Health Information Compliance Alert

HIPAA: Make Staff HIPAA Training a Priority

Tip: Outline the amount of PHI-handling by job.

You can't take chances with HIPAA compliance, and the key to combat breaches is education. This is more true now than ever before because the use of patient-centered health IT is widely expected and adopted - plus, stepped-up federal enforcement only makes the need for staff training more critical.

"It's often tempting to focus on sensationalized risks such as hackers and nation-states," explains **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with **Online Business Systems**. "However many breaches are caused by the actions of individuals within the organization."

There are essential steps that practices must take to better train their employees, Kehler suggests. Consider adding these five things to your HIPAA training checklist:

1. Know how to identify PHI. "This may seem obvious, but too often I see things like staff discarding bottle labels with patient identifiers in the regular trash saying, 'I didn't realize that was [protected health information] PHI.' Or texting patient initials instead of full names thinking that this makes the data de-identified," Kehler says.

2. Explain what phishing looks like. Time and again, phishing is the culprit that takes systems down with just one click on a link. Phishing tests are important to sidestep these common attacks. "A phishing test is the practice of sending phishing messages to employees and if someone clicks on it, they are afforded the opportunity to learn more about phishing," instructs Kehler. "This is an extremely effective training method and is relatively inexpensive."

He adds," Do not exempt physicians and executives. They are the biggest target and often the most likely victims."

3. Allow the job to dictate the level of PHI-handling. Security training material is commonly generic in nature, but Kehler recommends staff receive training that fits the specific jobs they do. "For example, a biller needs to know what are permissible ways of communicating with insurance companies and what are not. An IT person needs to know how to properly transfer PHI from one system to another," he counsels. "These are topics that may not be in the general training, but are critical for how workforce members handle PHI in their day-to-day activities."

4. Keep passwords safe and secret. Procedures for creating and protecting passwords are outlined in the HIPAA Security Rule, but that doesn't mean that password sharing isn't done. In fact, the practice is pervasive, even among providers and executives, Kehler warns. That's why, "it must be made clear to all staff that what happens in their account is their responsibility," he submits.

Reminder: So, if Bob hands his password to Anne and she is snooping at patient charts under his account, Bob could be liable.

5. Don't ignore security incidents. "This cannot be stressed enough, but it's usually relegated to the last slide of the security awareness training deck. You don't have to confirm a security incident before reporting it," Kehler advises. Cultivating an environment where employees understand security and feel safe to report suspicious activity is critical to a successful HIPAA plan.

Tip: Give staff multiple ways to report incidents with things like posters, intranet, email signatures, and reminders at staff meetings, says Kehler. "The most frustrating thing for a security officer is to discover an incident, only to learn that the staff have been aware of it for quite some time."

Resource: Read a summary of the HIPAA Security Rule at

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.