# Business Associates

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information (PHI) to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will:

- Use the information only for the purposes for which it was engaged by the covered entity;
- Safeguard the information from misuse; and
- Help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Covered 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.

## How the Rule Works

### General Rule

The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

### What Is a "Business Associate"?

A "business associate" is generally a person or entity that performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of PHI. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The following persons and entities are also considered "business associates" under the final omnibus rule:

- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate;
- Health Information Organizations, e-prescribing gateways, or other persons that provide data transmission services with respect to PHI to a covered entity and that require access on a routine basis to such PHI;
- Persons who offer a personal health record to one or more individuals on behalf of a covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of PHI. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; and patient safety activities. Business associate services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

## Examples of Business Associates

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to PHI.
- An attorney whose legal services to a health plan involve access to PHI.
- A consultant that performs utilization reviews for a hospital.
- 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.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.
- A shredding company hired by a third party administrator to handle document and media shredding to securely dispose of paper and electronic PHI.

## Business Associate Contracts

A covered entity's contract or other written arrangement with its business associate must contain certain elements specified by law. For the convenience of health plans and other covered entities, the U.S. Department of Health and Human Services has created a Sample Business Associate Contract. Among other requirements, the contract must:

- Describe the permitted and required uses 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; and
- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.

## Liability of a Business Associate under HIPAA

According to a U.S. Department of Health and Human Services (HHS) fact sheet, the HHS Office of Civil Rights has authority to take enforcement action against business associates for the following HIPAA violations:

1. Failure to provide HHS with records and compliance reports, cooperate with complaint investigations and compliance reviews, and permit access by HHS to information, including PHI.
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 and disclosures of PHI.
6. Failure to disclose a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement).
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 disclosures.
9. Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.
10. Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.

## Obligation to Cure Breaches of a Business Associate

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the HHS Office for Civil Rights (OCR).

## Additional Information

- Sample Business Associate Contract
- HIPAA Privacy Rule
- HIPAA Security Rule