Report on
MEDICARE COMPLIANCE
Volume 25, Number 23 • July 25, 2016

Business Associate Agreement Is Opening To Cover More Privacy, Compliance Bases

A health care organization learned the hard way to think more broadly about privacy and security when one of its vendors was attacked by ransomware. The cybercriminals stole employee information from the vendor, compromising the data of the health care organization in the process. Although their business associate agreement (BAA) required the vendor to comply with the health care organization's policies on HIPAA breach reporting and indemnify it for losses stemming from a breach, this wasn't any help with the theft of W-2s.

"Everything in the business associate agreement was limited to HIPAA," said Hartford, Conn., attorney William Roberts, with Shipman & Goodwin. "As their lawyers were happy to point out, [the vendor] didn't violate any of those policies."

Because the vendor had no obligation to pay for breach mitigation, the health care organization was on its own. "There was nothing binding them in the contract to help, and there was such animosity between them," Roberts said at a July 19 webinar sponsored by the Health Care Compliance Association (HCCA). It turned out to be a large breach that had to be reported to two states. Although neither state levied a fine on the health care organization, it was required by one of the states to increase protection of Social Security numbers consistent with state law requirements, he said.

If the BAA had been modified to include security incident reporting beyond HIPAA, there would have been a softer landing for the health care organization. "There is value in taking a holistic approach to privacy and security, especially as privacy laws expand in scope," Roberts said. "Providers have a lot more valuable information than just PHI. When you are developing breach notification policies, you might as well protect everything you have." For example, companies should protect trade secrets as well as PHI. They may have great HIPAA policies but "a lot of other data is tossed out all over the place."

And there is a balancing act with vendors. Vendors are often the source of breaches and, on June 30, a business associate for the first time settled a HIPAA case with the HHS Office for Civil Rights (see briefs, p. 8). But health care organizations can't function without vendors and need their goodwill. "The biggest source of dispute is breaches," Roberts said. "To avoid having a breach torpedo the relationship, include in your BAA or in your confidentiality agreement with non-business associates exactly what you want."

He recommended that covered entities have a "master BAA" with each business associate. "I have found that to save a massive amount of hassle." Last year, Roberts worked with a small hospital chain that had a breach caused by a vendor. The hospital chain had seven BAAs with the same vendor. "Every time they engaged the vendor, there was a new consulting agreement and their staff diligently said, 'we need a BAA,'" he said. Instead of referencing the BAA already in place, the hospital chain added a new one. That caused a lot of trouble when a laptop was stolen from the vendor. The breach was governed by three of the BAAs, which had different provisions on breach reporting, and the vendor and hospital chain didn't exactly see eye to eye on which should apply, Roberts said. "If the hospital had used one BAA, it would have saved a lot of time and hassle and the result for the hospital would have been a lot better."

As covered entities move through the BAA process, they should keep in mind the concept of vicarious liability. It means covered entities may be liable for the acts and omissions of business associates, and business associates may be liable for the acts and omissions of subcontractors. "You don't want to be sued for something your business associate did," he said.

Covered entities may be liable if business associates are their "agents," he said. There's no bright-line rule for when business associates are the agent of covered entities, but they probably are if you can control their conduct. For example, if a hospital tells a consultant to use 128-bit encryption instead of 256-bit encryption, and then it's hacked, "it was the consultant using poor encryption, but acting at the direction of the hospital," he said. Stating the BA is not your agent in a contract isn't going to help.

When hiring a vendor, never assume it's HIPAA compliant. "It's amazing how many times clients will say 'this IT vendor or this consultant has been in business for a decade. They must comply with HIPAA,'" he said. "Don't rely on experience or a statement on a website saying they are HIPAA compliant." Covered entities need written assurances from business associates, and

resources permitting, you may want to request a copy of their HIPAA policy. You can get a flavor for how seriously the vendor takes privacy by looking at a subset of their policies."

