Tackling the Training Mandate: How to Get Your Work Force Privacy Training Under Control and Under Way

by Sandra Nutten, CHC

One of the privacy rule's biggest tasks is work force training. In this article, we offer helpful tips for getting started and staying on track.

Training your work force on the HIPAA privacy rule isn't only federal law—it's the foundation on which the entire organization's compliance rests. As we know, HIPAA requires all healthcare providers, payers, and clearinghouses to comply with detailed regulations aimed at protecting information as it is used in the healthcare industry. In addition, the privacy rule contains the mandate that "a covered entity must train all members of its work force on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the work force to carry out their function within the covered entity." This article offers guidelines to help your organization meet this mandate.

Who Needs Training? The Entire Work Force

The first step in meeting HIPAA's mandates is understanding exactly what is expected of your entity in terms of work force training. According to section 164.530 (b), each entity must provide training to its work force no later than the compliance date for the covered entity. Because the privacy regulations are final, every member of your work force should have had some form of privacy training by April 14, 2003. When the other areas of HIPAA security are published in the final version, additional training may be necessary to fulfill the obligations as set forth in those rule sets. (There is no mention of work force training in the transactions and code set final rule.)

The privacy requirement does not specify how long or how involved the training must be. However, the requirement does explicitly state that the training must cover policies and procedures with respect to protected health information with a stipulation: the training on policies and procedures is only as needed and appropriate for work force members to carry out their function within the covered entity. Before constructing the privacy training sessions, take the following four steps:

1. **Define the entity**: Declare who is considered a part of the covered entity and who is not. Defining the work force for an entity is impossible without knowing the composition of the entity itself. You do not need to provide training to anyone other than your own work force, unless you stipulate that contracted agents attend your entity's training sessions as a contractual obligation, as stated in partner agreements. Business associate contracts and trading partner agreements should address the behaviors and performance expectations of those who are contracted to support the entity's work force.
2. **Define the work force**: Consider all roles (including volunteers, students, and agency help) that carry out a function for the covered entity. All work force members must receive at least one training session to comply with the regulation. Consider this obligation as you would any other "mandatory" training session such as fire safety. All members of the work force should be identified, scheduled, and audited as having attended a HIPAA training session. The requirement specifies that each covered entity must document that training has been provided. Department managers should ensure their staff complies with this requirement.
3. **Identify who will be responsible for developing the training curricula**: The rule does not identify who should develop and conduct the training, but states that the privacy official is held accountable for ensuring that training occurs. The format for training is not specified in the regulation; thus, you may use any or all of the following training delivery methods:

- classroom lecture
- self-study handout
- video presentation
- computer-based training

Remember that documentation must exist to prove that training was conducted. Each member of the work force attending the training session should acknowledge his or her participation by signing in on an attendance sheet (at a minimum), participating in discussion questions or case presentation dialogue (standard teaching tools), or taking a test (to demonstrate effective comprehension of expected behavioral outcomes or competence in the subject matter). Remind the attendees that HIPAA compliance is everyone's responsibility.

4. **Schedule educational sessions**: Put several sessions on the upcoming education calendar and allocate at least 45 minutes to complete each session. One of your existing mandatory training sessions is probably focused on patient rights, so if you have already scheduled a patient rights session before April 14, 2003, remember that each patient has new rights under HIPAA. Your session objectives must include references to the newly created or edited policies and procedures that protect those rights. A general, all-work-force-based HIPAA privacy training session should briefly—and on an adult learning level specific to your general audience—include the following elements:

    - HIPAA objectives (or "Why Are We All Doing This?")
    - information source (or "Where Can I Learn More About HIPAA?")
    - definitions (or "What Do These Terms and Acronyms Mean?")
    - what HIPAA privacy regulations cover (or "How Does This Affect Me and When?")

    The last topic in the above list should encompass the following subjects, using the entity's policies and procedures as source documents:

    - use and disclosure of protected health information (PHI)
    - how public responsibility and HIPAA work together
    - individual rights under HIPAA
    - organizational accountability
    - administrative safeguards of PHI
    - physical safeguards of PHI
    - technical safeguards of PHI
    - how HIPAA relates to state law
    - how the entity will become HIPAA compliant
    - complaint procedure

Form Follows Function for Role-specific Training

In addition to, or as a substitute for the general HIPAA training session, role-specific training should be developed for those individuals whose function is more intensely connected to HIPAA compliance activities. When this session replaces the basic session, you should include content from the basic training session with the role-specific subject matter. Consider the following groups as you develop these training sessions:

- board of directors
- entity executives
- medical staff
- department directors and management
- clinical staff
- technical staff
- security and safety staff
- compliance office, risk management, and legal staff

The role-specific training sessions can contain much more detail about the group's particular responsibilities with regard to HIPAA compliance. In these sessions, the HIPAA standards can be illustrated with greater depth. The HIPAA privacy requirement states that all members of the work force be trained "on policies and procedures, with respect to protected health

information, as necessary and appropriate for the members of the work force to carry out their function." For some of the functional groups listed, training may need to be broken down into several sessions to achieve what is "necessary and appropriate." Another possibility is to conduct a HIPAA training workshop by blocking out two or three hours for the topic. This method works best at the director or manager level. These sessions might also include training trainers as an additional behavioral objective or goal. In that instance, attendees would be expected to conduct future training sessions (probably the basic version) for groups of their colleagues or subordinates.

