will be familiar to you.

But there are changes. The U.S. government has begun to strengthen 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 the company learned 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.

As the number of cases of health information being misused rises, Congress has taken action to make healthcare providers do more to protect health information privacy and confidentiality.

And with enactment of the Health Insurance Portability and Accountability Act of 1996, or HIPAA as it's known, the idea that residents have the right to privacy and confidentiality became more than just an ethical obligation of health care organizations. It became the law.

What are my facility's policies and procedures for protecting resident privacy and confidentiality?

Protecting privacy

The privacy regulation

Regulations implementing the privacy component of HIPAA protect individually identifiable health information that is transmitted or maintained in any medium by covered entities. They were published in the *Federal Register* on December 28, 2000 and were updated in an August 14, 2002, *Federal Register* notice.

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 that is maintained or transmitted electronically, but also information conveyed on paper or via the spoken word.

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

1. A doctor brings a resident into an unused room to discuss the resident's medical condition.

2. A nurse who is reviewing a resident's record leaves the folder in the nurse's lounge to review later.

3. A doctor e-mails a physician friend about a resident's condition. She explains the condition but omits any identifying information regarding the resident

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

- names
- addresses
- employers
- relatives' names
- date of birth
- telephone and fax number
- e-mail address
- Social Security number
- medical record number
- member or account number
- 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 resident. Releasing any of this

information for other than permissible purposes is a violation of the HIPAA privacy regulation. For example, you cannot disclose a resident's condition, other than in general terms, such as "fair."

Case scenario #1

Family members are standing outside the resident's room. The hospice intake nurse is explaining the protocol for admitting a resident into the hospice program. Other visitors and staff are walking past them in the hallway.

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

This resident's case should have been discussed in a private room or area where details could not be overheard. Even when the resident'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 resident in the facility, has had an adverse reaction to his medications. The nurse tries several times to reach the resident'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 resident 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 him. Whether in person, on the phone, or via voicemail, never leave a message with a third party that contains specific information about a resident that can identify him or her. The nurse should have simply requested an immediate call back from the physician about an urgent resident matter.

Case scenario #3

Susan is the charge nurse on a unit. She was told by several certified nursing assistants (CNAs) that William, her best night CNA, was admitted to a local hospital. Susan's friend is the admissions clerk at the hospital. So, Susan decides to call her friend to find out why William was admitted.

Should Susan try to get information about William?

Absolutely not. This is clearly an unauthorized use of medical information. Remember that any time resident information is used for purposes other than treatment, payment, or operations, it must be authorized.

Notice of privacy practices and authorization

Notice of privacy practices

After HIPAA takes effect on April 14, 2003, one of the first things you should do when you admit a resident to your facility is give him or her a copy of the facility's notice of privacy practices. This is your facility's statement of how residents' protected health information might be used for treatment, payment, and health care operations—and it explains your residents' privacy rights.

But handing the resident a copy of the notice isn't good enough. After April 14, 2003, you'll also have to make a good faith effort to get a signed acknowledgement from the resident that he or she received the notice (some facilities might develop forms that you can ask residents to sign after they've read the notice). At this point, the resident can also ask for further restrictions on how the facility uses his or her information.

Just be aware that your facility can't provide care to residents before they have received the notice and you made a good faith effort to have them sign an acknowledgement. The exception is emergency care. In that case, your facility can try to obtain a signed acknowledgement as soon it's reasonably able to after the emergency treatment.

You won't have to do this every time you provide treatment to a particular resident, though—just the first time.

Also, you should know that some states and individual facilities might require an additional layer of notification: a consent program. These may vary from facility to facility or from state to state. But in general they require that residents sign a form giving the facility their consent to use their protected health information for treatment, payment, and health care operations.

Authorization

Authorization is required for the use and disclosure of health information for business-related purposes, 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 of the final rule.

Authorization is also required to disclose psychotherapy notes, but it's not necessary to disclose information about an organ donor or a deceased resident, or for fundraising, as long as the information is limited to individual demographics or dates of service.

