COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 3. March 11, 2021 After a Breach Is Too Late: Ensure BA, Subcontractor Compliance Now

By Theresa Defino

Sometime during the fall, a worker for a subcontractor of Humana Inc. decided to share actual member information from medical records via a Google document with people he was training to be medical coders, part of his attempt to run a "personal coding business endeavor."[1]

Early last month, Humana had to notify 65,000 individuals, multiple state officials, the press and the HHS Office for Civil Rights (OCR) of the worker's data breach. In its notification, Humana said unauthorized access continued from October to December before it was discovered by the now-former worker's employer, which Humana said is named Visionary. Technically, Visionary is (or was—current status isn't clear) a subcontractor for a company called Cotiviti, which Humana uses to develop risk adjustment scores needed for payment of certain members. Cotiviti is a business associate (BA) of Humana, the covered entity (CE).

Around the same time, Accellion Inc. was informing its clients that hackers had accessed its file transfer system[2] —among them a big law firm whose exposed documents included prescriptions written for hundreds of patients, including their names. As of *RPP's* deadline, it did not appear the patients had been notified (see related story, p. 1).[3]

HIPAA compliance officials know that patient data must be safeguarded everywhere it resides and when it travels from CEs to BAs and then on to subcontractors. And as these recent incidents show, the ties that bind these organizations are crucial to ensuring proper notifications are made in the event of a breach.

But how can CEs be certain that BAs and subcontractors will perform well after an unauthorized disclosure, and in general, be compliant during their usual handling of protected health information (PHI)?

For Erin Smith Aebel, a shareholder in the Tampa, Florida, office of Trenam Law, the answer begins with due diligence in selecting BAs and subcontractors that are "worthy," insisting on a strong business associate agreement (BAA), and implementing other oversight efforts.

Is Your Subcontractor 'Worthy'?

Issues with subcontractor noncompliance may arise because the government hasn't taken enforcement action against one, which could prompt some of them to say they are "three levels down" from BAs, which have been party to enforcement settlements, Aebel told *RPP.*

And while signing an agreement might not come with a fight from a subcontractor, "what I'm more worried about is: Can they actually comply with the terms? Do they have the internal processes to really do what they're saying they're doing? I almost think that business associates, if they were really worried about it—and they should be—should be doing their own internal audits for compliance of their subcontractors," she said.

The BA should know if the subcontractor is "truly worthy of the contractual arrangement where we are sharing protected health information," Aebel said. "It seems like there should be some due diligence beyond signing the

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

vendor agreement." The BA could request to review privacy and security policies and procedures and even talk to the subcontractor's information technology employees, she suggested.

In her experience, Aebel has found that often she's the one telling health care providers, particularly small physician practices, when a BAA is needed.

Know When a BAA Is Necessary

"Almost all of my clients are health care providers, but I am not always [acting as] a business associate," she said. "But the minute they [say], 'I've got this patient issue, and they're complaining about this, can I send you their name and information and let's talk about it?' I [say], 'Wait a minute, let me send you our law firm's HIPAA business associate agreement.' Thankfully, most law firms are sensitive to security, confidentiality and data breaches, as well as [being] lawyers."

In turn, Aebel knows when she, as the BA, needs to sign an agreement with a subcontractor that will be working with her clients' PHI. Such an agreement, she told *RPP*, is nearly identical to the BAA that she signs with CEs.

"The HIPAA law requires that the business associates have a contract with a covered entity to protect the confidentiality and security of the protected health information that they get," said Aebel. "And if [BAs] have a subcontractor, like Accellion, they have to have a subsequent agreement with them for that," Aebel said.

Include Certain Essential Provisions

While specifics will vary, Aebel said provisions in agreements should address three essential areas: notification timeframes, indemnification and cyber insurance in the amount of $1 to $3 million. Her law firm's agreements with subcontractors—and she recommends this for others—require cyber insurance to cover notification and breach-related costs "because sometimes the actual cost of doing the investigation and notifications could be more than any penalties the government would likely assess." Indemnification is also required.

