Health Information Compliance Alert

Case Study: Follow Through With Security Rule Requirements

Tip: Feds want to see that you've addressed your risks with a compliance plan.

If your practice is doing an annual security risk analysis, that's great. But, if you find yourself on the wrong side of a breach, you'll need more than an analysis of your risks to convince the HHS Office for Civil Rights (OCR) that you're serious about HIPAA compliance.

Background: Many providers, especially those who participate in federal healthcare programs, perform security risk analyses to comply with Promoting Interoperability requirements, but HIPAA compliance with the Security Rule requires much more than just assessing the risks. After evaluating the potential problems, covered entities (CEs) are tasked with "implement[ing] appropriate security measures to address the risks identified in the risk analysis; document[ing] the chosen security measures and, where required, the rationale for adopting those measures; and maintain[ing] continuous, reasonable, and appropriate security protections," reminds the OCR summary of the Security Rule.

Last January, the feds amended the HITECH Act, requiring the HHS Secretary to consider specific "recognized security practices" when investigating HIPAA violations. If CEs and their business associates (BAs) show they've implemented the "recognized security practices" for 12 months, then OCR must consider that when deciding their audit timeline, penalties, and resolutions, suggests the amendment.

Here's the Problem

Though the amendment does define "recognized security practices" as "standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act" and "the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015," it gets a little hazy after that.

This latest HITECH amendment, similar to the language of the Security Rule, allows providers a considerable amount of leeway to determine the route they want to take with designing and implementing HIPAA compliance. There are both pros and cons to this kind of flexibility, especially for providers with limited resources.

"The good news for small practices is that the government designed the Security Rule to be 'scalable and flexible,' meaning that a solo practitioner or a two-person office does not have to implement a HIPAA compliance program with the same level of detail and investment that would be required for a large multi-state hospital system or health insurer," explains attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida. "These smaller practices have some room to maneuver when deciding exactly what they will do to comply with HIPAA's requirements. They have to comply, but they may not be required to have a compliance program that is as detailed and involved as a larger practice," she adds.

Caveat: However, size and scope don't necessarily factor into enforcement, and recent settlements have shown that OCR can be tough on smaller healthcare providers, depending on the situation.

"Small organizations can be penalized for violations. The costs of responding to a data breach add up based, in large part, on how many patients are involved, rather than the size of the entity experiencing the breach," warns Hartsfield.

Consider These Tips

Luckily, there are several things that small practices can do to build their HIPAA compliance plans - and ensure they are implemented according to the Rules. For instance, as part of its training resources, OCR offers "a beginner's overview of what the HIPAA Rules require, security training games, risk assessment tools, and other aids," online guidance says. The agency partners with the HHS Office of the National Coordinator for Health Information Technology (ONC) to provide CEs and BAs with these resources.

Even with the plethora of federal resources and guidance available, compliance planning can be daunting and complicated. "Security Rule compliance still requires significant effort and IT-related expertise so, no matter the entity's size, it may be necessary to hire qualified consultants to help with the risk analysis process," Hartsfield says. And "beyond the risk analysis, covered entities and business associates must also develop a written plan to manage and mitigate the risks identified. They must also update the risk analysis as needed," she advises.

In smaller practices, the appointed security officer needs to cultivate compliance and educate the new employees on the HIPAA Rules. Workforce compliance training needs to be ongoing and take into account both state privacy laws and federal updates, too. "Training isn't something that is given once to a new employee and never again. Training also has to be documented," says Hartsfield.

Overall, HIPAA training programs must resonate with staff, boost security awareness, and align with the CE's specific needs, policies, and protocols.

"If your workforce members have not been trained in your policies and procedures, it not only increases the risk of a data breach, but it could result in increased penalties if that breach happens," Hartsfield cautions. "Staff must be trained in the privacy and security policies and procedures they need to know in order to do their jobs and keep the data they handle private and secure."

BAs also need to up their game on HIPAA compliance, too. "Some business associates only offer employees canned training modules designed for providers, so there is a risk that the employees won't understand the special requirements for business associates. A telehealth physician may need different training than an in-person receptionist," for example, Hartsfield points out.

Resources: Check out OCR and ONC's online tools at www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers. Review the HITECH amendment at www.congress.gov/116/bills/hr7898/BILLS-116hr7898eh.pdf.