September 2011 Vol. 9, No. 9

CNA TRAINING ADVISOR From HCPro

# HIPAA and resident confidentiality

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and required complete regulatory compliance on the part of all healthcare providers by April 2003.

Under HIPAA, all healthcare workers are required to uphold the **privacy, confidentiality,** and **security** of every person's healthcare information, which of course includes long-term care residents.

This issue will explain the meaning of **covered entities** under HIPAA and describe the type of data that constitutes **protected health information.** It will also cover the difference between authorization and resident consent.

All CNAs should familiarize themselves with the general HIPAA rule of thumb: **the right information, to the right person, for the right reasons.** CNAs will also learn techniques for safeguarding information and how to maintain confidentiality in the nursing home.

Have a good day of training, and stay tuned for next month's issue of **CNA Training Advisor,** which will cover end-of-life care.

## PROGRAM PREP

### Program time

Approximately 30 minutes

### Learning objectives

Participants in this activity will learn how to:

- Uphold the privacy, confidentiality, and security of residents' protected health information
- Summarize the critical components of HIPAA
- Meet the specific challenges of HIPAA in the nursing home setting

### Preparation

- Review the material on pp. 2–4
- Duplicate the **CNA Professor** insert for participants
- Gather equipment for participants (e.g., an attendance sheet, pencils, etc.)

### Method

1. Place a copy of **CNA Professor** and a pencil at each participant's seat
2. Conduct the questionnaire as a pretest or, if participants' reading skills are limited, as an oral posttest
3. Present the program material
4. Review the questionnaire
5. Discuss the answers

## Be mindful of what's left in the open

Think of all the sensitive resident information you deal with daily, most notably residents' protected health information (PHI). Much of it is shared and stored electronically; however, some PHI is found on clipboards and in hard copy files. As a CNA, it is important to remember that these items cannot be left out in the open. When not in use, they should be returned to the proper storage location.

# HIPAA AND RESIDENT CONFIDENTIALITY

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which is now standard practice for every healthcare institution in the country. In a nutshell, the law requires healthcare facilities to uphold the privacy, confidentiality, and security of every person's healthcare information:

- **Privacy** refers to who should and should not have access to health information. Residents have the right to privacy, meaning that information about them should be available only to people who need it to provide care.
- **Confidentiality** refers to preventing someone from hearing or seeing a person's private health records and information unless he or she has the proper authorization. All health information is confidential. Anyone who possesses personal health information is responsible for protecting it.
- **Security** is the means used to provide privacy and confidentiality. The purpose of security is to ensure that only authorized individuals may access personal health information.

More and more of today's health information is in the form of electronic data, either instead of or in addition to traditional paper files.

Facilities must protect data sent from state to state via telephone or over the Internet, and federal laws make sure that every state and provider follows the same rules for privacy, confidentiality, and security.

## Navigating HIPAA

HIPAA rules must be obeyed by the following public and private organizations:

- Health plans and health insurance companies (e.g., HMOs and preferred provider organizations)
- Healthcare clearinghouses (e.g., billing services)
- Healthcare providers (e.g., doctors, dentists, chiropractors, therapists, hospitals, nursing facilities, clinics, pharmacies, home health agencies, hospices, and long-term care or personal care facilities of any type or size)

The HIPAA rules refer to these organizations as covered entities. The privacy protections of HIPAA apply to protected health information (PHI), which includes the following:

- Information created or received by a covered entity or an employer that relates to a person's past, present, or future health condition, health treatment, or payment for healthcare services
- Information that can identify an individual (e.g., name, address, telephone number, date of birth, diagnosis, medical record number, Social Security number, employer, position, or other identifying data)
- The resident record

PHI can be in any format (i.e., paper, electronic, or oral). If a provider wants to disclose a person's PHI for the purposes of providing healthcare, the provider must obtain that person's consent.

These purposes include routine healthcare-related uses of the information, such as when a doctor consults with another doctor in order to provide better care for an individual.

If a covered entity wants to disclose a person's PHI for purposes other than providing care, the covered entity needs that person's specific authorization.

The difference between consent and authorization is that to give consent, a resident must sign a form only once for each provider. The consent will apply whenever that provider discloses the person's PHI for purposes of providing healthcare.

