HIPAA Compliance for Business Associates

Businesses that have access to protected health information (PHI) on behalf of a covered entity (for example, an employer's group health plan) typically qualify as "business associates" under the HIPAA Privacy, Security and Breach Notification Rules (HIPAA Rules).

If a covered entity uses a business associate, it must have a **written business associate agreement** with the business associate that requires the business associate to protect the privacy and security of PHI. In addition to these contractual obligations, business associates are directly liable for compliance with many of the HIPAA Rules' requirements. For example, among other compliance steps, business associates must:

- Enter into business associate agreements with any subcontractors who create or receive PHI on their behalf;
- Implement reasonable and appropriate safeguards for protecting electronic PHI (ePHI); and
- Not use or disclose PHI, except as permitted by the Privacy Rule and business associate agreements.

LINKS AND RESOURCES

- HHS' FAQs for Business Associates
- HIPAA Rules – Privacy Rule, Security Rule and Breach Notification Rule
- Compliance & Enforcement

Business Associates

The HIPAA Rules apply to covered entities, which include health plans, health care clearinghouses and most health care providers. The HIPAA Rules also apply to other entities that perform functions or activities on behalf of a covered entity **when those services involve access to, or the use or disclosure of, PHI**. These entities are called business associates.

In general, a business associate means a third party that:

- Creates, receives, maintains or transmits PHI on behalf of the covered entity for a HIPAA-regulated activity or function, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management and repricing; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for the covered entity where the provision of the service involves the disclosure of PHI from the covered entity (or from another business associate of the covered entity) to the service provider.

Examples of business associates for employer-sponsored group health plans include:

- Third party administrators (TPAs) that assist health plans with claims processing.
- An attorney whose legal services to a health plan involve access to PHI.
- Insurance brokers that serve as health plan consultants and receive PHI.
- Pharmacy benefits managers (PBMs) that manage health plans' pharmacist networks.

What Is PHI?

PHI is individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity (or a business associate) and relates to the past, present or future physical or mental health condition of an identified individual. Examples of PHI may include health plan claims and appeals, claims data, provider bills and explanations of benefits (EOBs).

Business Associate Agreements

The HIPAA Rules allow a covered entity to share PHI with a business associate if the covered entity receives satisfactory assurances from the business associate—through a business associate agreement—that it will appropriately handle and safeguard PHI. A business associate may use or disclose PHI only as permitted or required by its business associate agreement or as required by law. In general, a business associate is prohibited from using or disclosing PHI in a manner that would violate the HIPAA Privacy Rule if done by the covered entity.

Required Provisions

The business associate agreement must e**stablish the permitted and required uses and disclosures of PHI** by the business associate. The business associate agreement must also require the business associate to:

- Not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards to prevent improper use or disclosure of the PHI;
- Report to the covered entity any known use or disclosure of PHI not permitted by the contract or any breach of unsecured PHI;
- Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions that apply to the business associate;
- Make PHI available, including for amendment, to individuals as required by the HIPAA Rules;
- Maintain an accounting of disclosures, made during the last six years, and make the accounting available upon request; and
- Make its internal practices, books and records relating to use and disclosure of PHI available to HHS.

The business associate contract must also allow the covered entity to terminate the contract in the event of a material breach. At termination, the business associate must be required to destroy or return all PHI, if feasible, or extend the limitations on use and disclosure beyond termination of the contract.

Subcontractors

If a business associate delegates any of its functions to a subcontractor that creates, receives, maintains or transmits PHI on its behalf, the business associate must **enter into a written business associate agreement with the subcontractor**. This agreement must ensure that the subcontractor will agree to comply with the same restrictions and conditions that apply to the business associate with respect to PHI.

HIPAA Liability

HHS' Office for Civil Rights (OCR) has authority to take enforcement action against business associates for certain HIPAA violations. OCR released a fact sheet clarifying that business associates are directly liable for the following HIPAA violations:

- Failing to comply with the requirements of the Security Rule;
- Impermissible uses and disclosures of PHI;
- Failing to provide breach notification to a covered entity (or another business associate);
- Failing to enter into business associate agreements with subcontractors that create or receive PHI on the business associate's behalf, and failure to comply with the implementation requirements for those agreements;
- Failing to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement;
- Failing to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request;
- Failing, in certain circumstances, to provide an accounting of PHI disclosures;
- Failing to provide access to PHI, as required by 45 C.F.R. §§ 164.524.
- 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; and
- Failing to provide HHS with records and compliance reports, cooperate with complaint investigations and compliance reviews, and permit access by HHS to information, including PHI, relevant to determining compliance.

HIPAA Enforcement

OCR has steadily increased its enforcement of the HIPAA Rules, with some costly settlements for covered entities and business associates. For instance, OCR recently entered into a $100,000 settlement agreement with a business associate after hackers accessed the ePHI of approximately 3.5 million people. OCR found that the business associate, a company that provides software and electronic medical record services to healthcare providers, violated the Security Rule by failing to perform an adequate risk analysis prior to the security breach.
