COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Patient Privacy and Security: Business Associates

By Isabella A. Porter,[1] JD, CHC, CHPC

What Are Business Associates in Relation to Patient Privacy and Security?

When the Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, the world of healthcare operations vis-à-vis technology differed vastly from today. How healthcare entities functioned shifted between then and 2009, when the Health Information Technology for Economic and Clinical Health Act (HITECH) was passed by Congress within the omnibus American Recovery and Reinvestment Act (ARRA). The healthcare industry was eager to acquire technology and to contract for services that would facilitate patient care, support efficient healthcare operations, enhance organizations' ability to collect revenue, and minimize their risks.

Advances in technologies during the last 10 years have changed the healthcare industry with such developments as moving from web applications to mobile apps, handling data analytics and data increasingly through cloud-based services, and the rise of telework opportunities (especially in the context of COVID-19). The advances also have posed challenges—managing cyber risk, vendor risk, and various other threats. Healthcare providers often contract with entities to perform or outsource certain functions related to treatment, payment, and operations if the covered entities lack the necessary internal capabilities or skill sets, or need assistance with activities that are out of scope of the healthcare entity's normal business. If these functions involve individual health information of patients, which is often the case, contractors or vendors engaged to perform such functions on behalf of the healthcare organization are known as **business associates**.

Business Associates and Their Roles

Business associates are individuals or entities that perform services on behalf of covered entities involving the use or disclosure of the covered entity's protected health information (PHI) and electronic PHI (ePHI). Business associates are vendors or contractors that are not directly involved in the treatment of a covered entity's patients or members. For instance, their services include such functions as claims processing or administration, quality assurance, billing, practice management, legal, and accounting.[2] A legal definition of "business associate" can be found in 45 C.F.R. § 160.103.[3]

Common examples of business associates include:

- Certified public accountants (CPAs)
- Attorneys
- Consultants
- Auditors
- Coding companies

- Third-party administrators (TRAs) performing billing
- Security consultants
- IT support contractors
- Data aggregation services (such as population health and de-identification)
- Transcription services
- Contracted ambulance companies
- Electronic health record (EHR) vendors that support their applications/tools and can view PHI

Owing to the sensitive nature of information that business associates need to perform their contracted services, covered entities are required to obtain satisfactory assurances that business associates will protect the privacy and security of the PHI they access, use, and disclose. These assurances are codified in a business associate agreement that essentially supports the PHI chain of trust for PHI that a business associate receives from a covered entity. Lastly, depending on the services provided, one covered entity can be considered a business associate of another covered entity, and so can subcontractors that are creating, receiving, maintaining, or transmitting PHI on behalf of a business associate may also be considered a business associate.[4][5][6]

Business Associates After HITECH

Before HITECH was enacted, healthcare providers were required to obtain satisfactory assurances that business associates would protect PHI before contracting and sharing PHI with them. Providers, however, soon learned that contracting for services and technology from business associates carried its own set of risks. Namely, the HIPAA security standards and penalties applicable to healthcare providers did not apply to contracted business associates accessing PHI to perform services on their behalf.[7] In fact, prior to HITECH, a business associate could be held liable for a HIPAA breach by a covered entity only under a breach of contract claim.[8] HITECH made business associates directly responsible for HIPAA compliance within their individual businesses that would not otherwise be subject to HIPAA regulations and penalties.[9]

Even if no written contract exists between the covered entity and a contracted company performing services related to handling PHI in some form, the company is deemed a business associate by law. This deemed status essentially classifies contracted vendors or individuals as business associates solely by the nature of the services they provide to a covered entity, regardless of whether they intended to be classified as business associates or were aware of their status as such. HIPAA and HITECH may hold these vendors to business associate obligations as long as they *act* as business associates.

To protect healthcare entities and their patients, a robust compliance program is essential for monitoring business-associate relationships and contracts.

Risk Area Governance

In the context of business associates, HIPAA, HITECH, and the Omnibus Final Rule all work in concert to expand statutory requirements surrounding privacy and security protections of PHI to include vendors indirectly involved in the treatment of patients. While HITECH enhanced HIPAA by extending its Privacy and Security Rules' penalties to contracted business associates and their subcontractors accessing a covered entities' PHI, the Omnibus Final Rule added direct liability to noncompliant business associates, which includes imposing fines by

the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR). Additionally, 45 C.F.R. § 160 and Subparts A and C of 45 C.F.R. § 164 detail the HIPAA Security Rule. These sections explain the basic standards required by statute to protect ePHI by covered entities and their business associates. Further, they require both to incorporate appropriate physical, administrative, and technical safeguards to protect the confidentiality, integrity, and security of ePHI.[10][11]

The HIPAA Privacy Rule only applies to covered entities that are defined as health plans, healthcare clearinghouses, and healthcare providers "who transmit any health information in electronic form in connection with a transaction for which the HHS has adopted a standard."[12][13] Business associates are defined as "person[s] or entit[ies] that [perform] certain functions or activities . . . involv[ing] the use or disclosure of [PHI] on behalf of, or [provide] services to, a covered entity."[14]

