Business associate agreements 101

By Daniel F. Shay, Esq.

Every month, DermWorld *covers legal issues in "Legally Speaking." This month's author is a health care attorney at Alice G. Gosfield and Associates, P.C.*

Want to read more about legal topics?

Check out *DermWorld* for more Legally Speaking at **www.aad.org/dw**.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has been a fact of life for physicians for decades. Regulations for the Privacy Rule were first published in 2000, with the Security Rule being published in 2003, and additional modifications published over the years since then. In that time, many physician practices have grown familiar, even comfortable, with aspects of HIPAA and especially the Privacy Rule.

One aspect of the privacy rule — business associate agreements (BAA) — is a familiar term to most physicians, but they may not really understand what it means, when BAAs are necessary, or what a BAA must include. Understanding what BAAs are and how they function is essential because if the business associate breaches its agreement, it can create direct liability for the physician practice, as if it breached the law itself. In this article, we clarify and explain a few misconceptions and address what to look for when presented with a BAA.

When is a BAA needed?

A BAA is necessary when a physician practice (a 'covered entity' or CE under HIPAA) enters into a relationship with another business or individual (the "business associate, or BA) where the nature of the services provided by that business or individual *on behalf* of the CE requires or is likely to involve having access to the CE's protected health information (PHI).

If a contractor is hired to perform services where disclosure of PHI is not limited or incidental, the contractor is a BA, and a BAA is necessary. Examples of these types of services include those provided by billing companies, document storage and retrieval providers, and EHR services. In each case, the services provided involve the disclosure and use of PHI as part of the duties and not merely as an incidental byproduct of the services. The question is whether the services performed on behalf of the CE involve the use or disclosure of PHI in the performance of the contractor's duties.

Incidental access to PHI does not make someone a BA. For example, janitorial staff are not considered business associates. The types of potential disclosures of PHI that could arise from janitorial work (e.g., seeing PHI in trash cans or on desks) are incidental, occur as a byproduct of the janitorial duties, and could not be reasonably prevented. These disclosures are permitted under HIPAA.

A BAA is also not necessary when the service provider is under the CE's direct control, in which case they are considered "workforce" under HIPAA, and no BAA is necessary. For example, if a dermatologist had a staffing agency provide front desk staff, the front desk staff would be considered "workforce" under HIPAA because they would be under the direct control of the dermatology practice. On the other hand, if the staffing agency also provided billing services, and those

services were rendered off site at the staffing agency's own office, then a BAA would be required; not for the services of the front desk staff, but for the services of the off-site billers.

A covered entity may also function as a BA for another covered entity. Because a BAA is only necessary when the services are provided on behalf of a CE, this can lead to some confusion as to whether a CE is acting in its own capacity on its own behalf or is functioning as a BA which will require a BAA.

For example, if a dermatology practice refers certain pathology slides to a laboratory, where the pathology lab will analyze the slides and submit claims in its own name for the analysis, such an arrangement would not require a BAA. The disclosure here would be treated as a disclosure between two covered entities for the purpose of treatment and payment; no BAA is necessary. On the other hand, if the dermatology practice hired the pathology lab to perform interpretations for it and the dermatology practice then submitted a claim for the lab services in its own name, the lab would be a BA. In the first instance, the lab is acting on its own behalf. In the second instance, the lab is performing services on behalf of the dermatology practice.

Required BAA elements and what to look for

Most BAAs look very similar, although there are often differences in their details. In large part, this is because the Privacy Rule requires certain core elements in a BAA. If you are reviewing a BAA, you should make sure it contains these elements, or have a knowledgeable attorney review the document.

The BAA must describe the permitted and required uses and disclosures of PHI by the BA, and those uses and/or disclosures may not exceed what the CE itself is permitted to do. The BA may use and disclose PHI for its own management and administration or may perform data aggregation services relating to the health care operations of the covered entity. Data aggregation itself is where data (which may include PHI) is combined and analyzed to determine common patterns. These data can have both clinical and commercial value for CEs and BAs alike.

Note that a BAA may state that the BA may perform data aggregation services, but those services must be related to the health care operations of the CE, not solely for the BA's benefit. For example, if an EHR vendor performed data aggregation on the PHI entered into the EHR by physicians, it would need to

AADA Practice Management Center

For more resources and information on compliance and legal issues, visit **www.aad.org/member/practice**.

use that aggregated data for the CEs in some way (e.g., providing clinical decision-making tools that are developed from the aggregated data), rather than to simply use aggregated data for the vendor's own purposes (e.g., to sell to a pharmaceutical company).

The BAA must also specify that the BA will not use or further disclose the PHI other than as permitted under the BAA or as required by law. The BA must also use appropriate safeguards and comply with the Security Rule. It must report to the CE any uses or disclosure of information that the BA learns of, including breaches of unsecured PHI. This should be done as soon as possible, to permit the CE time to meet its own reporting requirements under HIPAA.

The BA must also require subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA to agree to the same restrictions as the BA itself. In essence, this means the BA will pass the terms of the BAA on to its subcontractors.

The BA must make PHI available upon request from a patient and must make amendments and incorporate any amendments made by the CE. It must also provide an accounting of disclosures of the PHI upon request, meaning that it must keep track of such disclosures and provide that information to a patient when the patient requests. These duties are all time-sensitive. Under the HIPAA regulations, these obligations must be performed between 30 and 60 days from the date of the patient's request, depending on the specific duty. As a result, most BAAs will involve shorter timeframes (e.g., 10-45 days) to allow the CE to meet its own requirements within the regulatory window. Be careful of the timeframes involved.

Other requirements include that a BA must make its internal practices, books, and records relating to use and disclosure of PHI available to the Secretary of Health and Human Services (or their designee), and that, upon termination, the BA must return and/or destroy all copies of PHI where feasible. If this is not feasible, then the BA must maintain the PHI until such time as it becomes feasible, under the terms of the BAA. In practice, this could mean that the BAA obligations will apply forever. For example, if the BA has incorporated PHI into a larger data set that merges the PHI of multiple CEs, it may not be able to remove individual pieces of PHI or destroy them.

Conclusion

The specific requirements and form of BAAs can be complex. While common elements are typical, determining whether and when a BAA is necessary, as well as whether the provisions of a BAA are adequate or required, can be daunting. Experienced health care counsel can help. **DW**

Academy HIPAA resources

Learn more about HIPAA requirements at **www.aad.org/member/practice/compliance/hipaa**.