Authorization, on the other hand, is required for each specific instance in which a covered entity wants to use or disclose a person's PHI for purposes not related to providing healthcare.

The HIPAA Privacy Rule generally permits covered entities to disclose healthcare information without a person's specific authorization in the following situations, depending on state or local law:

- Emergencies
- Public health needs (e.g., infectious disease registries)
- Mandatory reporting of child or elder abuse and neglect
- Judicial and administrative proceedings
- Substantial communication barriers

If there is no state or local law specifically requiring disclosure of information in the instances listed above, covered entities are required to use professional judgment in deciding whether to disclose information and exactly how much to disclose.



**CNA Training Advisor** (ISSN: 1545-7028 [print]; 1937-7487 [online]) is published monthly by HCPro, Inc., 75 Sylvan St., Suite A-101, Danvers, MA 01923. Subscription rate: $149/year; back issues are available at $15 each. • Copyright © 2011 HCPro, Inc. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro, Inc., or the Copyright Clearance Center at 978/750-8400. Please notify us immediately if you have received an unauthorized copy. • For editorial comments or questions, call 781/639-1872 or fax 781/639-7857. For renewal or subscription information, call customer service at 800/650-6787, fax 800/639-8511, or e-mail: *customerservice@hcpro.com*. • Visit our website at *www.hcpro.com*. • Occasionally, we make our subscriber list available to selected companies/vendors. If you do not wish to be included on this mailing list, please write to the marketing department at the address above. • Opinions expressed are not necessarily those of **CTA.** Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.

A covered entity must allow a person to view and photocopy his or her PHI if that person submits a request. An organization may charge the person for copies of records.

In a few special circumstances, such as when a covered entity has compiled information for use in a civil, criminal, or administrative proceeding, that entity does not have to give a person access to his or her PHI.

A covered entity may deny a person access to PHI if it has reason to believe that access would create a risk to that person's health.

If a person believes that his or her PHI contains information that is incorrect, he or she may ask the covered entity to make changes. The covered entity may deny the request if it believes that the current information is accurate and complete, or if it did not create the information. Covered entities are also required to do the following:

- Notify residents about their privacy rights. This can be done by producing a clear, written explanation of how the provider may use and disclose the resident's health information.
- Adopt written privacy procedures that clearly define who has access to PHI, how the entity will use the information, and when the entity might disclose the information to others
- Train employees so that they are fully aware of the privacy procedures
- Implement safeguards to prevent intentional or accidental misuse of PHI
- Appoint an individual to make sure employees follow the privacy procedures
- Give an account of instances in which the entity has disclosed PHI for purposes other than treatment, payment, or healthcare operations

## Protecting resident privacy and confidentiality

Quality resident care requires communication among healthcare workers. Computers, the Internet, e-mails, and faxes make it easier to share resident records.

However, this information is often readily available to anyone who happens to walk past a fax machine or a computer.

Some people fear that the exposure of their personal health information could result in job discrimination, personal embarrassment, or the loss or denial of health insurance.

Confidentiality of information, whether in written, electronic, or verbal form, is a priority. Confidentiality should extend to all health information, and you should handle all resident records as though they are confidential at all times. Do not leave them open where unauthorized people can see them.

The rule of thumb for HIPAA compliance is the right information, to the right person, for the right reasons. Keep the following in mind:

- You should learn the safeguards that your organization requires for the use, disclosure, and storage of personal health information. Know your organization's privacy policies and procedures.
- Individuals have the right to know and decide who may have access to their health information and under what circumstances they may have it.
- Discuss resident information in a private place so others cannot overhear the conversation.
- A cover sheet marked "confidential" should accompany all faxed information.
- When e-mailing information about a resident, remove any detailed identifying information. For example, refer to the resident either by his or her initials or internal resident number, rather than his or her full name.
- Only authorized personnel should enter confidential medical information into a computer-based resident record. Computer systems should be password protected to help guard against unauthorized access and use.

- Use only objective, precise language when documenting in the resident record. Avoid casual remarks and abbreviations that might be misunderstood.
- Always take the utmost care to protect the privacy and confidentiality of all health information. Be aware of who is around you while you are working and do not allow unauthorized people to hear or see any personal health information.
- Think about how you would want your personal health information treated, or that of an immediate family member, and give your residents that much protection and more.