When drafting BAAs, Roberts suggested focusing on certain areas, including:

(1) Breach notification: Certain requirements must be included, such as deadlines for reporting breaches to covered entities. While HIPAA gives business associates 60 days from discovery, "regulators will not look fondly on covered entities that give their business associates that much time. Push for a shorter maximum reporting time frame," Roberts said. Consider a "bifurcated obligation": the business associate must inform the covered entity of the breach first (e.g., within three days), and give it the details later. Also, take into account state laws that require faster breach reporting, especially when Social Security numbers are involved.

(2) Breach mitigation: "This is often overlooked in BAA negotiations," he said. There may be a reference to a mitigation obligation, but it's better to be concrete. For example, if the business associate is responsible for the breach, it agrees to set up a call center to answer questions from affected people and to make records, staff and advisers available to help the covered entity investigate the breach.

(3) Cooperation: Put it in writing that business associates will participate if the covered entity comes under investigation by the HHS Office for Civil Rights (OCR), a state attorney general or another state or federal agency. "You may need to say to business associates that 'we need copies of books or policies to respond to OCR,' and if you don't have this in the BAA, you will be wasting time and in some cases looking foolish to the [government]," he said. It's not a great time to play tug of war with a vendor because the relationship may already be tense as a result of the breach.

(4) Indemnification: Roberts suggested addressing indemnification — which means the party that caused the breach will pay the costs, expenses, fines and losses — in the BAA. Business associates should agree to indemnify covered entities for breaches that are their fault, but if they refuse to agree to write a blank check, covered entities should nail down what they want to be reimbursed for. Breach notification costs? The call center? Attorneys' fees? Public relations expenses? Figure out the most expensive items in a breach investigation because they should drive the indemnification. "If you are certain there will be a call center, then certainly those are costs you want indemnification for," he said.

Business associates will request an indemnification cap, and for good reason. "Covered entities should tie the cap to the amount of PHI at issue or link the indemnification to cybersecurity insurance," he said. If the covered entity disclosed only 50 records to the BA, there's probably no reason for a standard $50 million liability cap. Studies show the average cost of a breach is $250 per record plus fines and penalties. Two caveats: (1) If you agree just to accept the BA's cybersecurity insurance and it gets hacked by a criminal organization, the BA's insurance company may not come through, Roberts said. "Possibly the insurance policy doesn't cover criminal acts by terrorist states. There could be exclusions that result in your not being indemnified at all"; and (2) Whatever is negotiated in the BAA is worthless if the underlying service contract says something different. "You have to make sure all agreements work in concert," Roberts said. If the service agreement, with a $30,000 liability cap, trumps the BAA, you're out of luck.

(5) Mutual indemnification: Both covered entities and business associates agree to cover the other party's costs and damages for any breach they cause. This generally benefits covered entities more because it's "more likely to be the one seeking to recover costs or damages."

(6) Compliance addendum: Cover other bases in the BAA. For example, covered entities could require vendors to screen employees for exclusion from Medicare and other federal health care programs and certify their compliance with the anti-kickback laws and Joint Commission standards.

Some vendors don't require BAAs, but confidentiality agreements are necessary for "incidental disclosures." According to OCR, "the Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure."

For example, hospitals don't need BAAs with electricians, plumbers or copy-machine technicians, said Donna Wypych, principal at Health Care Program Design. Any PHI disclosures that occur while they work are considered a byproduct of their job duties, she said at a May HCCA webinar. "Does it mean it's safe to leave PHI out when they are there? No. PHI must always be protected. If you have to leave a workstation for a moment, put papers face down." Clean off the fax machine and turn computer screens away. "There is some degree of risk, but it's permitted."

Have the vendors sign confidentiality agreements that define confidential information, Roberts said. They also should "prohibit requesting or accessing confidential information outside the scope of the engagement."

Contact Roberts at WRoberts@goodwin.com and Wypych at dwypychhcpd@gmail.com. ✧