For sample language that Aebel uses in subcontractor and business associate agreements, see box.[4]

Assuming Accellion is a subcontractor, it would be required to notify its BA clients, and the BAs must notify their CEs when there is a breach. Formal notification to patients and OCR rests with the CE, although CEs and BAs can negotiate who will make notification and, perhaps more importantly, who will pay for notification and associated breach costs should the BA—or subcontractor—be found at fault, Aebel said.

The law "does not say [BAs] have to personally contact every single patient," but "if it does involve individuals, they have to provide the covered entity with the information" to make an accurate notification to them. This might take more than one notification if a lot of patients are involved or if the number grows over time with more investigation, she said.

The agreement also may obligate the BA or subcontractor to coordinate and discuss notification with the CE. "Usually health care providers will want to have some control and say over what's said to their patients" and will not "want some third party telling their patients" about a breach, Aebel said. "However, they may impose the cost upon the business associate."

Speed Up Subcontractor Notification

Ensuring quick notification is "definitely a concern" that should be addressed in subcontractor agreements, according to Aebel. "When you have [subcontractors] several layers down and you just use the same form for all of them...it is troubling. You need to have shorter notice periods to be cautious," she said, and allow the CE

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

enough time to investigate and determine if notifications are required.

By law, CEs are required to notify patients and OCR within 60 days of learning of a reportable breach, if the disclosure affects 500 or more individuals (smaller breaches are reported annually to OCR). To make that deadline, CEs need to give their BAs, and BAs their subcontractors, a quicker notification requirement, Aebel pointed out.

In some instances, the BA or subcontractor may be required to give notification within 24 hours of a "security incident;" the time can be negotiated but it should be as quickly as possible to enable the CE to meet the 60-day reporting deadline, she said.

Aebel, in contrast, wouldn't propose shortening CEs' 60-day notification requirement—that time is often needed, she said, and why she supports the shorter time periods for BAs and subcontractors to report to them.

The 60-days is "perfect" for CEs, Aebel said.

After a breach, "they have to do an investigation, and that's expensive and timely," to determine whether there was a reportable breach based on HIPAA, but also state laws, she said. Notification is supposed to be as specific as possible, informing individuals what information was or may have been disclosed, a "level of detail" that may take time to uncover, said Aebel, who termed the 60-day notice requirement on the "long end of reasonable."

She noted that some BAs and subcontractors—and smaller CEs—may lack the resources to respond quickly and appropriately to a breach. This is what appeared to be the case with the physician whose PHI was part of the Jones Day breach.

Office staff told *RPP* they were not aware his patients' PHI was on the dark web, a fact that meant any investigation and ultimately notification to patients had not yet begun.

Keep Patient Expectations in Mind

Aebel said she may have sympathy for a small physician practice that "is not going to have a public relations firm to tell them how to deal with responding to a data breach" and "doesn't have the same tools" available as a large hospital system.

"But this is the thing…they have the same laws" governing their actions, said Aebel, and perhaps as important, the same obligations to patients.

Big or small, BAs and subcontractors—along with their CEs—must ensure patients' PHI is kept safe from hackers like those who hit Accellion and others who may want to misuse it, such as the Humana subcontractor starting his own coding business.

Patients "don't want their sensitive records out there, and they want to know about it, and want to know that it's being taken care of" in the event of a breach, "regardless of all the relationships between the parties and where they stand," said Aebel. "That's really at the core of what these laws are about."

Contact Aebel at eaebel@trenam.com.

1 "Alerts and notifications," Humana, March 5, 2021, http://huma.na/38klj9y.
2 Accellion, "Accellion Provides Update to FTA Security Incident Following Mandiant's Preliminary Findings: Mandiant Identifies Criminal Threat Actor and Mode of Attacks," Security Update, February 22, 2021, http://bit.ly/3rsiomx.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

3 Theresa Defino, "Fallout From Accellion, Humana Breaches Puts Focus on Subcontractors, Notifications," *Report on Patient Privacy* 21, no. 3 (March 2021).
4 Trenam Law, "Select Provisions of Subcontractor Agreement (Sample)," *Report on Patient Privacy* 21, no. 3 (March 2021).

This publication is only available to subscribers. To view all documents, please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.