## Challenges in the nursing home setting

Maintaining resident confidentiality can prove to be difficult in healthcare facilities, especially in nursing homes. Often, residents share bedrooms, the dining room, and lounge areas with others. As a result, roommates, staff members, and visitors are able to overhear almost everything that takes place in residents' rooms and common areas. Because of this, residents are often unable to express their needs and emotions in private. In many cases, their most intimate conversations can be overheard by others.

This makes it a real challenge for nursing home staff to keep residents' personal information confidential and respect their privacy. However, federal nursing home regulations require that staff provide care in such a way that preserves or builds each resident's dignity and self-respect. In addition to HIPAA, these regulations also require nursing homes to keep each resident's personal and medical records private and confidential.

Resident privacy can be easily violated if staff members are not careful. Remember that good nursing practice includes making sure that residents are subjected to as little loss of confidentiality and privacy as possible.

It is important for all staff members to be constantly aware of possible violations. Staff are so accustomed to going about their daily work routine and accomplishing their assigned tasks that they sometimes forget to watch out for violations of resident confidentiality and privacy. One way to help avoid this is to be fully aware of the areas in which privacy can be violated.

The following guidelines will help reduce violations of resident confidentiality:

- Do not discuss resident information in elevators, hallways, lunchrooms, restrooms, or other public areas.
- Take hearing-impaired residents to private areas before asking them sensitive questions.
- Be on guard against carelessly voicing comments that might include resident-identifiable information.
- Be careful about using a speakerphone or listening to taped messages that might include confidential resident information in a place where it can be easily overheard.
- Share resident information only with those who need to know. If you are uncertain as to whether a family member or staff member from another unit needs to know information about a resident, check with your supervisor.
- Do not access any resident information that you should not see.
- Offer only appropriate information, when requested. Do not share more than is required.
- Ensure that resident information and records are not left out in the open on desks or tabletops or in resident rooms.
- Ensure that sensitive resident information (e.g., resident notes from your daily assignment) is disposed of properly.
- Do not take resident information home with you.

As you can see, it isn't an easy task to protect and respect resident confidentiality in a nursing home. However, protecting every resident's rights and dignity must be a top priority of every nursing home. ■

September 2011 Vol. 9, No. 9

# CNA PROFESSOR From HCPro

## HIPAA AND RESIDENT CONFIDENTIALITY

*Mark the correct response.*

Name: Date:

**1.** HIPAA, passed in 1996, stands for _____.
   a. Health Inclusion Portability and Assurances Act
   b. Health Information Protection and Assurances Act
   c. Health Identification Protection and Accountability Act
   d. Health Insurance Portability and Accountability Act

**2.** _____ refers to preventing someone from hearing or seeing a person's private health records and information unless he or she has the proper authorization.
   a. Privacy
   b. Confidentiality
   c. Security
   d. None of the above

**3.** HMOs are not considered "covered entities" under HIPAA.
   a. True
   b. False

**4.** The resident record is included in protected health information (PHI).
   a. True
   b. False

**5.** If a provider wants to disclose a person's PHI for purposes of providing healthcare, the provider needs to obtain the person's _____.
   a. electronic health record
   b. authorization
   c. consent
   d. none of the above

**6.** A covered entity must allow a person to view and photocopy his or her PHI if that person submits a request.
   a. True b. False

**7.** SNFs and other covered entities are required to do all of the following except _____.
   a. notify residents about their privacy rights
   b. maintain all resident records in print under lock and key
   c. train employees so that they are fully aware of the privacy procedures
   d. implement safeguards to prevent intentional or accidental misuse of PHI

**8.** A cover sheet marked "confidential" should accompany all faxed information.
   a. True b. False

**9.** Even if CNAs are certain that the person they are speaking with is permitted to hear certain information, they should not discuss a resident's PHI in _____.
   a. hallways
   b. lunchrooms
   c. restrooms
   d. all of the above

**10.** If uncertain as to whether a family member or staff member from another unit needs to know information about a resident, CNAs should _____.
   a. consult with other CNAs
   b. notify the resident
   c. check with their supervisor
   d. ask the family member or staff member whether they are permitted to know the information