A GUIDE TO IDENTIFYING BUSINESS ASSOCIATES AND UNDERSTANDING THEIR RESPONSIBILITIES UNDER HIPAA

Vandenack Weaver LLC

Attorneys at Law

A Business Associate is a person or entity that performs certain functions that involve the use or disclosure of protected health information (PHI). As defined in 45 CFR § 160.103, a business associate "creates, receives, maintains, or transmits" PHI in the course of performing services on behalf of the covered entity (i.e. data storage, document destruction companies, or vendors who routinely access PHI). Business associates can be from legal, actuarial, consulting, data aggregation, management, administrative, accreditation, and/or financial organizations. A non-exhaustive list of business associate functions include:

- Claims processing or administration
- Data analysis, processing, or administration
- Quality assurance
- Billing
- Benefit Management
- Repricing

How to Determine if You Are a Business Associate

An individual or entity is a business associate if

- ✓ an entity provides services to or on behalf of a covered entity
- ✓ an entity creates, receives, maintains, or transmits PHI in the course of providing services to or on behalf of the covered entity
- ✓ they are a subcontractor of business associates, if

    i) the business associate delegates to the subcontractor a function or service that the business associate has agreed to perform for the covered entity, or for another business associate, and

    ii) any of the delegated functions or services involve the creation, receipt, maintenance, or transmission of PHI

- ✓ a covered entity *may* be a business associate of another covered entity.

An entity is *not* a business associate if

- ✓ the entity is a healthcare provider who is receiving the PHI for purposes of treating the individual
- ✓ the individual is a member of the covered entity's workforce
- ✓ the individual is a researcher or a research sponsor of a covered entity for research purposes

Examples of When a Business Associate Agreement (BAA) is Needed

Scenario 1:

A medical practice stores old medical records in sealed containers in an off-sit location. Does the medical practice need a business associate agreement with the storage company?

Answer to Scenario 1:

Yes. Before the Omnibus Rule, the Office of Civil Rights (OCR) stipulated that a document storage company would not be considered a business associate if the PHI was maintained in a closed container and the document company did not access the PHI. However, after the Omnibus Rule, a medical practice that stores old medical records in an off-site location must enter into a business associate agreement with the storage company.

Scenario 2:

A large state-based public academic health center and research university that includes a hospital and two clinics in the state is storing credit card information, and patient information on a vendor's cloud-based server. The cloud-based vendor has provided the health center and research university with documentation of its security practices. Is this documentation sufficient or should the business associate (the cloud-based service provider) have a business associate agreement with the academic health center and research university?

Answer to Scenario 2:

The cloud-based vendor must enter into a BAA with the academic health and research university. The OCR has stipulated that covered entities and business must enter into a business associate agreement if electronic protected health information (ePHI) is being used on the cloud service provider. If the cloud service provider does not know that a covered entity is using the cloud service to store ePHI it may not be obligated to satisfy the HIPAA rules. However, once they become aware, the cloud service provider must comply with the HIPAA rules and enter into a business associate agreement or securely return the ePHI, or destroy it, if both parties agree.

Scenario 3:

Business associate V engages subcontractor W to perform part of business associate V's responsibilities involving the covered entity's PHI. Then, subcontractor W delegates some of her responsibilities involving the PHI to subcontractor S. Do the business associate obligations that clearly apply to V with respect to the covered entity equally apply to W? What about S?

Answer to Scenario 3:

Subcontractors W and S, as well as business associate V, would all qualify as business associates of the covered entity and the HIPAA business associate obligations would trickle down from W, to V, to S. Thus, business associate agreement would be required between:

1) The covered entity and business associate V
2) Business associate V and subcontractor W
3) Subcontractor W and subcontractor S

Responsibilities of a Business Associate

First, business associates of HIPAA covered entities must sign a BAA with the covered entity that states the responsibilities of the business associate. The BAA is a contract that outlines the types of PHI that will be provided to the business associate and the procedures which the business associate must abide by in using and disclosing the PHI. Even if there is no signed BAA between a covered entity and a business associate, the latter is still subject to the business

associate obligations under the HIPAA Rules. The general rule is that a business associate may not use the PHI for its own purposes without the patient's authorization. HIPAA underscores two exceptions when the business associate may use the PHI for its own purposes, without the patient's authorization. Pursuant to 45 C.F.R. § 164.502(e) (4); and (2), the agreement *may* permit the business associate to:

A. use and disclose PHI for the proper management and administration of the business associate, and

B. provide data aggregation services relating to the health care operations of the covered entity.

If a business associate fails to comply with HIPAA Rules, it is the responsibility of the covered entity to take action to ensure the business associate comes into compliance and, if not, that the contract is terminated. However, business associates can still be fined directly for HIPAA violations under the authority of the Department of Health and Human Services' Office for Civil Rights and the state attorneys general.

After the BAA is formalized between a covered entity and a business associate, the Privacy Rules also mandates that a covered entity receive satisfactory assurances from its business associates that the business associate is appropriately enforcing the safeguards that were outlined in the BAA. Even if a vendor is not given PHI to perform tasks for a covered entity, if ePHI passes through a vendor's system (i.e. a software provider), that vendor is still classified as a business associate. And encrypting ePHI that is stored or transmitted, while necessary, is insufficient as a safeguard. The HIPAA Privacy Rule requires physical safeguards and administrative safeguards be put in place for protecting all types of PHI including paper, electronic, and oral

In 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act. This Act makes business associates of a covered entity directly liable for compliance with certain requirements of the HIPAA Rules. Those requirements are as follows:

1) Failure to provide the Secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary to information, including PHI, pertinent to determining compliance.
2) Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules.
3) Failure to comply with the requirements of the Security Rule.
4) Failure to provide breach notification to a covered entity or another business associate.
5) Impermissible uses of disclosures of PHI.
6) Failure to disclose a copy of ePHI to either the covered entity, the individual, or the individual's designee (whichever is stipulated in the BAA) to satisfy a covered entity's obligations regarding the form and format, and the time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii).
7) Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
8) Failure, in certain circumstances, to provide an accounting of disclosure.

9) Failure to enter into a business associate agreement with a subcontractor(s) that creates or receives PHI on their behalf, and failure to comply with the implementation specification for such agreements.

10) Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement under 45 C.F.R. § 164.504(e)(1)(iii).

However, a business associate is not always held to the same expectation and liability as a covered entity. For example, if there is a BAA that states the business associate will furnish an individual with a copy of their ePHI upon the individual's request, and if the business associate fails to do so, the OCR lacks enforcement authority directly over the business associate's failure. Additionally, pursuant to 45 C.F.R. § 164.524(c)(4), the OCR has the power to make sure a covered entity charges a "reasonable, cost-based fee" to an individual who requests a copy of their PHI. If a BAA stipulates that a business associate has the role of fulfilling an individual's request for a copy of their PHI and the business associate charge a fee that exceeds the "reasonable" limitation, the OCR can only take enforcement action against the covered entity, and not the business associate. This is because the HITECH Act only applies the fee-based limitation provision to covered entities.

Conclusion

Covered entities should identify all their business associate relationships so they can take necessary actions to comply with the HIPAA Rules. In some cases, it will be apparent that a relationship exists between a covered entity and its respective business associates. In other instances, however, further analysis will be required to determine if, given the particular circumstances, a covered entity has a business associate relationship with an individual or entity. Moreover, because of the intricacies of HIPAA, it is important to have a lawyer make sure your business associate agreement has been drafted properly.