Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

To BAA or Not to BAA: Must You Have One?

Insight — October 24, 2023

HIPAA applies to both covered entities (*e.g.*, healthcare providers and health plans) and their business associates. A "business associate" is generally a person or entity that "creates, receives, maintains or transmits" protected health information (PHI) in the course of performing services on behalf of the covered entity, *e.g.*, consultants; management, billing, coding, transcription or marketing companies; information technology contractors; data storage or document destruction companies; data transmission companies or vendors who routinely access PHI; third party administrators; personal health record vendors; lawyers; accountants; malpractice insurers; etc.).[1] "A covered entity may be a business associate of another covered entity" when it performs such functions on behalf of another covered entity.[2] Also, with very limited exceptions, a subcontractor or other entity that creates, receives, maintains or transmits PHI on behalf of a business associate is also a business associate.[3] To determine if an entity is a business associate, see our Business Associate Decision Tree.

Business Associate Requirements. In general, an entity that is a business associate under HIPAA must do the following:

1. Perform and document a security risk assessment of its information systems containing electronic PHI.[4]

2. Implement specified administrative, technical and physical safeguards as required by the HIPAA Security Rule to protect the integrity, confidentiality, and availability of electronic PHI (*e.g.*, establish access controls; use firewalls, virus protections, and encryption; backup data; implement appropriate security policies and procedures; *etc*.).[5]

3. Execute and perform according to written business associate agreements (BAAs) with covered entities that essentially require the business associate to maintain the privacy of PHI; limit the business associate's use or disclosure of PHI to those purposes authorized by the covered entity; and assist covered entities in responding to patient requests concerning their PHI.[6]

4. Report security incidents and privacy breaches to the covered entity.[7]

5. If the business associate uses subcontractors or other entities to provide any services for the covered entity involving PHI, execute BAAs with the subcontractors.[8]

Business associates who violate HIPAA may be subject to penalties of $127 to over $1,919,173 per violation.[9] If the violation resulted from willful neglect, the Office of Civil Rights (OCR) must impose a penalty of at least $12,794 per violation.[10] If the business associate acted with willful neglect and fails to correct the violation within thirty (30) days, the OCR must impose a penalty of at least $63,973 per violation.[11] A single breach may result in numerous violations. For example, the loss of a laptop containing hundreds of patients' PHI may constitute hundreds of violations. Similarly, each day that a covered entity or business associate fails to implement a required policy constitutes a separate violation.[12] In addition to regulatory penalties, business associates who fail to comply with BAAs may also be liable for contract damages and/or indemnification requirements set forth in the BAA.

Avoiding Business Associate Requirements. Given the cost of compliance and penalties for noncompliance, entities may want to avoid becoming a business associate or executing BAAs if possible. The following are not business associates and may properly decline to execute a BAA:

1. **Entities that do not create, receive, maintain, or transmit PHI.** If you want to avoid business associate obligations, the safest course is to ensure that you do not handle PHI on behalf of either a covered entity or a business associate of a covered entity. Accidental receipt of or incidental access to PHI outside your contracted job duties does not trigger business associate obligations. The OCR has stated:

> A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of [PHI], and where any access to [PHI] by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of [PHI], and any disclosure of [PHI] to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy

> Rule.[13]

Similarly, "[t]he mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the [PHI] of the covered entity."[14] Entities seeking to avoid business associate obligations may want to include a provision in their service contracts confirming that they do not require PHI to perform their functions, and that its clients who are covered entities or business associates will not provide PHI without the entity's prior agreement.

2. **Members of an entity's own workforce.** Members of an entity's own workforce are not business associates of the entity, including "employees, volunteers, trainees, and other persons whose conduct, in performance of work for a covered entity or business associate, is under the direct control of such entity or business associate, whether or not they are paid by the covered entity or business associate."[15] To avoid business associate obligations, contractors may seek to be classified as members of the covered entity's workforce. The OCR has stated:

> If a service is hired to do work for a covered entity where disclosure of [PHI] is not limited in nature (such as routine handling of records or shredding of documents containing [PHI]), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.[16]

Similarly,

> For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a BAA before allowing the software company access to [PHI]. However, when an employee of a contractor, like a software or information technology vendor, has

> his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity's workforce, rather than as a business associate.[17]

Although characterization as a workforce member would help contractors avoid business associate obligations, covered entities may resist classifying contractors as members of their workforce because doing so would likely make the covered entity vicariously liable for the contractor's actions.[18]

3. **Members of an organized health care arrangement.** Covered entities that participate in an organized health care arrangement (OHCA) are not business associates of each other while performing functions on behalf of the OHCA; thus, they "are permitted to share [PHI] for the joint health care activities of the OHCA without entering into business associate contracts with each other."[19] An OHCA is (1) "A clinically integrated care setting in which individuals typically receive health care from more than one health care provider" (*e.g.*, a hospital and its medical staff); (2) an organized system of health care in which more than one covered entity participates and in which the participating covered entities engage in joint utilization review, quality improvement, or payment activities (*e.g.*, provider networks); or (3) certain arrangements between group health plans and other insurers.[20] The OHCA exception only applies to covered entities (*e.g.*, healthcare providers and health plans) that perform functions for the OHCA; it does not apply to other entities that require PHI to perform functions on behalf of the OHCA.