The HIPAA Privacy Rule permits covered entities to disclose PHI to business associates if they "obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule."[15] These satisfactory assurances are met through the explicit prerequisite that a covered entity obtain a business associate agreement "or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the [HIPAA] Rules' requirements to protect the privacy and security of [PHI]," and "[i]n addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules."[16][17] On the condition that a covered entity has obtained a valid and appropriate business associate agreement, "[c]overed entities may disclose [PHI] to an entity in its role as a business associate only to help the covered entity carry out its health care functions—not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate."[18] Conversely, if a covered entity only plans to disclose a limited data set to the business associate, as specified in 45 C.F.R. § 164.514(e)(2) and 45 C.F.R. § 164.514 (e)(3), then a business associate agreement is not required and a data use agreement may be obtained in its place.[19]

Under HIPAA and HITECH, individuals or entities who have been identified as business associates are obligated to enter into a business associate agreement with their contracted covered entities. At a minimum, the business associate agreement must do the following:

1. Address permitted and required uses and disclosures of PHI by the business associate.
2. Restrict business associate from disclosing PHI in a manner not permitted or required under the agreement or as required by law.
3. Require appropriate safeguards be implemented by the business associate to prevent unauthorized use or disclosure of PHI, which would include HIPAA Security Rule provisions concerning ePHI.
4. Require business associates to report any use or disclosure of PHI to the covered entity that is inconsistent with the permitted uses and disclosures allowed for by the agreement (e.g., breaches of unsecured PHI). At this time, there is no statutory timeframe specifying what is a reasonable turnaround for a business associate to notify a covered entity, so it is crucial for covered entities to consider a timeframe that would allow it to comply with the totality of its breach notification obligations under the law. This task can be extremely constricted if it concerns a breach of PHI of more than 500 patients and patients from different states with separate breach reporting mandates.
5. Require business associates to disclose PHI in order to fulfill a covered entity's patient request for copies of

their information, amendments to their information, and/or accounting of disclosures.

6. Require the business associate to comply with the applicable obligation(s) in the event that the business associate is to fulfill a covered entity's obligation as specified under the Privacy Rule.
7. Require the business associate to make available to HHS its internal practices, books, and records related to the use and disclosure of the covered entity's PHI for HHS to determine the covered entity's compliance with the HIPAA Privacy Rule.
8. Require business associates to return or destroy all PHI received from the covered entity at the termination of the agreement, if feasible. If a covered entity does opt for the destruction option, they should consider requesting a certificate of destruction upon completion. If not feasible, then covered entities should ensure that the agreement contains language extending the protections of the agreement to the PHI *beyond* its termination.
9. Require business associates to impose on their subcontractors the same restrictions from their agreement on accessing PHI, so as to ensure that the information will be consistently protected at the same level of care from covered entity to business associate to its subcontractor. It should be noted that per the OCR, "contracts between business associates and business associates that are subcontractors are subject to these same [overall business associate agreement] requirements."[20]
10. Authorize termination of the agreement by the covered entity should the business associate commit a material breach of contract or violate an essential term of the agreement. Some business associate agreements will indicate a cure period prior to termination for a material breach of this agreement (such as 30 days to cure an identified material breach); covered entities should consider whether there would be instances when a cure would be inconceivable, thus immediate or expedited termination of an agreement would be preferred.[21]

In addition, while it is important to recognize when a relationship with an individual or entity triggers the business associate agreement mandate under the HIPAA Privacy Rule, it is equally important to be cognizant of its exceptions. For instance, according to HHS, "a covered entity is not required to have a business associate [agreement] or other written agreement in place before [PHI] may be disclosed to the person or entity" for the following situations:

- Disclosures of an individual's PHI by a covered entity to another healthcare provider for the purposes of treating that individual.
- When appropriate, disclosures by a group health plan (or similarly situated insurers) to a health plan sponsor.
- When appropriate, the gathering and transmission of PHI by a public benefits program health plan and the agencies that assist with determining eligibility and enrollment.
- Disclosures made for payment purposes by a healthcare provider to a health plan.
- Relationships with individuals or entities providing services to the covered entity that do not involve the use or disclosure of PHI, but the services are being performed in or around the covered entity's physical location (e.g., building maintenance). *Note: In these situations, while a business associate agreement would not be necessary, it is still advisable for covered entities to execute confidentiality agreements with these individuals/entities and perform routine vendor screening and due diligence on them.*]

- When individuals or entities act solely as conduits of PHI (e.g., the U.S. Postal Service delivering letters containing PHI).
- When appropriate, disclosures by covered entities participating in an organized healthcare arrangement (OHCA).
- Disclosures made to a health insurer by a group plan purchasing insurance.
- Disclosures made to an insurer through the purchase of a health plan product or other insurance by a covered entity.
- When appropriate and as provided for under HIPAA, disclosures made to a researcher solely for research purposes.[22][23]
- Disclosures made by a financial institution pursuant to any activity directly affecting or assisting with the application of funds for payment for healthcare or health plan premiums.[24]

In sum, it behooves covered entities to be familiar with the circumstances that either require or exempt an individual or entity from executing a business associate agreement.