Next Challenge: Employee Training on Privacy, Security (HIPAA on the Job)

Save to myBoK

by Bonnie S. Cassidy, MPA, FHIMSS, RHIA

HIPAA assumes that policy and technology together cannot provide adequate protection for patient-identifiable healthcare information. The integral piece of this puzzle is employee training.

Organizations must provide **general awareness** training for every employee and affiliate. This process should build general awareness of confidentiality and security issues for all employees. For employees with access to electronic health information, the organization should include job-specific training focused on protecting confidentiality and security.

This article describes the next steps for your organization's privacy and security training program, as well as a look at what the proposed regulations require. Remember, training requirements may change as the final rules are issued, so it's a good idea to review your training program regularly.

What Does the Proposed Privacy Rule Require?

The proposed rule for standards for privacy of individually identifiable (protected) health information (available online at the HHS administrative simplification site, http://aspe.hhs.gov/admnsimp/) addresses training of work force members.

According to the proposed rule, covered entities are required to provide training on policies and procedures with respect to protected health information. Each entity is required to provide initial training to all employees, volunteers, and affiliates by the date on which the proposed rule becomes applicable. After that date, each entity would have to provide training to new members of the work force within a reasonable time period. In addition, if an organization makes material changes to its privacy policies or procedures, it would be required, within a reasonable time period, to retrain members of the work force whose duties are directly affected by the change.

Covered entities are required to train all members of the work force (e.g., all employees, volunteers, trainees, students, residents, members of the medical staff, and others) who are likely to have contact with protected health information.

Upon completion of the training, employees would be required to sign a statement certifying that he or she received the privacy training and will honor all of the entity's privacy policies and procedures.

The most effective means of communicating with the work force depends on the organization. For example, in a small physician practice, the training requirement could be satisfied by providing new members of the work force with a copy of the practice's information policies and requiring them to acknowledge that they have reviewed the policies. A large health plan could provide a training program with live instructions, video presentations, or interactive software programs. The small practice's solution would not protect the large plan's data, and the large plan's solution would not be economically feasible or necessary for the small practice.

At least once every three years after the initial training, covered entities would be required to have each member of the work force sign a new statement certifying that he or she will honor all of the entity's privacy policies and procedures. The initial certification would be intended to make members of the work force aware of their duty to adhere to policies and procedures. A recertification every three years would remind them of this duty.

The proposed rule's authors conclude that "the goals could be achieved by only requiring recertification once every three years and retraining in the event of material changes in policy."

What Does the Proposed Security Rule Require?

The administrative procedures section of the proposed rule for security and electronic signature standards also addresses training. It is also available online at http://aspe.hhs.gov/admnsimp/.

This proposed rule requires security training for all employees and staff regarding the vulnerabilities of the health information in an entity's possession and the procedures that must be followed to ensure the protection of that information. This is important because employees need to understand their security responsibilities and make security a part of their day-to-day activities.

The rule would require the following implementation features:

- awareness training for all personnel, including management
- periodic security reminders
- user education concerning virus protection
- user education in the importance of monitoring login success/failure and reporting discrepancies
- user education in password management

Now That I Know What the Requirements Are, What Do I Do Next?

Your organization's privacy and security training program must address and include all transactions dealing with individually identifiable health information.

In preparing your security and privacy training program, some ideas for your consideration include:

- **organize** a coordinated approach
- **prepare** a training work plan for the next three years
- **conduct** an inventory of people who will need to attend training
- **inventory** policies and procedures dealing with protection of health information (privacy)
- **identify** job descriptions that correlate to the majority of the policies and procedures that would enable you to monitor the need for retraining when there are material changes to policies and procedures
- **inventory** polices and procedures dealing with security of information
- **determine** how you will record/keep track of attendance
- **develop** a plan for the certification and recertification process
- **identify** resources (manpower, software) needed
- **allocate** budget, time, and resources for training
- **conduct** general awareness sessions
- **educate and update** executives and management team

Detailed planning for the development of your training program will ensure your organization's success. All organizations must be prepared to train employees and the medical staff on new or revised security and privacy policies and procedures. The work plan for the training program should address the questions "who, what, when, where and why?" for its planning and implementation. In other words, an organization needs to document the plans for training and the training sessions to keep a record of who presented, who attended, what the topic was, when it was conducted, where it was conducted, and address any reasons "why"-e.g., material changes in policy.

What's the Bottom Line?

The bottom line can be described in terms of the who, what, when, and why, as well:

Who needs to participate in privacy and security training? All current employees, volunteers, and affiliates need to participate. How is your work group going to identify all of these employees and affiliates? You will need to document the steps and tasks, such as:

- obtain employee records from human resources
- obtain records of all clergy from your pastoral affairs office

- work with your accounting department to identify who has been issued a check for services (affiliates, moonlighters, PRN nurses, etc.)
- work with the education department to identify rotations of interns, residents, and fellows, and so on

Looking forward, all new hires must be included in the training program, which should be incorporated into your new hire orientation.

What is the scope of privacy and security training? The training program should include a review of all policies and procedures related to the handling of health information, security, and confidentiality. There should be general awareness training for all employees with periodic security reminders. Training should include user education on virus protection, login procedures, and password management.

When does this need to be done? The answer is now. Start training your employees, medical staff, volunteers, and affiliates now to create a baseline for your organization. After the initial training, follow-up training will need to be done at least every three years. In order to provide evidence that the training was provided, you must provide certification to the employees (work force) and affiliates.

Job-specific training must also be provided whenever there are material changes in policies and procedures dealing with the handling of health information. For example, if your hospital outsources release of information and then decides to bring it in-house, there would be material changes in the policies and procedures of specific functions of a particular job position. The employees in that position would be required to be trained on the material changes in policy. This requires the development of a monitoring process to track the material changes of policies and procedures. It also requires you to identify job descriptions and employees who will need focused re-training based on the new policies and procedures.

Why are we doing this? We are doing this for the continuing benefit of all consumers of healthcare services, working towards the protection and security of health information and for HIPAA compliance. Our current challenge is to provide ongoing education and training within our organizations on privacy and security of protected health information.

***Bonnie Cassidy**, MPA, FHIMSS, RHIA, is a principal with The North Highland Company, Atlanta, GA. She can be reached at [bcassidy@ north-highland.com](mailto:bcassidy@north-highland.com).*

Article citation:
Cassidy, Bonnie S. "The Next Challenge: Employee Training on Privacy, Security (HIPAA on the Job)." *Journal of AHIMA* 72, no.1 (2001): 16A-C.
