COSMOS
Navigate the Compliance Universe

Compliance Today - July 2020
Follow the money … to your business associates

By Tiffany Holman, MS, CHPC

Tiffany Holman (tiffany.holman@adventhealth.com) is the Director of Privacy at AdventHealth in Orlando, FL.

Are we still discussing business associate agreements (BAAs) after all this time? Yes, and privacy professionals continue to have questions and confront challenges. Here are a few questions that linger for privacy professionals:

- Does our organization have compliant BAAs in place for all vendors?
- Who are our vendors, and how do I obtain a list to identify them?
- Is our leadership/staff trained to know how to properly obtain a BAA from a vendor?
- If a staff member obtains a signed BAA, is there a procedure in place to submit the BAA to the privacy officer?

We are slowly moving away from denial that a BAA is needed altogether toward understanding that BAAs are needed, and privacy professionals must continuously monitor vendors as part of an effective compliance and privacy program. Let's start from the beginning to understand the evolution of BAAs.

Business associate regulation review

The regulations that govern BAs are not new, and most privacy professionals are familiar with them, but an overview is helpful. In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act, making BAs liable for noncompliance with certain requirements of the Health Insurance Portability and Accountability Act of 1996 regulations. As of September 23, 2013, the HITECH Act and the Office for Civil Rights' (OCR) final rule required BAs to comply with the Security Rule, Breach Notification Rule, and parts of the Privacy Rule. Failure to comply subjects a BA to liability under these regulations.[1]

The regulations also expanded the definition of business associate to include persons or entities that create, receive, maintain, or transmit protected health information (PHI) on behalf of a covered entity[2](e.g., attorneys who provide legal services for the organization, a company that destroys or stores PHI, or companies that provide a callback service to members/patients after business hours).

To aid with this process, the OCR provided a decision tree to help determine if a BAA is needed or whether specific exclusions apply. Exclusions include, but are not limited to, other covered entities or vendors with access to PHI that is considered "incidental," such as a janitorial service.[3] Although the decision tree provided by the OCR is helpful, consulting with your legal counsel is always a good idea when you are unsure whether a BAA is needed.

OCR enforcements

Six years after the Omnibus Rule passed, failure to have a BAA in place remains one of the trending areas for OCR enforcement. In December 2018, Pagosa Springs Medical Center, a hospital in Colorado, agreed to pay the OCR

$111,400 and adopt a corrective action plan due to failure to obtain a BAA with a calendar company. In turn, electronic PHI of 557 individuals was disclosed to a former employee and the web-based scheduling calendar vendor.[4]

Also, in December 2018, Advanced Care Hospitalist PL, a physicians' group located in Florida, agreed to pay OCR $500,000 and adopt a correction plan due to failure to obtain a BAA with a company providing medical billing services to the physicians' group.[5] They also failed to adopt a policy requiring BAAs until April 2014. The groupwas able to identify at least 400 affected individuals and asked the billing company to remove the PHI from its website.

The recent OCR fines pertaining to BAAs are a clear indication that a breach involving a third-party vendor, without a BAA in place, is almost guaranteed to result in monetary damages. The risks are high, and it is very important for organizations to implement a process and, preferably, a policy to identify their vendors and know when a BAA is needed.