You’ve Been Appointed as a HIPAA Officer. Now What?

by Chris Vogel, CEBS
Senior Editor
International Foundation of Employee Benefit Plans
Brookfield, Wisconsin

The following is based on a presentation by Petula Workman, CEBS, at the 2016 Symposium. Workman is division vice president, compliance counsel, for Arthur J. Gallagher & Co. in Houston, Texas.

When an organization appoints its Health Insurance Portability and Accountability Act (HIPAA) privacy and security officers, that’s just one step in complying with the act’s Privacy and Security Rules.

“Following the HIPAA Privacy and Security Rules is really more of a process,” said Petula Workman, CEBS, who breaks that process into several steps: identify, assess, train, implement, document, retain and repeat.

Identify

“The main thing to do is identify your players,” Workman said.

• The **privacy officer** or official is responsible for developing and implementing an organization’s privacy policy and procedures. The individual investigates security incidents and complaints and oversees responses to requests for access to protected health information (PHI). Often organizations also have a privacy contact or privacy liaison officer—someone who helps with administrative tasks and may be the contact person for plan participants.

• The **security officer** or official generally is an information technology (IT) person—usually an organization’s highest ranking IT official. The privacy and security officers may be the same person but typically aren’t, as very different skills sets are involved.

• **HIPAA workforce members**, sometimes referred to as **firewall employees**, are employees identified by job title or category who can and do access PHI. They include employees who handle benefits-related functions like marketing, claims analysis, helping employees with claims and benefits issues, and COBRA administration. They also include IT personnel who have access to PHI and, perhaps, payroll employees because of their role in payroll deductions to pay premiums. In the event of a Department of Health and Human Services (HHS) audit, “you would be asked for a job description for each of these folks” that spells out how these employees handle PHI, Workman said. Organizations should conduct background checks for HIPAA workforce members.

• **Business associates** are outside persons or organizations that have access to employees’ PHI, such as broker/consultants, third-party administrators, 6055/6056 reporting vendors, COBRA and health FSA vendors, and benefits confirmation vendors. Less obvious may be cloud storage providers, off-site document storage providers, and document and electronic media shredders. Organizations need to have business associate agreements in place with these vendors.

Assess

A HIPAA privacy officer must stay on top of new developments and make sure to review periodically how PHI is handled and where it’s stored. “Are you doing something different?” Workman asked. “Did you hire a third party to help you with something? . . . Did you decide you’re going to start sending out benefits confirmation statements and are going to use health plan data to do that? Now we’ve got a new way to transmit PHI or a new organization to do that?” She recommends mapping that out to show all players and methods of PHI transmission.

“You also want to look where your PHI is stored. Did you get a new server? Or do you have a shared file drive where inappropriate members of your organization also have access to it?” Workman asked.
An area of growing concern is where PHI is accessed, as many organizations allow employees to access PHI on personal devices such as cell phones. Android devices don’t have the same level of encryption as Apple products, and organizations need a policies or mechanism to encrypt PHI on personal devices.

“Another good thing to do is to periodically review your policies and procedures. Here’s a big one. You notice I assume you all have policies and procedures?” Workman said. These should be written and easy to understand. “I recommend the HIPAA privacy and security officers meet at least once a year to be sure what you’re doing on the privacy side and what you’re doing on the security side mesh up. . . . I so often find that IT doesn’t know what Benefits does on a day-to-day basis. (What do you mean, you use e-mail to conduct business transactions? I thought you did everything on a secure portal!)”

HIPAA officers need to determine whether policies and procedures have any gaps created, for example, by a service provider change. They also should look at any security incidents that may have occurred—“What happened, what can we make better, do we need to change our policies and procedures?” They also should do a risk analysis to look for vulnerabilities—perhaps annually because of rapid changes in the electronic environment. And officers should ask business associates for copies of their HIPAA policies and procedures.

**Train**

HIPAA workforce members should be trained on the organization’s own policies and procedures—“some real down-to-earth sorts of things”—rather than giving them general HIPAA training, Workman said. For example, employees should be taught never to click on a suspicious link that could potentially install malicious software on the organization’s system or the employees’ personal devices. They should know good password management and who to contact if they make unsuccessful attempts to log into the system and are locked out. Employees should also be taught to recognize what constitutes a “security incident,” the term Workman prefers to “security breach.”

Workman recommends annual training—with changes made to training so it doesn’t become stale. She said HHS has indicated it’s reasonable for organizations to train new HIPAA workforce members within 30 days.

**Implement**

If an organization were to be audited, HHS would look to see whether privacy policies and procedures match up with what the organization says it’s doing in its notice of privacy practices. “If there’s a use or disclosure of PHI that’s not covered in your notice, and you have it in your policies and procedures, that’s going to be a violation.”

At their core, policies and procedures for privacy are asking organizations to figure out how to identify individuals seeking access to PHI, and a key area is PHI of a spouse or child. A parent has the right to access PHI of an unemancipated minor. At what age a child is considered a minor and how someone becomes emancipated vary by state. Plans need a process for making sure parents of children between the ages of 16 and 26 are actually entitled to view the child’s PHI before being allowed to see it.

Policies and procedures should cover what to do when a plan participant invokes his or her right to PHI.

A security officer has an ongoing job of keeping track of all information systems—the hardware and software—that create, transmit and retain electronic PHI. “You also have to do what’s called an information system activity review, and that’s looking to see who accesses areas where PHI is, and whether they have the right to that access.”

Technical safeguards need to be in place to support privacy procedures—such as a shared drive accessible only by particular employees. Workman suggested organizations consider using an automatic log-off mechanism so that, after 15 minutes or so of inactivity on a system, a person would have to log back in to access the system.

Organizations need to be sure electronic PHI is encrypted when it’s being transmitted. “If you have misplaced encrypted electronic PHI, it’s not a breach,” Workman said. “The most common culprit for unintentional breaches . . . involves e-mail,” she said. For example, if someone mistakenly e-mails an entire claim file to the wrong person, as long as that document in the attachment is encrypted and password protected and thus inaccessible, it’s just a security incident instead of a breach.

And when somebody’s job duty or employment ends, the

(continued on page 20)
person should immediately lose access to systems containing PHI, she said.

The workforce should be trained to identify security incidents such as misdirected e-mail. Organizations should put together a security incident team that includes the privacy and security officers, probably legal counsel, a broker or consultant if the organization has one, and the public relations department or consultant. Breaches must be communicated to the media—and communication should be written by someone who understands the nuances of press releases. Organizations also should have a computer forensics expert available and a budget for security incidents.

“Definitely consider cyberliability insurance, and be careful when you’re looking at your cyberliability policies because they don’t all cover the standard things,” she said. “You want to make sure you have something that suits your needs.”

And “make sure you communicate. One of the things that can get you into trouble in your organization is having rumors of a breach circulating without any communication from you.”

Document

Workman noted that there are rules for what must be documented under both privacy and security. Among them are nonroutine disclosures of PHI—accidental disclosures, even if they aren’t breaches, and disclosure pursuant to a court order or subpoena. Organizations need to document how they respond to employees invoking their right to inspect a copy of their PHI. Security policies and procedures, and certain security actions, activities or assessments, must be documented.

Retain

Documents must be retained for six years from the date the documentation was created or the date they were last in effect, whichever is later.

Repeat

These steps should be done or reviewed at least annually.

“I understand that you’ve been busy with a few things in the past year,” but organizations need to make HIPAA a priority, Workman said. “HIPAA is . . . getting a lot of attention from auditors,” with large penalties involved and very large amounts involved for security breaches.