HIPAA Training Requirements:
An Overview for NC Local Health Departments

Jill Moore, JD, MPH, UNC School of Government
May 2018

Summary of Requirements

The HIPAA regulations require covered entities to train their workforce members in privacy, security, and breach notification.

The Privacy Rule requires a covered entity to train all of its workforce members on the policies and procedures that are required by the Privacy Rule and by the Breach Notification Rule, as necessary and appropriate for the workforce members to carry out their functions within the covered entity. Training for new workforce members must be provided within a reasonable period of time after they join the workforce. Training must also be provided to any member of the workforce whose functions are affected by a material change in policies or procedures required by the Privacy Rule or the Breach Notification Rule, within a reasonable period of time after the change becomes effective. The training must be documented. 45 C.F.R. 164.530(b).

The HIPAA Security Rule requires a covered entity to implement a security awareness and training program for all members of its workforce, including management. The program must include periodic security updates; procedures for guarding against, detecting, and reporting malicious software; procedures for monitoring log-in attempts and reporting discrepancies; and procedures for creating, changing, and safeguarding passwords. 45 C.F.R. 164.308(a)(5).

The remainder of this document uses a question and answer format to provide further information and prompts for discussion about HIPAA training in North Carolina local health departments.

Questions and Answers about HIPAA Training

Who must be trained?

HIPAA requires a covered entity to train the members of its *workforce*. The term workforce is defined under HIPAA to include not only employees, but also volunteers, trainees, and potentially others:

> *Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. 45 C.F.R. 160.103.

Most local health departments (LHDs) are hybrid entities under HIPAA. This means that they have some functions and activities that are covered by HIPAA, but other functions or activities that are not covered by HIPAA. The HIPAA training requirements apply only to the workforce of a local health department's HIPAA-covered component (also known as the "health care component"). Each LHD must determine for itself which of its programs, services, activities, or functions are part of the department's HIPAA-covered component.

What must workforce members be trained in?

The Privacy Rule requires covered entities to train workforce members in the policies and procedures the entity has adopted to implement the HIPAA Privacy Rule and the HIPAA Breach Notification Rule.

Note that this requirement is clear that the training must address the *entity's own policies and procedures*. While an overview of the requirements of the HIPAA Privacy Rule and the HIPAA Breach Notification Rule might be part of the training a covered entity offers, overviews alone are not enough. Workforce members need training in the policies and procedures of the covered entity they work for. This doesn't necessarily mean that every workforce member must be thoroughly trained in every policy or procedure. The rule specifies that workforce members must be trained "as necessary and appropriate" for them to carry out their functions within the covered entity. Different groups of workforce members could receive different training tailored to their different needs.

The Security Rule also requires training and awareness programs. It specifically identifies the following issues as matters to be addressed by such programs:

- Procedures for guarding against, detecting, and reporting malicious software.
- Procedures for monitoring log-in attempts and reporting discrepancies.
  Procedures for creating, changing, and safeguarding passwords.

Although it is not specifically required by HIPAA, I recommend training employees in the covered entity's sanctions policy as well. Both the Privacy Rule and the Security Rule require covered entities to have policies for sanctioning workforce members who fail to comply with HIPAA policies and procedures. The rules also require covered entities to apply those sanctions when a compliance failure occurs—they are

not optional. I believe it is important for workforce members to know that sanctions will be applied if they fail to comply with a rule, and what those sanctions are.

When must new workforce members be trained?

The HIPAA Privacy Rule requires the training in privacy and breach notification policies and procedures to occur "within a reasonable period of time after the person joins the covered entity's workforce." The rule doesn't specify what constitutes a reasonable period of time. Its reference to "after" the person joins the workforce suggests the person can begin work before being fully trained, but the covered entity should be thoughtful about what a new workforce member may need to know before beginning to work with PHI in order to avoid an inadvertent violation, and full training should not be unreasonably delayed.

The HIPAA Security Rule does not specify a timeframe for training, but the types of things that need to be addressed – such as password procedures, and procedures for guarding against malware – are critical to avoiding breaches. New workforce members should be trained in these before beginning work on systems or devices that allow access to electronic PHI.

When should additional training of workforce members occur?

The Privacy Rule requires additional training for workforce members when there is a material change in privacy or breach notification policies and procedures that affects their work. The training must occur within a "reasonable period of time" after the change becomes effective. The rule doesn't specify what constitutes a reasonable period of time, but it should be as soon as practicable, bearing in mind that a material change in policies or procedures may require workforce members to change their work habits. If it's possible to train workforce members *before* a material change becomes effective, that would probably be a good thing to do.

The Privacy Rule does not have a specific requirement for annual training for all workforce members, but annual training is a common practice, and periodic refreshers are certainly a good idea.

The Security Rule specifically requires periodic security updates as part of the security awareness and training program. The rule does not specify what it means by "periodic." At a minimum, training should occur whenever policies, procedures, practices, or technology changes occur. Periodic reminders and refreshers are also a good idea.

How must training be documented?

HIPAA specifies that training should be documented in accordance with the documentation rule in 45 C.F.R. 164.530(j). That rule does not provide a lot of detail. It simply requires a covered entity to "maintain a written or electronic record" that the training required by the rules has occurred.

At a minimum, documentation about a workforce member's training should clearly identify the name(s) of the workforce member(s) trained, the date and time of the training, and a title or brief description of the training.

The covered entity should also document information about the content of the training provided. In the event of a compliance investigation or an audit, the entity may need to demonstrate that appropriate training was provided to workforce members.