Don't Forget New Employees

Another implementation specification of the HIPAA training standard states that training is to be given to all members of the existing work force and "thereafter, to each new member of the work force within a reasonable time after the person joins the covered entity's work force and to each member of the covered entity's work force whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective." This means that anyone who takes a new position with the entity, regardless of the role, must receive HIPAA training that focuses on the functional requirements of the job and details those policies and procedures that give direction to the work force member.

As new employees are hired, discuss the privacy rule as a topic under patient rights so management's expectation that all work force members comply with the HIPAA regulations is clear.

Is the Training Effective?

Once your work force has received HIPAA privacy training, it is important to validate the effectiveness of the education and demonstrate employee competency. At a minimum, perform the following table top exercises as case presentations to members of the work force at all levels:

- patient complaint procedure for HIPAA privacy issues
- request for information protocol
- request for designated record set amendment protocol
- notice of privacy practices protocol
- review of HIPAA definitions: personally identifiable information, role-based access, and minimum necessary

The ultimate goal of HIPAA privacy training is to have all members of the work force change the way they perform job-related tasks that involve personally identifiable health information. Procedures and protocols address the steps required to accomplish the intended function or task. If work force behavior does not change with the completion of education sessions, management must address the issue to achieve compliance. Unlike other healthcare regulations, there will be no "HIPAA survey" or team of inspectors validating that all the required elements of compliance are in place. At best, a patient who believes that his or her personally identifiable information has been used or disclosed in violation of the privacy rule will seek redress with your entity by using the complaint protocol established specifically for that purpose. The Department of Health and Human Services Office for Civil Rights may seek action against the entity on behalf of the patient if the complaint comes to them, and if an entity is found guilty of a HIPAA privacy breach, the following may occur:

- Civil monetary penalties up to $100 per violation, capped at $25,000 for each calendar year for each standard
- Criminal penalties increasing with the intent of the action and likely enforcement by the Justice Department and Federal Bureau of Investigations:
  - wrongful disclosure: $50,000 and/or one year imprisonment
  - false pretenses: $100,000 and/or five years imprisonment
  - malice or intent to sell information for personal gain: $250,000 and/or 10 years imprisonment

It is in the best interest of all concerned that HIPAA privacy education be taken seriously and proven effective. Job descriptions, even for unpaid positions such as volunteers, should include a line item about HIPAA privacy and the organization's expectation of compliance. Consequences for failing to comply are stated in the regulations: The entity "must have and apply appropriate sanctions against members of its work force who fail to comply with the privacy policies and procedures."

One Size Does Not Fit All

All healthcare providers, payers, and clearinghouses, otherwise known as HIPAA entities, are bound by law to educate their work force to HIPAA privacy standards by April 14, 2003. Remember that HIPAA asks that you use a reasonable approach to achieving compliance and that your efforts should reflect the size and scope of your business.

Start Your Training Program Now

Completing all the required training sessions prior to April 14, 2003, can seem daunting when considering the preparation needed before the first session is held. The smartest move you can make is starting now. Convene the HIPAA privacy training subcommittee and develop a timetable that fits your organization's style. Use the following schedule as a guideline:

February: Complete HIPAA privacy training-for-trainers sessions.

March: Conduct all work force sessions. New employees should receive their training with general orientation sessions beginning March 1, 2003.

April: Department managers need to be vigilant about staff completing their training. Any work force member who has not attended a HIPAA privacy training session by April 14 must seek direction from the HIPAA privacy official.

Keep in mind that each and every time a policy that addresses HIPAA standards is created or revised, all members of the work force who are affected by the change must receive training on the subject. Evidence of effective training is changed work force behaviors.

Where Can I Find the Privacy Rule?

For a copy of the final privacy rule, go to www.hhs.gov/ ocr/hipaa. You'll also find helpful policy guidance and a place to submit questions to the Office for Civil Rights.

Reference

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available at http://aspe.hhs.gov/admnsimp/.

Sandra Nutten *(Sandra_Nutten@superiorconsultant.com) is a senior management consultant at Superior Consultant Company, Inc.—The Chi Group in Ann Arbor, MI.*

Article citation:
Nutten, Sandra. "Tackling the Training Mandate: How to Get Your Work Force Privacy Training Under Control and Under Way." *Journal of AHIMA* 74, no.2 (2003): 22-25.