



Vendor Business Associate Agreements

Are Your Service Providers Business Associates Under HIPAA? Business Associates – The Basics

What is a HIPAA Business Associate?

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 (“PHI”). A Business Associate is also a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another Business Associate (“Subcontractor”).

What is Protected Health Information?

PHI is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as a diagnosis or treatment.

NOTE: Health-related information that is personally identifiable because it includes personal identifiers such as name or address, may not be considered PHI if the data is not associated with or derived from a health care service event (treatment, payment, operations, medical records) and the data is not entered into the medical records.

HIPAA Business Associate Agreements

A business associate agreement (“BAA”) establishes a legally binding relationship between HIPAA-Covered Entities and Business Associates to ensure complete protection of PHI. **If a Business Associate can potentially access PHI during their work for the Covered Entity, then a BAA is necessary.**

When is a BAA Subcontractor Agreement Required?

A BAA Subcontractor Agreement or “Downstream BAA” is required when a Business Associate contracts services to a Subcontractor who will use, have access to, or transmit PHI from the Covered Entity. In these circumstances, a BAA is required between the Covered Entity and the Subcontractor or between the Business Associate and the Subcontractor. The provisions of these agreements must reflect the same terms, conditions, and protections for the Covered Entity as those contained in the original BAA.

Customizing the BAA to Suit Your Needs

Other protective provisions and contractual terms may be added to the BAA beyond the terms required by the Privacy and Security Rules, such as cyber insurance requirements, indemnification or payment for losses associated with a breach and **delineation of roles in the event of a data breach. Often BAA’s and Subcontractor agreements require revisions and configurations to meet the specific needs of a particular Covered Entity or Business Associate.**

Common Examples of Business Associates:

- 1 An electronic medical record vendor (for maintenance of the software).
- 2 A billing or collection company.
- 3 A patient portal vendor.
- 4 A third party administrator that assists a health plan with claims processing.
- 5 An accounting firm if their accounting services to a health care provider involve access to PHI.
- 6 An attorney whose legal services to a health plan involve access to PHI.
- 7 A consultant that performs utilization reviews for a hospital.
- 8 A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- 9 An independent medical transcriptionist that provides transcription services to a physician.
- 10 A pharmacy benefits manager that manages a health plan's pharmacist network.

Common Examples of Non-Business Associates:

Postal and
FedEx
personnel

Landlords

Members of
the Covered
Entity's
workforce

Pathology and
reference labs
(Considered
Covered Entities)

Physician
referrals

Checklist for HIPAA Business Associate Agreements

Required items under the HIPAA Rules

- ☐ Describe the permitted and required uses and disclosures of PHI by the Business Associate;
- ☐ Provide that the Business Associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
- ☐ Require the Business Associate to use appropriate safeguards to prevent unauthorized use or disclosure of PHI other than as provided for by the contract and law;
- ☐ Require the Business Associate to report to the Covered Entity any use or disclosure of the PHI not provided for by its contract, including incidents that constitute breaches of unsecured PHI;
- ☐ Require Business Associate to disclose PHI as specified in its contract to satisfy a Covered Entity's obligation with individuals' right to request copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings;
- ☐ Require the Business Associate to comply with the requirements applicable to the obligation, to the extent the Business Associate is to carry out a Covered Entity's obligation under the Privacy Rule;
- ☐ Require the Business Associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity for purposes of HHS determining the Covered Entity's compliance with the HIPAA Privacy Rule;
- ☐ Require the Business Associate to return or destroy all PHI received from, or created or received by the Business Associate on behalf of the Covered Entity, if feasible, at the termination of the agreement;
- ☐ Require the Business Associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the Business Associate; and
- ☐ Authorize termination of the BAA by the Covered Entity if the Business Associate violates a material term of the contract.

The Day Pitney Team

Questions about HIPAA compliance or think you may need a Business Associate Agreement?
Contact our team.



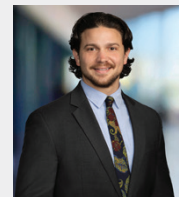
William J. Roberts
Hartford, CT
wroberts@daypitney.com



Magda C. Rodriguez
Miami, FL
mdrodriguez@daypitney.com



Mindy S. Tompkins
Hartford, CT
mtompkins@daypitney.com



Damian J. Privitera
Hartford, CT
dprivitera@daypitney.com



Stephanie M. Gomes-Ganhão
Hartford, CT
sgomesganhao@daypitney.com



Colton J. Kopcik
Washington, DC
ckopcik@daypitney.com



Phoebe A. Roth
Hartford, CT
proth@daypitney.com