Annual HIPAA Training: A Preventive Measure

Save to myBoK

By Diana Flood, MS, RHIA

Every year many patients go to their doctors for an annual exam in which preventive care measures for conditions are explored and enacted. These appointments help patients avoid further, more intensive care down the road. Annual HIPAA training programs are similar to an annual exam—organizations study and enforce compliance with privacy and security regulations to prevent a larger problem in the future. Annual physical exams, like regular HIPAA training, have benefits that far outweigh their inconvenience. Though perhaps—not unlike an annual doctor visit—some dread annual training, it is necessary as shown by the number of HIPAA breaches continuing to occur in healthcare—a number that climbs each year. Annual training is the key to preparing employees to know their organization's policies and procedures and will give employees the skills to assist with and prevent sticky situations.

It is broadly accepted in healthcare that anyone who comes in contact with protected health information (PHI) is required to undergo HIPAA training, including covered entities of all sizes, business associates, clearinghouses, health plans, etc. This includes new hires as well as existing employees that have access to PHI.

The federal standard only requires that training be "as necessary and appropriate for the members of the workforce to carry out their functions," with an annual training time frame. While there is a large variety in the types of organizations that are required to comply, no single training program is "one size fits all." Too often healthcare professionals just go through the motions to get their certificate of completion because they are not invested in the outcome. To encourage a higher level of employee engagement, HIPAA educators should customize their training to fit the needs of every employee type within their facility. For example, the HIPAA training needs for billing and coding specialists should have a different focus than training needed by direct caregivers. Customizing the training at your organization to fit the needs of your employees and type of facility is critical to ensuring buy-in of compliance from employees.

Annual training should include a focus on both privacy and security. Privacy training is outlined in 45 CFR § 164.530(b)(1) under the administrative requirements. Requirements for security training are found under the administrative safeguards in 45 CFR § 164.308(a)(5).

In addition to requiring a review of privacy and security policies and protocols, the HIPAA Security Rule also necessitates addressing the implementation of periodic security reminders, protection from malicious software, log-in monitoring, and password management. At this time, training around the Breach Notification Rule (45 CFR § 164.400-414) is not required by law; however, privacy experts highly encourage training employees on the protocols revolving around what to do in the event of a breach. After all, a doctor doesn't provide preventive care for conditions without describing for the patient the possible outcomes if they don't adhere to his or her advice.

One of the best ways to ensure retention of information and focus on HIPAA training is to have a short quiz at the end portion of the curriculum. If training materials stay the same every year, at least switch out the quiz questions to keep trainees on their toes. It's also helpful to provide examples of privacy or security incidents that happened in the facility where the training is taking place. For example, if an organization had a reportable breach due to an employee posting PHI on social media, include questions regarding organizational policies on social media. Quizzes shouldn't be too long—five to 10 questions is plenty, but make sure the questions are meaningful and bring value to the training program.

As with any type of healthcare documentation, if there isn't proof, it didn't happen. When employees have successfully completed their training, provide a certificate of completion and retain a copy in their employee record. In addition, maintain logs of the dates of training and who completed them on each day in compliance files. Should an investigation or audit with the US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) occur, this documentation will be key in proving that HIPAA training did in fact take place.

Though annual training can seem cumbersome, it truly makes a difference in conformity to the law. Ignorance of the regulations is not an excuse when it comes to violations. HHS, as well as many commercial companies, provide helpful guides and resources to assist facilities of all sizes and types to comply with the rules.

Prepare and protect your employees and organization from an infectious HIPAA violation. Complete your annual preventive training and work harder towards a healthier, more compliant HIPAA future.

References

Department of Health and Human Services Office for Civil Rights (OCR). "Breach Notification Rule."

OCR. "The HIPAA Privacy Rule."

OCR. "The Security Rule."

OCR. "Training Materials: Helping Entities Implement Privacy and Security Training." www.hhs.gov/hipaa/for-professionals/training/index.html?language=es.

Diana Flood (dflood@ofmq.com) is clinical consultant II for the Oklahoma Foundation for Medical Quality.

Article citation:
Flood, Diana. "Annual HIPAA Training: A Preventive Measure" *Journal of AHIMA* 88, no.6 (June 2017): 36-37.