

Business Associates [45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)]

Background

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, clearinghouses, and particular providers. However, most healthcare providers and health plans do not carry out all their healthcare activities and functions alone. Instead, they often use the services of various other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information 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 the covered entity engaged it, 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. Covered entities may disclose protected health information 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 Provision. The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in a contract or other agreement between the covered entity and the business associate.

What Is a “Business Associate?”

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity.

- A member of the covered entity’s workforce is not a business associate.
- A covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity.

The Privacy Rule lists some of the functions or activities and the particular services that make a person or entity a business associate if the activity or service involves using or disclosing protected health information.

The functions or activities that may make a person or entity a business associate include payment or health care operations activities and 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; and re-pricing.
- *Business associate services include* legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

See the definition of “business associate” at 45 CFR 160.103.

Business Associate Contracts: A covered entity’s contract or other written arrangement with its business associate must contain the elements specified in 45 CFR 164.504(e). For example, the contract must:

- Describe the permitted and required uses of protected health information by the business associate; 2 OCR HIPAA Privacy December 3, 2002 Revised April 3, 2003
- Provide that the business associate will not use or further disclose the protected health information 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 the use or disclosure of protected health information other than as provided for by the contract.

Healthcare Facility Name & Address Below:

CEO / Administrator Signature

First and Last Name & Date

Raquel Martinez Signature, Date
Business Associate