HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

APRIL 2018

A smooth transition

an interview with
Gerry Zack
Incoming CEO
SCCE & HCCA

ARTICLES

Compliance TODAY

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to Compliance Today, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

VOLUME 20, ISSUE 4

by Marti Arvin

Business associates: Have you really integrated them into your risk profile?

» When applicable, business associate agreements (BAA) that meet all of the regulatory requirements must be in place.

» Having an appropriate BAA does not necessarily mitigate the risk for the covered entity.

» The BAA should require the associate to notify the covered entity of incidents that involve a violation of the HIPAA Privacy or Security Rules.

» Covered entities should determine if a business associate's data compromise is a breach.

» Covered entities must exercise ongoing due diligence for business associate compliance.

Marti Arvin *(marti.arvin@cynergistek.com) is Vice President of Audit Strategy at CynergisTek in Austin, TX.*

When the HIPAA Privacy Rule became enforceable in April of 2003, many organizations made efforts to assure a business associate agreement (BAA) was in place when a vendor was clearly going to handle protected health information (PHI). However, the level of effort was quite varied. Since that time, organizations have increased and improved on these efforts. With the changes under the HITECH Act[1] and the corresponding implementing regulations, organizations updated their agreements and made efforts to get newly signed BAAs with current vendors by the September 23, 2014 deadline.

Arvin

In April of 2012, the Office for Civil Rights (OCR) entered the first Resolution Agreement and Corrective Action Plan (RA/CAP) that involved a finding regarding the lack of a BAA.[2] Still, many organizations did not give this significant attention until OCR began its Phase II audit process in the beginning of 2016. One of the initial steps of that process asked covered entities to provide a list of their business associates. This request had some covered entities scrambling to produce the list and questioning the completeness of their list. Later in 2016, OCR had its first RA/CAP that involved the failure to update a BAA in a timely manner.[3] The resolution amount was $400,000. Almost exactly six months later, another agreement was entered with OCR over the failure to obtain a BAA.[4] This time the amount was only $31,000.

All of this demonstrates the regulatory obligation to assure that when a covered entity engages a vendor to perform a service for or on its behalf and the vendor will create, receive, maintain, or transmit PHI in the performance of said activities, the covered entity will obtain satisfactory assurance that the business associate will appropriately safeguard the information.[5] These assurances are obtained through a BAA. However, obtaining a BAA that meets the regulatory provisions may not be sufficient to appropriately address risks.

Implications to the covered entity's risk profile

Although an organization might be doing a good job of getting a BAA in place, that is not enough to fully address the risk a business associate relationship may pose to the covered entity. This is not a one-and-done undertaking. The assessment of how the business associate fits in to the covered entity's risk profile is an ongoing process throughout the life cycle of the relationship. It starts with the due diligence necessary prior to beginning the relationship and goes through the processes needed to end the relationship. Questioning the business associate's compliance during this entire process is necessary to accomplish this.

The regulations require the covered entity to obtain satisfactory assurances through the BAA, but there is no guarantee the business associate will appropriately safeguard the information. Further, other than the mandated provisions of a BAA, there is no definition in the regulations that clarifies what the "satisfactory assurances" must be. OCR has clarified through its FAQ process that a covered entity is not obligated to monitor how a business associate specifically is safeguarding the covered entity's data. However, failure to perform any due diligence can create risks for the covered entity. Let's look at one example to demonstrate this—a data compromise at the business associate.

Under the HIPAA Security Rule, a BAA must include a provision requiring the business associate to notify the covered entity of any security incidents.[6] The rule defines a security incident as "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with systems operations in an information system."[7]

Most organizations have dozens if not hundreds of business associates. Although all of the vendors who fit the definition of a business associate might not have large volumes of an organization's PHI, a significant percentage will. Most organizations I speak with have had very few notifications from their business associates of a security incident. In that same vein, I have encountered very few organizations that believe their business associates are not being impacted by the same cybersecurity issues as others in the healthcare space.

Why are there so few reports of security incidents by vendors?

The answer to the question could be quite simple. Either the vendors don't know about the attempted or actual cyberattacks on their systems, or they know but are not reporting them. Whichever it is has implications to the risk profile for the covered entity.

Another consideration is whether, as a covered entity or a business associate with a downstream subcontractor, the only interest is in security incidents. By definition, a security incident only involves electronic PHI (ePHI). If the BAA only discusses the need to notify the covered entity of "security incidents," the vendor has no explicit obligation to notify the covered entity of other types of data incidents, such as those involving improper access to paper or verbal information and/or use, disclosure, and modification or destruction of PHI.

Many might think this issue of reporting only security incidents is resolved by the requirement of the HIPAA Breach Notification Rule that states a business associate must notify a covered entity of a breach without undue delay but no more than 60 days after discovery. However, this provision may still not lead to the covered entity being notified by the business associate of non-security incident data compromises.

This is because the rule only requires the business associate to notify the covered entity of a "breach." A breach, as defined by the regulations, means an assessment has already occurred to determine whether notification is

required.[8] This means if the BAA requires the business associate to notify the covered entity of a breach, the business associate is determining whether notification is required. If the business associate makes a determination that a notice is not required, the obligation to notify the covered entity is not triggered. This could be a problem for the covered entity.

