HIPAA Workforce Training Tip Sheet

What Does HIPAA Require for Workforce Training?

Both the HIPAA Privacy Rule and the HIPAA Security Rule have training requirements. The HIPAA Privacy Rule training requirement is at 45 CFR § 164.530(b)(1). The HIPAA Security Rule training requirement is an administrative safeguard at 45 CFR § 164.308(a)(5).

Privacy Rule Training

Although the HIPAA laws require development of policies and procedures, there is nothing more important to ensuring HIPAA compliance than training your workforce. A covered entity (CE) is responsible for ensuring that every member of its workforce receives training in HIPAA privacy policies and procedures. New members must be trained within a reasonable period of time after joining the workforce and when material changes are made to policies and procedures. If you have contract employees who come in contact with protected health information (PHI) and work routinely on the premises, they should also receive HIPAA training. Business associates should also provide training to their workforce. You are required to maintain documentation that the training has taken place. (45 CFR 164.530)(b)(2)(ii). Although the HIPAA law does not specifically require annual training, it is recommended because of the increased risks of a privacy or security violation and the heightened liability associated with privacy and security of protected health information (PHI).

Security Rule Training

Security awareness and training is also required for all members of the workforce, including management. Employees can create the most significant risk to the organization's security. HIPAA requires training that is tailored to meet the organization's needs and must be provided for new and existing members of the workforce. Training updates should be provided periodically and should include any changes to the Security Rule and when there are updates to policies and procedures. The workforce should also be trained when the organization has new or upgraded hardware or software or new technologies that impact security. (45 CFR 164.308(a)(5)).

What Topics Must the Training Cover?

Privacy

The HIPAA Privacy Rule does not specify the specific topics that must be covered in workforce training. Rather, it states that training must be "as necessary and appropriate for the members of the workforce..."
to carry out their functions within the covered entity.” Some employees may have functions with only a limited involvement with patients or PHI. For example, a billing clerk in a medical office may receive different training than a nurse. If an employee’s job function does not involve release of information, they may not need training on this topic.

The most common and important HIPAA privacy topics to train about include:

- Identify the organization’s Privacy Officer
- What is PHI
- Document retention and destruction
- The minimum necessary rule
- Rules about when and how PHI may be disclosed
  - Disclosures that require a written authorization
  - Disclosure that do not require an authorization
    - Treatment, payment, healthcare operations, public health and safety, research, organ and tissue donations, work with a medical examiner or funeral director, workers’ compensation, law enforcement, other government requests
- The importance of confidentiality
  - Confidentiality policy
  - Social media policy
- Accounting of disclosures
- Patient rights
  - Obtaining a copy of their medical record
  - Requesting a correction of their medical record
  - Requesting confidential communications
  - Requesting limitations on their medical information
  - Maintaining a list of those with whom we have shared information
  - Obtaining a copy of the Notice of Privacy Practices
  - Choosing someone to act on their behalf
  - Choosing to whom we share information (family, friends, or others involved in their care)
- How to handle a patient complaint related to privacy
Security

Training is also required under the HIPAA Security Rule. The implementation specifications are all addressable, which means that they must be followed unless there is a documented reason for not doing so or a documented alternative measure that is substituted. Specifically the HIPAA Security Rule requires that you implement a security awareness and training program for all members of the workforce, including management.

The most common and important HIPAA security topics to train about include:

- Organizational policy on security updates
- How to respond to a patient’s request for electronic communication
- Physical safeguards of equipment, medical devices that contain PHI
- Procedures for guarding against, detecting, and reporting malicious software
- Procedures for guarding against, detecting, and reporting social engineering attacks
  - Phishing
  - Dangers of certain website
- Remote access procedures
- Procedures for monitoring log-in attempts and reporting discrepancies
- Procedures for creating, changing, and safeguarding passwords
- Use and security procedures related to portable devices
- New or upgraded hardware or software or new technologies that impact security
- HIPAA Breach/Data Security Incident
  - Definition of breach
  - How to respond in the event of a potential breach or a security incident
- Procedures for destruction of sensitive information (hard-copy and electronic)

Important Note: These lists are not intended to be an exhaustive list of HIPAA training topics. It is important to remember that HIPAA requires training that is tailored to meet the organization’s needs and the employee’s specific job functions. The content and information contained herein is intended to be used for general information and is not legal advice. Consult your own legal counsel to assist with specific situations that require legal advice or counseling.

Training Resources for Current Policyowners

- MagMutual HIPAA Staff Training Learning Module
• MagMutual HIPAA On-Demand Webinar
• MagMutual’s HIPAA Toolkit

Public Training Resources

• HIPAA 101: The Basics of HIPAA Administrative Simplification
• Worried About Using a Mobile Health Device for Work? Here’s What To Do
• OCR offers Patient Privacy: A Guide for Providers (login required), an educational program for health care providers on compliance with various aspects of the HIPAA Privacy and Security Rules. Physicians can earn free Continuing Medical Education (CME) credits and health care professionals will receive Continuing Education (CE) credits.
• HealthIT.gov's Guide to Privacy and Security of Electronic Health Information provides a beginners overview of what the HIPAA Rules require, and the page has links to security training games, risk assessment tools, and other aids.
• Guidance from the National Institute of Standards and Technology
  o NIST Special Publication 800-50 - Building an Information Technology Security Awareness and Training Program
  o NIST Special Publication 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model

The content and information presented here is intended to be used for general information and is not legal advice. It does not create an attorney client relationship. Consult a licensed attorney to assist with specific situations that require legal advice or counseling.

06/08/2016