COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 3. March 10, 2022 Privacy Officers: Press BAs Hard on Data Location, Breach Notification Timeline

By Jane Anderson

Business associates (BAs)—particularly those that have operations outside the United States—pose heightened security risks to covered entities (CEs) as remote work becomes entrenched due to the pandemic, privacy officers said.

In a roundtable held at a recent national HIPAA conference, top privacy officials from five health organizations discussed their main concerns and potential solutions for privacy issues.[1]

BAs were top of mind for those who took part in the discussion. Lori Lamb, system vice president and privacy officer for CommonSpirit Health, said her organization is "seeing quite a few issues with vendors large and small," and "it does seem that many of our breach events are at the hands of, or occur at, our vendors."

Complicating that, Lamb said, is the fact that some of these vendors are not headquartered in the United States, and "therefore they do not necessarily have as good an understanding of HIPAA and how to work with us on breach issues [and] notification. Understanding the BAA [business associate agreement] is in place, how does one actually operationalize that when it occurs?"

Vendors also want to offshore data and use international contractors, Lamb said. "That is something we take a very hard look at, because once PHI [protected health information] leaves the U.S., it becomes more challenging to manage."

CE Sees Delayed Notification

Jacki Monson, vice president, chief technology risk officer, chief information security officer and chief privacy officer for Sutter Health, based in California, noted that COVID-19 has changed the way BAs and CEs manage data. Prepandemic, she said, Sutter Health had "compensating physical controls in place to manage data" that no longer are in place "because we sent everyone home." Vendors are in the same position, she said.

Still, the biggest issue Monson said she sees with BAs is delayed notification of an incident, "regardless of what the business associate agreement says. That's often challenging in California because we have really, really short timelines for reporting, depending on [if it involves] a licensed facility or not."

Vendors with many CE clients face challenges with breaches, since they may be dealing with thousands of providers and attempting to determine what data was involved, said Greg Radinsky, senior vice president and chief corporate compliance officer for Northwell Health, based in New Hyde Park, New York.

"For that reason, there's a wide variation with the vendors as to how well they respond," Radinsky said. "Some are great. They'll hire a law firm, or they have the process down, and they're great with the communication. That makes it super easy. Other times, you can't really get information from those vendors. It's very difficult, and you're left trying to decide what to do because you just don't have enough information to decide if your entity was even impacted."

Before the pandemic, Northwell Health made a point of performing audits of large BAs "to make sure that if we have a lot of data stored somewhere with a vendor, that we check them out in a more thorough fashion," Radinsky said. These audits haven't occurred in the last two years because of the pandemic, he said. Still, "breaches are going to happen. It's just part of the business that we're in. We're just trying to make sure that we're as responsive as possible in mitigating the issues."

Bianca Sellinger, director of privacy and enterprise ethics and compliance for One Medical, noted that her organization often functions as a BA, "so any vendors that we are hiring are sub-BAs. And so we have to often make our vendors realize that we have some certain flow-down requirements that come from our contractual relationships with the covered entities, most notably our health system partners in various markets, as we are a national organization."

There are multiple new players in health technology, Sellinger said, and those may be relying on very standard BAA templates, such as the one from HHS. "We have to emphasize that certain things in that template really are the floor—they're not the ceiling," she said. "We might require things that are a little bit stricter in terms of breach notification, timelines, turnaround times and things like that. And so we might get pushback from vendors, especially newer ones who don't realize that there's sort of a sequence of events that needs to happen when the vendor notifies us. If we're a business associate, we need to then notify the covered entity."

This means One Medical must "be pretty aggressive in our timelines," Sellinger said. "And that can often be a sticking point in negotiations when a 24- or 48- or 72-hour turnaround might not be feasible for a lot of vendors, especially smaller ones." At times, she said, "we have to be very firm and sometimes say 'no' to vendors that some of our internal clients wish to engage with, just because they don't have the operational wherewithal or the infrastructure to support the very strict time frames that we need to meet."

One Medical's technology-powered business model means the company considers working with newer vendors "that perhaps aren't as familiar with how to play in the health care space. We are a very heavily regulated industry," Sellinger said. Some of the newer, smaller vendors don't have the infrastructure to comply with the complex regulatory requirements, she said, which means "we need to work with a more established vendor in this space because the risk to patient data is too high. There's often a balancing act and an internal negotiation between our internal stakeholders and the vendors that they wish to work with."