COSMOS
Navigate the Compliance Universe

Compliance Today - June 2023

Taryn Bevilacqua (tarynb4@hotmail.com, linkedin.com/in/taryn-bevilacqua-b158764/) is Assistant Vice President, Global Healthcare Compliance, at EXL Health, based in New York, NY.

Compliance through the eyes of a business associate

by Taryn Bevilacqua

Am I a business associate (BA)? I am not a covered entity; therefore, I think I am. But how do I know? If you do anything where you receive, create, transmit, or maintain protected health information (PHI) for a function or activity regulated by HIPAA on behalf of a covered entity or another BA, then your answer is yes. Following is a simple example to better understand. Hospital ABC outsources its billing to Smith's Billing and Co. Smith's is a BA of Hospital ABC because it receives PHI from a hospital—a covered entity—to provide billing, which is a function or an activity. This is just one example, but there are many others as well, such as shredding services or subcontractors. The simplest way to identify a BA is by asking the question of whether there is any type of PHI received, created, transmitted, or maintained for a function or activity regulated by HIPAA on behalf of a covered entity or another BA.[1]

A business associate agreement (BAA) is a type of contract dictated by HIPAA, which outlines the responsibilities of another party you're doing business with when it comes to PHI. The HIPAA Privacy Rule requires all covered entities to have a signed BAA with any BA they hire that may come in contact with PHI.[2] In addition to the BAA with the covered entity, the BA must have a BAA with each of its sub-BAs that create, receive, maintain, or transmit PHI on behalf of the BA.

BAs are responsible for compliance the same way covered entities are. Prior to the HIPAA Omnibus Rule, BAs' HIPAA responsibilities and liabilities concerning PHI were based only on the BA's contractual responsibilities with the covered entity; however, once the HIPAA Omnibus Rule of 2013 passed, BAs became subject to the HIPAA security and enforcement rules and parts of the HIPAA Privacy and Breach notification rules.[3] What does this mean exactly? In a nutshell, BAs now have the same responsibilities as covered entities under these rules; they need to be aware of what these regulations require, such as training, policies, etc., and not only worry about their contractual obligations with the covered entity. Of course, those are still required, but now there are additional requirements. Depending on the size and number of vendors or BAs involved, this can be quite the task for some.

BAs do not typically receive requirements from just one source. The requirements come from multiple resources such as regulations, attestations, contracts, and audits. It is up to the BA to be able to manage all these requirements. The BA can be responsible for things from training to sanction reviews depending on their world. Compliance training, incident reporting, vendor oversight, and protecting PHI are now responsibilities of all BAs and not just covered entities. BAs have a duty to report disclosures to the covered entity and are responsible for maintaining an accounting of the disclosure log. They need to ensure HIPAA and security awareness training are implemented, are responsible for vetting all vendors, and provide a secure environment for PHI by conducting activities such as implementing locking workstations, audits, and encryption.