Residents have the right to revoke their authorization at any time. And they may ask providers to restrict how their medical information is used to carry out treatment, payment, and health care operations.

Anyone besides the resident requesting access to resident health information must submit an authorization form to the facility.

Psychotherapy notes

Not all protected health information is treated the same under the privacy rule. Psychotherapy notes have much stronger protections. The rationale? Personal notes of the treating psychotherapist can be damaging if they fall into the wrong hands; they're also of little or no use to those absent from therapy sessions. Under HIPAA, the general consent for treatment, payment, and health care operations isn't adequate for psychotherapy notes. Instead, the law requires individual authorization.

The final 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."

Ways to protect confidentiality

The minimum necessary standard

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

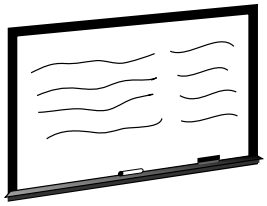
However, they can disclose information requested by other health care providers if the information is vital for treatment. To determine what is necessary to be disclosed and what should be withheld, consider the following questions:

- How *much* information are you planning to use or disclose?
- By using the information, will the number of people who are likely to have access to that information increase?
- How important is it that you use/disclose this information?
- What's the likelihood that further uses or disclosures could occur?
- Where is the information being disclosed (location) and in what form (e-mail, conversation, fax)?

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

There is no minimum necessary requirement when it comes to treatment. But there still will be occasions when you will have access to confidential information that you don't need for your work.

For example, if a resident 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 resident; do not communicate it to anyone else.



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

You must keep this information confidential. Do not use it in any way, and do not disclose it to anyone, including coworkers, other residents, visitors, or anyone else who may ask.

In the course of doing your job, you may also find that residents speak to you about their condition. While 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 resident privacy

Here are some common sense ways clinical and nonclinical staff members can protect resident privacy:

- Close resident 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 residents in elevators and cafeteria lines
- Do not leave messages on answering machines regarding resident conditions or test results
- Avoid paging residents using identifiable information, such as their condition, name of physician, or unit, that could reveal their health issues

The right to privacy is essential to the organization's mission, and it's important to residents, many of whom will be uncomfortable or confused in their surroundings.

Maintaining records

When resident information is in your possession, you are responsible for keeping it safeguarded. 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 done using paper resident information, return it to its appropriate location, i.e., the medical records department or a file at a nursing station. When you are done accessing electronic resident information, log off the system. Do not leave the information visible on an unattended computer monitor.

When discarding paper resident information, make sure the information is shredded and, preferably, locked in a secure bin. Leaving paper resident information intact in a wastebasket can lead to a privacy breach. What if the wastebasket is knocked over and the information is not placed back along with the rest of the contents? What if the paper information falls off a recycle truck and blows down the street?

The security regulation and electronic information

The security regulation

HIPAA's Security and Electronic Signatures Standard proposed rule (published in the August 12, 1998 *Federal Register*) sets forth regulations to protect health information that is stored or transmitted electronically. The Department of

Health and Human Services expects to release the final version of these regulations by the end of 2002.

The proposed security regulations call for certain technologies to protect electronic individually identifiable health information. The regulations require organizations to

- send and store information on public networks only in encrypted form. When transmitting resident information to the Common Working File, it must be encrypted. This is already being done by your state's computers.

- have procedures by which it is possible to identify the senders and recipients of data and ensure that they are known to each other and are authorized to receive and decrypt the information. Nursing home requirements state that the file being transmitted must be identified prior to transmission to identify who may review the file.

- use passwords or other authentication technologies to protect information from unauthorized users.

Your information technology department should be working on ensuring that this technology is employed by 2003, if it is not in use already.

Ways to protect electronic data

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

- Use screen savers to block resident information that is displayed on unattended computer monitors. (Better yet, log off the system before you walk away.)
- Point computer monitors so that visitors or people walking by cannot view information.
- Send and store information on public networks only in encrypted form.

Passwords

Do not post passwords on monitors or walls, and do not leave them in easily discovered places. 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.

Case scenario #4

It has been the practice to leave the records system open and logged on at the various computer stations for staff to save time when entering data into the system.