4. **Healthcare providers who receive PHI to treat patients.** A healthcare provider is not a business associate of other covered entities while rendering treatment to patients.[21] As explained by the OCR:

> The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See 45 CFR 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share [PHI] with a health care provider for treatment purposes without a business associate contract.[22]

For example,

- A hospital is not required to have a business associate contract with the specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.
- A physician is not required to have a business associate contract with a laboratory as a condition of disclosing [PHI] for the treatment of an individual.
- A hospital laboratory is not required to have a business associate contract to disclose [PHI] to a reference laboratory for treatment of the individual.[23]

This exception only applies to the extent that the healthcare provider is using the PHI for treatment purposes; it would not apply if the healthcare provider is using the information to perform other functions on behalf of the covered entity. "For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to [PHI]."[24] Even in that example, however, the hospital and physician would not need a BAA if they were members of an OHCA.

5. **Entities acting on their own behalf or on behalf of the patient.** The business associate requirements only apply to entities who are performing a function involving PHI on behalf of a covered entity or its business associate. Entities that handle PHI for their own purposes are not business associates. For example, "[a] provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the 'business associate' of the other."[25] Similarly, a bank or financial institution is not a business associate of a covered entity when it "processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums"; in such cases, "the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity" and is not a business associate.[26] Researchers are not business associates of covered entities even if

the researcher is hired by the covered entity to conduct research.[27] "Where a physician or other provider has staff privileges at an institution, neither party to the relationship is a business associate based solely on the staff privileges because neither party is providing functions or activities on behalf of the other."[28] Covered entities that simply provide PHI for another covered entity's healthcare operations are not business associates of the other entity.[29] Finally, an entity performing services on behalf of the patient, not on behalf of the healthcare provider, is not a business associate (*e.g.*, an attorney who requests health information to represent the patient, or a company that collects and interprets data on behalf of a patient).

6. **Entities performing management or administrative functions for business associates.** Covered entities may allow business associates to use PHI for the business associate's own management and administration or legal responsibilities.[30] If so,

> [d]isclosures by a business associate … for its own management and administration or legal responsibilities do not create a business associate relationship with the recipient of the [PHI] because such disclosures are made outside of the entity's role as a business associate…. In contrast, disclosures of [PHI] by the business associate to a person who will assist the business associate in performing a function, activity, or service for a covered entity or another business associate may create a business associate relationship depending on the circumstances.[31]

However, even if no BAA is required because an entity is assisting the business associate in its own management or administration functions, HIPAA still restricts the use or disclosure of PHI by the entity:

> for [any] such disclosures that are not required by law, [HIPAA] requires that the business associate obtain reasonable assurances from the person to whom the [PHI] is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person notifies the business

> associate of any instances of which it is aware that the confidentiality of the information has been breached. See § 164.504(e)(4)(ii)(B).[32]

Such "reasonable assurances" may be obtained through a limited confidentiality agreement; a full-blown BAA is not required.

7. **Entities who are mere "conduits" for PHI.** Entities that transmit PHI for a covered entity are not business associates if they are not required to access the PHI on a routine basis, *i.e.*, they are merely "conduits" of the PHI (*e.g.*, internet service providers, phone companies, etc.).[33]

> Regarding what it means to have "access on a routine basis" to [PHI] with respect to determining which types of data transmission services are business associates versus mere conduits, such a determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to [PHI] to perform the service for the covered entity. The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to [PHI] when it reviews whether the data transmitted over its network is arriving at its intended destination. Such occasional, random access to [PHI] would not qualify the company as a business associate. In contrast, an entity that requires access to [PHI] in order to perform a service for a covered entity, such as a

> Health Information Organization that manages the exchange of [PHI] through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate.[34]

Avoiding Unnecessary BAAs. Unfortunately, out of ignorance or an abundance of caution, many covered entities or business associates are requesting BAAs even when such agreements are not technically required. Entities should avoid executing unnecessary BAAs; doing so may subject them to contractual liabilities they would not have but for the agreement, including the costs of complying with regulations that do not otherwise apply; limits on the use of disclosure of information; and damages for failure to comply. In addition, by executing unnecessary BAAs, the entity may be inappropriately admitting that it is a business associate, thereby exposing itself to HIPAA penalties for noncompliance. To avoid such situations, entities who are asked to execute unnecessary BAAs might consider responding as follows:

1. **Explain the limits on business associate obligations discussed above.** Hopefully, the covered entity will recognize that a BAA is not required and will be willing to forego the agreement.

