

HIPAA: Back to basics with the BAA

August 12, 2021

Rachel V. Rose, JD, MBA

With cybersecurity and criminal government actions involving protected health information (PHI), now is a good time to understand the importance of the required Business Associate Agreement (BAA).



Before delving into the nuances of the requisite BAA, it's important to highlight the following three items:

- Two of the U.S. Department of Justice's (DOJ) [False Claims Act enforcement priorities](#) are cybersecurity and electronic health records;
- The [Eastern District of Texas U.S. Attorney's Office](#) recently announced that another individual out of a group of co-conspirators was sentenced in July 2021 for the "theft of protected health information, the fabrication of physicians' orders, and the sale of prescriptions will not be tolerated in the Eastern District of Texas";
- A former Scripps Health employee, as well as three alleged co-conspirators, [were charged in San Diego for the theft of patient information](#), which was in turn used to submit false and fraudulent unemployment claims.

These three items are important because HIPAA, like the Federal Anti-Kickback Statute (AKS), has criminal penalties available to HHS. The DOJ is responsible for criminal prosecutions, as illustrated by the two aforementioned examples. As HHS states on its [website](#),

A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to \$50,000 and up to one-year imprisonment. The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm.

The [inter-play between the FCA, AKS, and HIPAA](#) is illustrated by the DOJ's 2015 enforcement action against pharmaceutical manufacturer Warner Chilcott to resolve a felony healthcare fraud scheme that resulted in a \$125 million settlement to resolve criminal and civil liability. Here, the pharmaceutical company remunerated physicians either in cash or in-kind through speaker programs and meals in exchange for access to patient records, which led to reps evaluating and assisting with pre-authorizations or submissions to government programs. In light of the Supreme Court's 2016 *Escobar* decision, which upheld that false claims can be predicated upon the theory of implied certification, this is an area to watch because it difficult to argue that HIPAA, HITECH Act, and 21st Century Cures Act compliance is not material to the United States Government.

This leads up to the discussion around the BAA. First, a BAA is required between a covered entity and its business associate; and, in turn, between a business associate and its subcontractor. As HHS articulated on its [website](#):

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A

*“business associate” also is a subcontractor that **creates, receives, maintains, or transmits protected health information** on behalf of another business associate. (emphasis added).*

Business Associates encompasses a wide range of persons, which include, but are not limited to: accountants, attorneys, private equity firms, technology companies, app developers, independent contractors, medical device companies, and pharmaceutical companies. Bottom line—if you or your company “creates, receives, maintains, or transmits” protected health information in an electronic form, a BAA is required. This is not new—the requirement existed long before the HIPAA Final Omnibus Rule was published in the *Federal Register* on January 25, 2013.

This leads us to the four primary purposes of the BAA:

1. provide reasonable assurances that both parties have the requisite technical, administrative, and physical safeguards in place;
2. that the parties will act in accordance with the HIPAA Privacy and Security Rule, including what entity has the obligation to provide patients with their medical record requests;
3. breach notification requirements; and
4. destruction or return of data when the relationship between the parties ends.

Later this month, I will delve into the specifics of the BAA to alleviate any confusion. For those who have read numerous BAAs, it should come as no surprise that certain language is consistent throughout. This is because HHS provided a template. Parties are free to add additional language, but it must not contradict what is required.

The overall take-aways are that HIPAA compliance is not optional and depending on the facts and circumstances, may lead to significant civil and/or criminal liability.

About the Author

Rachel V. Rose, JD, MBA, advises clients on compliance and transactions in healthcare, cybersecurity, corporate and securities law, while representing plaintiffs in False Claims Act and Dodd-Frank whistleblower cases. She also teaches bioethics at Baylor College of Medicine in Houston. Rachel can be reached through her website, www.rvrose.com.