Is this an allowable practice under HIPAA?

Although it may seem to be a timesaver, this practice is equivalent to sharing a password. Remember that when others are allowed to access the system under your password, there can be no way to audit who sees records when. Never stay logged on to the system beyond the end of your shift. Generally, you shouldn't leave the system open when you leave the station for any reason.

Case scenario #5

An individual 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?

Before giving this person access, make sure he has passed through the appropriate clearance. Before giving this person access, make sure he has passed through the appropriate clearance. Call your supervisor or privacy officer to see whether this individual has signed a confidentiality agreement and a business associate agreement. If you are unsure of the individual's identity and his reason for requesting access, contact security or your organization's privacy officer.

Faxes

HIPAA does not address faxing resident information specifically, but, like any form of health information, it is protected under the privacy rule. Staff need to understand that faxed resident information can easily fall into the wrong hands, which would be a violation of privacy. Before faxing any resident information, check with your supervisor to see if your facility has a policy that limits its use.

If you do fax resident 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 resident 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 resident 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 nursing home, and a physician has asked you to fax his resident's lab test results to his office fax. The results are ready, but it's after hours in his office, and none of his 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 resident's name or other identifying information on the message.

E-mail

HIPAA does not ban the use of e-mail for sending resident information, but the proposed 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 if 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 performance of your job. This policy will protect both confidentiality of information and the computers from viruses that can harm it.

Remember that in your role at 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 resident in an e-mail unless it is coded.

When you send e-mails, always double-check the address line just before sending the message. 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.
- E-mail is not for personal use.
- Never share or open attached files from an unknown source.
- Never send confidential resident information in an e-mail unless it is encoded.
- Always double-check the address line of an e-mail before you send it. If you use a password to access the organization's computer system, 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

The rule is that in no case should you release confidential resident information outside the nursing facility or discuss it with anyone if it is not needed for treatment, billing, or operations. That's important to remember. But there are

exceptional cases in which providers are required to release resident information, and the law allows that.

The following list gives the conditions 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 residents have these diseases, even if the resident doesn't want the information reported.
- The Food and Drug Administration requires certain information about medical devices that break or malfunction to be reported.
- Some states require physicians or other people who provide resident care who suspect child abuse or domestic violence to report it to the police.
- Police have the right to request certain information about residents to determine whether they should consider the residents suspects in a criminal investigation.
- Certain courts have the rights, in some cases, to order providers to release resident information.
- The provider reports information about residents' deaths to the state clergy and funeral directors.

When reporting is required

In most cases, residents are informed when their health information is being 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 these cases, the organization complies with the law and makes reports when necessary. Remember, unless reporting this information is part of your job, you should not report this information 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 officer.

State requirements:

Case scenario #7

A family member brings her mother into your facility for admission. The resident has a bruise on her cheek and is speaking of how poorly she is treated at home. The daughter says, "Mom is confused." Upon admission to her room, the admitting nurse doing the assessment discovers multiple bruises on the resident's upper arms. The staff suspect abuse.

What should you do?

It's important to know your own state laws in this case. Check with your administrator or privacy officer, and that person can, if needed, check with legal counsel or the attorney general. If your state requires reporting, cases of suspected abuse must be reported 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 resident's information with others.

Summary

HIPAA requires organizations to have detailed policies and procedures in place that dictate how resident information is to be used, when it can be disclosed, and how it should be disposed of. Be sure to read these policies carefully. If you have questions, see your supervisor or consult your organization's privacy officer.

Reporting abuses

If a resident, a member of the public, or an employee suspects 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.

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 officer.

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.

On the following pages, you will find an exam you can use to make sure you understand the material presented in this pamphlet. If you're training other staff, use the quiz to test

their understanding. The answer page can be removed if you're using this as a competency test. Remember that this pamphlet serves as an overview of the privacy rules of HIPAA and does not necessarily ensure competence on all the regulations.