2. **Explain the limits on the covered entity's liability.** Some covered entities or business associates insist on BAAs because they mistakenly assume that they are vicariously liable for the contractor's HIPAA violations. HIPAA clearly states that covered entities or business associates are only liable for their business associates' or subcontractors' actions if the business associate or subcontractor is acting as an agent of the covered entity, *i.e.*, that the covered entity had the right to control the business associate's or subcontractor's actions.[35] The parties may avoid vicarious liability by ensuring that any contract between them clearly identifies the business associate or subcontractor as an independent contractor, not an agent, and that the covered entity does not control the actions or operations of the business associate or contractor.[36] To that end, an overly restrictive BAA may actually work against the covered entity because it may suggest an agency relationship by giving the covered entity too much control over the actions of the contractor.

3. **Offer to execute an appropriate confidentiality agreement.** In lieu of a BAA, the business associate or subcontractor might offer to enter an appropriate confidentiality agreement that protects the covered entity while avoiding the full responsibilities or regulatory liabilities of a BAA.

4. **Condition the BAA.** Finally, if the covered entity still insists on a BAA, the business associate or subcontractor might minimize its exposure by conditioning a BAA on the entity's status as a business associate, *i.e.*, confirm that the entity undertakes the BAA responsibilities if and to the extent that it is a business associate as defined by HIPAA. Although an imperfect solution, it might at least allow the entity to avoid regulatory penalties if it truly is not a business associate.

Conclusion and Caution. Hopefully, the foregoing will allow entities which truly are not "business associates" under HIPAA avoid business associate status and associated liabilities. On the other hand, if an entity is truly a business associate under the regulations, it cannot escape regulatory liability by avoiding a BAA. "[A] person or an entity is a business associate if the person or entity meets the definition of 'business associate' even if a covered entity, or business associate with respect to a subcontractor, fails to enter into the required business associate contract with the person or entity."[37]

[1] 45 CFR § 160.103.

[2] *Id*.

[3] *Id*.; 78 FR 5572.

[4] 45 CFR § 164.308.

[5] 45 CFR § 164.300 *et seq.*

[6] 45 CFR §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e). Read more information about business associate requirements.

[7] 45 CFR § 164.314(a), 164.410, and 164.502(e).

[8] 45 CFR § 164.314(a) and 164.504(e). For more information about business associate obligations, see our article at https://www.hollandhart.com/checklist-for-business-associates.

[9] 45 CFR §§ 160.404 and 102.3. The penalties are subject to annual adjustment.

[10] *Id.*

[11] *Id*.

[12] 45 CFR § 160.406.

[13] OCR FAQ, available at https://www.hhs.gov/hipaa/for-professionals/faq/243/is-a-business-associate-contract-required-for-inadvertent-contact-with-phi/index.html.

[14] OCR FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/256/is-software-vendor-business-associate/index.html.

[15] 45 CFR § 160.103.

[16] OCR FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/243/is-a-business-associate-contract-required-for-inadvertent-contact-with-phi/index.html; *see also* 78 FR 5574.

[17] OCR FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/256/is-software-vendor-business-associate/index.html.

[18] *See* 45 CFR § 160.402(c); 78 FR 5581.

[19] OCR FAQ at https://www.hhs.gov/guidance/document/faq-242-are-covered-entities-engage-joint-activities-under-organized-health-care; *see also* 45 CFR 160.103).

[20] 45 CFR 160.103.

[21] *See* 45 CFR 160.103; *see also* 65 FR 82476 and 82504.

[22] OCR FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/240/do-i-need-a-business-associate-contract-to-disclose-information-to-a-provider/index.html.

[23] OCR Guidance at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[24] OCR FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/240/do-i-need-a-business-associate-contract-to-disclose-information-to-a-provider/index.html.

[25] OCR Guidance at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[26] *Id*.; 78 FR 5575; 65 FR 82476.

[27] 78 FR 5575.

[28] 65 FR 82476.

[29] *Id.*

[30] 45 CFR 164.504(e)(4).

[31] 78 FR 5574.

[32] 78 FR 5574.

[33] 45 CFR § 160.103; 78 FR 5571; 65 FR 82476.

[34] 78 FR 5571-72.

[35] 45 CFR 160.402(c); 78 FR 5581.

[36] 78 FR 5581.

[37] 78 FR 5574.