If the business associate assesses an incident and determines no breach occurred, the covered entity has the liability for failure to timely notify the affected individuals and the OCR if the business associate is wrong. The regulatory provisions in the HIPAA Breach Notification Rule make it the obligation of the covered entity to notify individuals and the OCR when a breach occurs.[9] This is not the obligation of the business associate. The business associate's obligation is to notify the covered entity.[10] This is why it is important to assure the language of the BAA protects the covered entity and that covered entities are proactive in assuring business associates are meeting their obligations.

Covered entities should also be monitoring any reported incidents of data compromises at their business associates.

Covered entities should be proactive

The BAA language should require that the business associate notify the covered entity of all possible or actual data compromises, not just security incidents. The language should further clarify that, while the business associate is obligated under the HIPAA Breach Notification Rule to notify the covered entity of a breach, the covered entity should also be notified of any instance where the business associate assessed a situation and determined it was not a breach. Some organizations include language that requires the business associate to notify them of any HIPAA Privacy or Security Rule violation as a way of handling this issue. Once a covered entity is notified of an incident, it should be initiating interactions with the business associate to learn as much as possible about the nature of the incident, what data might have been compromised, and what the business associate is doing to handle the incident. Covered entities should also consider language that clarifies their right to make a final determination whether the incident is a breach and thus requires notification to the affected individuals and OCR.

Covered entities should also be monitoring any reported incidents of data compromises at their business associates. Once a data compromise has been publically reported, such as through the media, the incident is likely deemed discovered by the covered entity. For example, if the media reports that a business associate was the victim of a ransomware attack, covered entities should be reaching out to the business associate to determine what happened. Ransomware attacks are particularly significant. Whether a ransomware attack is a breach was debated by the industry until the OCR issued guidance on the topic.

The OCR guidance is that a ransomware attack is very likely a compromise of any PHI on the systems impacted by the attack.[11] The guidance tells us that if ePHI was encrypted by the attacker, it means the attacker has acquired the data, because they have taken possession or control of the ePHI. This acquisition by the attacker is a disclosure that would not otherwise be permitted by the Privacy Rule. There is some room in the guidance for a determination that the attack was not a breach if the covered entity or business associate

can demonstrate the data was not "accessed" or "exfiltrated" by the attacker. However, the guidance seems to imply the evidence of this must be very strong before an organization can say there is a low probability of compromise.

Because the regulations place the duty to notify on the covered entity, it is critical the covered entity be aware of what the business associate is doing and carefully review the determinations made by the business associate. A covered entity should carefully consider whether it will allow the business associate to be the final decision-maker regarding whether a breach has occurred. If the business associate's position is that no breach has occurred, the covered entity should ensure they are very confident in the evidence the business associate has used to demonstrate the low probability of compromise.

Although the covered entity, through the BAA, might transfer the activities and/or cost associated with breach notification to the business associate when the incident is the result of the business associate's acts or omissions, the legal responsibility to notify remains with the covered entity. This is why it cannot be emphasized enough that once the covered entity discovers that its business associate has had a data compromise, the communication channels are opened, and the discussions begin to ensure breach notification, if required, is done within the regulatory timeframe. The covered entity needs to assure the business associate is taking prompt action. The covered entity should question whether appropriate system analysis and forensics have been done. They should also know what steps have been taken to identify the data impacted. Failure of the business associate to act promptly can quickly absorb the limited time period for notification.

Conclusion

Covered entities may wish to reassess and/or update the language of their BAAs regarding what types of incidents the business associate must notify the covered entity about and the timing of such notification. They should also consider the language regarding who is responsible for what, if a data compromise like a ransomware attack occurs. Covered entities should not just rely on a statement from the business associate that notification is unnecessary. This is definitely a "trust, but verify" situation. Getting a valid BAA with a vendor may satisfy the regulatory obligations for the covered entity, but it does not necessarily eliminate the risk to the covered entity. Ongoing diligence through the entire relationship is a must.

1. Health Information Technology for Economic and Clinical Health (HITECH) Act Interim Final Rule. February 17, 2009. Available at http://bit.ly/2gu0mNS
2. U.S. Department of Health and Human Services, Office for Civil Rights: Resolution Agreement - Phoenix Cardiac Surgery. Available at http://bit.ly/2FEwF7q
3. DHHS, Office for Civil Rights: Resolution Agreement and CAP - Women and Infants Hospital. 2016. Available at http://bit.ly/2nD7JWz
4. DHHS, Office for Civil Rights: Resolution Agreement and CAP – Center for Children's Digestive Health. 2017. Available at http://bit.ly/2pA8Cm3
5. 45 C.F.R. 164.308(b)(1) and C.F.R. 164.502(e)(1) et. seq.
6. 45 C.F.R. 164.314(a)(2)(C)
7. 45 C.F.R. 164.304
8. 45 C.F.R. 164.402
9. 45 C.F.R. 164.404(a) and 164.508(a) et.seq.
10. 45 C.F.R. 164.410 (a)
11. DHHS, Office for Civil Rights: Fact Sheet: Ransomware and HIPAA. 2016. Available at http://bit.ly/2ml8Mgd