COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 32, Number 8. February 27, 2023
BAAs Have 'Become Almost Noise,' But BAs Were Implicated in Almost Half of 2022 Breaches

By Nina Youngstrom

When a hacker spoofed the email of an employee at a health care consulting firm, it set in motion a notification to clients that was mostly met with a shrug. The hacker had sent emails to the employee's clients with the intention of infiltrating their email accounts and gathering more contacts, but one of them recognized it was phishing and tipped off the consulting firm. Although the hacked email was shut down immediately, the consulting firm was concerned because some clients send unsecured protected health information (PHI) through email. As their business associate (BA), the consulting firm sent letters to clients who were potentially affected and explained the details of the security incident, said Regina Alexander, who worked for the consulting firm at the time. The response was surprising: about a third of the clients ignored the letter, another third asked one question about it and the rest were attorneys who wanted a meeting to discuss it, said Alexander, now a principal with BerryDunn.

The relative indifference was emblematic of the attitude toward business associate agreements (BAAs), Alexander said. "The key point is it's a document that has become almost noise. It's one of those check-the-box compliance items that people sign without reading," she explained. That's unfortunate because covered entities (CEs) pay the price when things go wrong with their BAs, Alexander said at a Feb. 9 webinar sponsored by the Health Care Compliance Association. Alexander noted that BAs were implicated in about 51% of the HHS Office for Civil Rights' (OCR) reportable breaches in 2022 affecting 500 or more people. More powerfully, about 89% of people affected by breaches last year were attributable to the cases involving BAs.

"It shows you where the risk is," she said. The CEs that landed on OCR's so-called wall of shame because of a BA include MCG Health, CommonSpirit Health, Texas Tech University Health Sciences Center and Shields Health Care Group Inc., all caused by hacking/IT incidents involving their network servers, according to OCR.

The HIPAA Privacy Rule allows covered entities to authorize a BA to use and disclose protected health information (PHI) "to carry out its legal responsibilities."[1] The BAA "must limit further disclosures of the protected health information for these purposes to those that are required by law and to those for which the business associate obtains reasonable assurances that the protected health information will be held confidentially and that it will be notified by the person to whom it discloses the protected health information of any breaches of confidentiality."

But some CEs aren't living up to that requirement, according to Alexander. "What's reasonable about two parties exchanging boilerplate agreements and not acknowledging on a deeper level what could be happening? A little more thought is necessary."

Buck Stops With CE

On the surface it may not seem that way. HIPAA doesn't insist on oversight of BAs, said attorney Dena Castricone, with DMC Law LLC, who spoke at the webinar. It takes a hands-off approach, with OCR saying in an answer to a frequently asked question that "covered entities are not required to monitor or oversee the means by

which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract."[2]

Castricone said CEs aren't required to do much before or after they engage the BA. "The only thing that HIPAA says is if the covered entity has actual knowledge of the business associate's material breach, the covered entity has to do something, but the actual knowledge standard encourages covered entities to take a head-in-the-sand approach," she said. Unless CEs do additional due diligence, the chances of a breach caused by the BA are higher, according to Alexander and Castricone.

"It is the covered entity that has the responsibility when something goes wrong," Castricone noted. "It's the covered entity's PHI." Although HIPAA requires BAs to notify the covered entity of a possible breach, it's the CE's job to report the breach to people and to HHS (and the media if more than 500 people are affected) unless the BAA requires the BA to report the breach.

Before CEs sign contracts with vendors, they should kick their tires, Castricone said. She encourages CEs to create due diligence forms and send them to vendors who will have significant access to PHI. Ask whether the potential BA has performed a security risk assessment as required by the HIPAA Security Rule and has a certification like HITRUST. "If you know your potential BA has achieved some of these things and has some baseline knowledge, that should give you a little comfort," she noted.

When it's time to execute the BAA, Alexander and Castricone suggest adding to OCR's model form.[3] "It's important to customize the BAA to meet your organization's needs," Castricone said. "It makes good business sense to use this document to provide as much protection to your organization as possible."

For example, if CEs spell out in the contract with the BA that it must complete a security risk assessment and have policies and procedures about protecting electronic PHI but the BA drops the ball, "it's a material breach of your BAA and an opportunity to terminate it," Castricone said. Also, although HIPAA doesn't require cybersecurity insurance, CEs should require their BAs to have it for both the BA's and the CE's damages. "They normally address it in the master services agreement, but make sure you spell out in the business associate agreement and that in the event of a conflict, the BAA shall govern," she said.

BA Breach Reporting May Backfire

In their BAAs, CEs may shift breach reporting obligations to BAs, but that may not go as planned. For example, in Syracuse, New York, a medical group required its medical billing company to send breach notification letters to patients when it was responsible for a breach, Alexander said. But many patients who got the August 2022 letter thought it was a scam and tossed it in the garbage. Because of buzz about it in the community, a local news station reported on the letter to let the public know it was a legitimate breach notification. The incident probably brought more attention to the medical group than it would have generated by reporting the breach itself, defeating the purpose of shifting the breach reporting to the billing company, Alexander said. "It probably seems like a great thing for practices to minimize their exposure, but it backfired."

BAAs should also address encryption and multifactor authentication although they're not required by HIPAA, Castricone said. BAs would be required to encrypt the CE's PHI when they transmit it or it's at rest. If the BA bungles it and there's a ransomware attack, the CE would be able to extricate itself from the master services agreement, Castricone said. The same goes for multifactor authentication on any services or platforms where PHI is stored or transmitted.

"Don't leave it to your business associate to determine what reasonable safeguards are. It's your data," she said. "The covered entity is responsible for breach notification so it should dictate how the BA will protect the data."

Because of the risks posed by BAs, Alexander recommends that CEs perform retrospective audits of their BAAs. CEs should focus on high-risk relationships, such as vendors who provide release of information, chronic care management and utilization management, because they have access to the CE's electronic health records, and billing vendors, which have access to Social Security numbers and other patient data on claim forms.

Identify the vendors by getting a list from the accounts payable department and winnowing it from there. Some obviously don't have access to PHI (e.g., cleaning companies, website designers). Then determine whether you have a BAA that was signed by both parties. Was it before or after the HITECH Act? "You should have a HITECH-compliant BAA," Alexander said.

Contact Alexander at ralexander@berrydunn.com and Castricone at dena@dmclawllc.com.

1 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000), https://bit.ly/3KwZR55.
2 U.S. Department of Health & Human Services, Office for Civil Rights, "Is a covered entity liable for, or required to monitor, the actions of its business associates?" FAQ, last reviewed January 9, 2023, http://bit.ly/3EvMX3v.
3 U.S. Department of Health & Human Services, Office for Civil Rights, "Model Business Associate Agreement," last accessed February 23, 2023, https://bit.ly/3lYtTEy.