HIPAA Training Requirements

The Health Insurance Portability and Accountability Act (HIPAA) has extensive training requirements, and many healthcare providers are not aware of them, or they simply don’t follow them. HIPAA provides more specific guidance than many laws about what training is required, however, HIPAA leaves a lot open to interpretation. To further complicate matters, HIPAA’s Privacy Rule and HIPAA’s Security Rule both have separate training requirements. This Fact Sheet is meant to be an overview of the training requirements for a typical healthcare provider.

What are the HIPAA Training Requirements?

Both the HIPAA Privacy Rule and the HIPAA Security Rule have training requirements. The HIPAA Privacy Rule has a specific training requirement, while the Security Rule training requirement is an administrative safeguard. Here is the full text of the training requirement.

**45 CFR § 164.530 HIPAA Privacy Administrative requirements.**

(b) (1) **Standard: Training.** A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) **Implementation specifications: Training.**

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity’s workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity’s workforce; and

(C) To each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

**HIPAA Security Rule 45 CFR § 164.308 Administrative safeguards**

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations. . . .

(5)(i) **Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).

(ii) **Implementation specifications.** Implement:


(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.


(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.
What types of organizations must provide HIPAA training?

HIPAA requires that both covered entities and business associates provide HIPAA training to any members of the workforce that handle Protected Health Information (PHI). This means that even small offices need to train personnel on HIPAA. Both doctors and team members need to be trained if they work with PHI.

What should be included in the training?

The guidelines don’t specify a minimum length for training. KMC University has created a comprehensive training module for team members to access that includes everything needed. You are not required to make everyone a HIPAA expert. What is important is that the basics of privacy and security are covered and the most significant day-to-day HIPAA-related issues are clearly and thoroughly explained for all team members.

The HIPAA Privacy Rule indicates that training must be “necessary and appropriate for the members of the workforce to carry out their functions.” This means that different team members may require different training based on job description. Many employees may have limited or no involvement with patients or PHI. If an employee is not involved in providing notice to patients or in providing patients with access to their records, there is no need to train them on these topics.

**Examples:** The most common and important HIPAA privacy topics that require training include identifying PHI, the minimum necessary rule, the rules about when and how PHI may be disclosed, the importance of confidentiality, avoiding snooping (even when one has access to PHI), and the need to log all disclosures. Patient rights and authorization are also important topics. Training should cover the consequences of failing to follow the HIPAA Privacy Rule — how people can be victimized by medical identity theft, how people can lose trust, how organizations can be penalized by HHS and other regulators for violations, and how employees can be penalized too — by their organizations, through civil and criminal penalties under HIPAA, and by state law.

How often must HIPAA training be provided?

The HIPAA Privacy Rule states that training must be provided for “each new member of the workforce within a reasonable period of time after the person joins the covered entity’s workforce” and for “each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures . . . within a reasonable period of time after the material change becomes effective.” Basically, the Privacy Rule requires training when hired or whenever there is a material change to policies and/or procedures. KMC University recommends annual refresher training as well. Your staff needs to be constantly reminded of HIPAA requirements because one lapse is all it takes to generate an incident.

The HIPAA Security Rule requires a security awareness and training program for all workforce members with an implementation specification for the program to include periodic security updates. The Security Rule doesn’t define “periodic” and it doesn’t explain when and how often people must be trained or define what comprises periodic security updates, KMC University recommends annual Security Training in addition to the annual Privacy Rule refresher training.