Bringing the C-Suite Up to Speed on HITECH-HIPAA

Save to myBoK

by Mary Butler

The HITECH-HIPAA Final Rule has changed the way healthcare organizations do business, and those with seats in the C-suite can't afford to stay out of the weeds with the new regulations.

Daniel Solove, founder of the HIPAA training firm TeachPrivacy, and law professor at George Washington University says that the recent changes to HIPAA—in terms of the government's enforcement power and financial penalties for noncompliance—make it more important than ever for executives to be engaged. This isn't news for health information management (HIM) professionals, particularly privacy and security officers, but attracting engagement from the C-suite is essential in promoting a culture of compliance.

What HITECH Changed for the C-Suite

Solove says that the tightening of regulations for a covered entity's business associates and subcontractors should serve as a wakeup call to the C-suite. According to the new regulations, all of a covered entity's business associates and subcontractors are subject to the HIPAA Privacy Rule. Additionally, business associates are responsible and liable to the covered entity for the activities of their subcontractors.

Before this change in the rule, Solove says healthcare organizations may not have worried as much if their business associates were compliant, "But now they have to take it seriously because if there's an issue, there could be big problems, and not just HIPAA," Solove says. "The costs, increasingly, of not adequately selecting a vendor and not managing a vendor, become higher."

Solove says organizations are slowly starting to realize that if they and their business associates aren't HIPAA-compliant, they won't be able to do business, or components of their business, as they used to. What's more, HITECH greatly increased the fines that can be levied for noncompliance, which is something people in the C-suite might not realize. In addition to federal fines and investigations, state attorneys general can levy their own additional fines for HIPAA violations. "Ultimately I don't think they [the C-suite] fully realize this is a risk. They think it might be maybe like a '3' on the risk scale, and now it's more like an '8' or a '9,'" Solove warns.

HITECH fundamentally changed the US Department of Health and Human Services' (HHS) approach to HIPPA enforcement.

"I think the original enforcement after 2003 was kind of a cooperative model where HHS was kind of like, 'you did wrong, we got a complaint, here's how you can do better. Let us help you.' It wasn't penal in nature, it wasn't punitive," Solove says. "Now it's different. Ever since HITECH, you start to see fines issued. And the hall of shame. And it's much more punitive at this point, we had time with the training wheels, but the training wheels are off."

Relaying the Risk

HITECH's change to the HIPAA breach notification standard raised the stakes for businesses and privacy and security officers need to be proactive in making sure the C-suite understands the risks—and the risks are many. Solove says privacy and security officers are key to keeping the C-suite apprised of regulations, training staff, and taking charge in the event of a breach.

Ideally, large healthcare organizations have whole teams of people dedicated to managing privacy and security. But for smaller organizations, such as critical access hospitals, CEOs and administrators wear many hats, with privacy and security being just

one.

Solove says that smaller organizations that don't have the staff for a privacy and security team should hire a consultant or outside counsel to help with training or risk assessments.

"The expertise is out there, people who can help. The first thing is recognizing this is a serious issue and a big issue and is worth spending some money on," Solove advises.

It's too easy for the C-suite to overlook the costs of not being compliant.

"It's not just the money cost, but the intangible reputation cost. The cost it's going to take in time and sweat to deal with everything," Solove says. "The investigation, that's going to be very time consuming. Dealing with the media, dealing with the agencies that might be investigating you. All of this is going to grab your time."

A security breach isn't a problem that can be solved by writing a check. Rather, it's like getting trapped in quicksand says Solove, and executives who have been through it "have a much greater respect for how disruptive it can be," he notes. "When you see someone has a breach, afterwards, they have a whole new religion when it comes to compliance and privacy and security."

Original source:
Butler, Mary. "Bringing the C-Suite Up to Speed on HITECH-HIPAA" (Journal of AHIMA), April 2014.