Final Exam

1. Which area is not addressed by HIPAA?

a. Insurance portability
b. Accreditation by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
c. Fraud enforcement
d. Administrative simplification

2. What are considered "covered entities" under HIPAA?

a. Hospitals
b. Hospitals and payors
c. Most providers, clearinghouses, and most health plans
d. Only nursing homes, home health agencies, and hospitals

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 Healthcare Financing Administration
d. The Federal Bureau of Investigation

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

a. Paper
b. Electronic
c. The spoken word
d. All of the above

6. Under HIPAA, what is an example of a "healthcare operation"?

a. Some fundraising activities
b. Medical record reviews
c. Billing
d. Accreditation surveys
e. All of the above

7. What does HIPAA say about faxing resident information?

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

8. Which of the following are some common features designed to protect confidentiality of health information contained in resident 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 nursing home to release information without a resident's permission?

a. When the resident is under sixteen years old
b. When the person requesting the information is a spouse, parent, or sibling
c. When a provider suspects abuse
d. None of the above

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

a. In most cases, when resident information is going to be shared with anyone for reasons other than treatment, payment, or healthcare operations
b. Upon admission to a hospital
c. When resident information is to be shared among two or more clinicians
d. When resident information is used for billing a private insurer

11. Confidentiality protections cover not just a resident's health-related information, such as his or her diagnosis, but also other identifying information such as social security number and telephone numbers.

True or false?

12. If you suspect someone is violating the organization's privacy policy, you should

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

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

True or false?

14. When disclosing resident information to another provider for the provision of treatment, should you limit the information you provide?

- No, you should provide whatever information the other provider requests.
- Yes, you should provide only the minimum amount of information necessary for treatment. You don't have to limit information for treatment under HIPAA. However, good practice and most policies today still say consider what's being asked. (e.g, Don't send the whole record if only the current medical problem is involved.)

Answers to the final exam

1. B
2. C
3. B
4. B
5. D
6. E
7. D
8. D
9. C
10. A
11. True
12. C
13. True
14. Yes

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 for 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.

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?

The Long-Term Care Compliance Manual

This easy-to-use resource goes beyond theory to bring you the practical, nuts-and-bolts advice on how to build a solid corporate compliance program. **The Long-Term Care Compliance Manual** will provide you with

- guidance in establishing the seven elements required of every compliance program
- sample forms and proven policies to mitigate the risk of fraud and abuse in your facility
- the tools you need to evaluate the effectiveness of your program

Newsletters

Briefings on Long-Term Care Regulations

This newsletter reports on the ever-evolving world of long-term care and helps readers thrive in an industry undergoing constant change and overburdened by regulations. Each issue of **Briefings on Long-Term Care Regulations** delivers essential information on topics that are most important to an administrator's professional success, including

- the latest news on PPS
- HIPAA updates
- CMS regulations

- innovations in quality care
- corporate compliance
- staff recruitment and retention

Briefings on HIPAA

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 HIPAA, 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
- establish privacy-conscious business practices

Briefings on Assisted Living

This monthly publication is the first newsletter dedicated to providing expert news, analysis, and advice about best practices in operations and development of assisted living facilities. Readers are the first to know about new initiatives and policies affecting the assisted living industry-in time to comply. From recruiting, training, and retaining staff to keeping your facility at maximum occupancy while satisfying state and federal inspectors, **Briefings on Assisted Living** helps manage on-the-job challenges and offers strategic solutions that improve day-to-day operations and positively affect your bottom line.

Video

Long-Term Care Corporate Compliance: Playing Your Part

Part of our award-winning Spotlight on Compliance series, **Long-Term Care Corporate Compliance: Playing Your Part** focuses specifically on corporate compliance in long-term care. It focuses on the OIG's Compliance Program Guidance for Nursing Facilities, which identifies a wide range of risk areas that relate specifically to long-term care. The video combines compelling, true-to-life scenarios that show how different staff members play a part in corporate compliance with expert advice and easy-to-remember guidelines for handling any compliance concern.

HIPAA Online Learning Courses from *www.hcprofessor.com*

Long-Term Care Privacy for Beginners

Long-term care clinical, frontline, ancillary, and adminstrative 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

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**
- 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