U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

July 2017

Train Your Workforce, so They Don't Get Caught by a Phish!

A covered entity's workforce is its frontline not only in patient care and patient service, but also in safeguarding the privacy and security of its patients' protected health information (PHI). The healthcare sector's risk landscape continues to grow with the increasing number of interconnected, "smart" devices of all types, the increased use of interconnected medical record and billing systems, and the increased use of applications and cloud computing.

Along with this increase in interconnectedness has come a ten percent increase over the past two years in the number of providers and health plans that have had instances of security-related HIPAA violations or cybersecurity attacks impacting PHI. This is according to the 2015 and 2017 KPMG Cyber Healthcare & Life Sciences Surveys (https://healthitsecurity.com/news/hipaa-data-breaches-cyber-attacks-reported-by-47-of-orgs).

This increase in HIPAA violations includes breaches due to ransomware events, such as WannaCry, and other cyber attacks which could have been prevented by an informed workforce trained to detect and properly respond to them. Training on data security for workforce members is not only essential for protecting an organization against cyber attacks, it is also required by the HIPAA Security Rule.

The Security Rule specifically requires covered entities and business associates to "implement a security awareness and training program for all members of its workforce (including management)". 45 C.F.R. § 164.308(a)(5)(i). Note the emphasis on all members of the workforce, because all workforce members can either be guardians of the entity's PHI or can, knowingly or unknowingly, be the cause of HIPAA violations or data breaches.

In order to implement this standard, the Security Rule requires covered entities and business associates to implement periodic security updates, or reasonable equivalents. 45 C.F.R. § 164.308(a)(5)(ii)(A). An organization's training program should be an ongoing, evolving process and flexible enough to educate workforce members on new cybersecurity threats and how to respond to them. As such, covered entities and business associates should consider:

- How often to train workforce members on security issues, given the risks and threats to their enterprises, and how often to send security updates to their workforce members. Many entities have determined that bi-annual training, and monthly security updates are necessary, given their risks analyses.

- Using security updates and reminders to quickly communicate new and emerging cybersecurity threats to workforce members such as new social engineering ploys (e.g., fake tech support requests and new phishing scams) and malicious software attacks including new ransomware variants.
- What type of training to provide to workforce members on security issues, given the risks and threats to their enterprises. Computer-based training, classroom training, monthly newsletters, posters, email alerts, and team discussions are all tools that different organizations use to fulfill their training requirements. OCR has training materials available, including Medscape training modules on security of PHI. See https://www.hhs.gov/hipaa/for-professionals/training/index.html and http://www.medscape.org/sites/advances/patients-rights.
- How to document that training to workforce members was provided, including dates and types of training, training materials, and evidence of workforce participation. Any investigator or auditor will ask for documentation, as required by the HIPAA Rules, to ensure compliance with the requirements of the Rules. See 45 C.F.R. §§ 164.316(b) and 164.530(j).

OCR's Security Rule guidance materials may be found at https://www.hhs.gov/hipaa/for-professionals/security/guidance.