HIPAA Business Associate Agreements - What Are They and When Are They Required?

Julie L. Hamlet and Ray H. Littleton
Foster Swift Health Care Law News E-blast
July 29, 2020

For individuals and organizations involved in healthcare industry related occupations, here is a brief informational article written by Julie L. Hamlet and Ray H. Littleton from our heath care law group on Business Associate Agreements and the need to consult with your attorney for review in order to avoid consequences. The failure to enter into HIPAA-compliant business associate agreements when required can result in steep penalties against both covered entities and business associates.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that covered entities must enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information ("PHI"). Business associates who hire contractors to perform certain functions involving PHI must also enter into subcontractor business associate agreements with their subcontractors. This article provides an overview of the rules regarding business associate agreements.

A. What is a Business Associate?

In order to understand the HIPAA definition of a business associate, it is helpful to first understand the definition of a HIPAA "covered entity." A "covered entity" is defined under HIPAA to include health plans, health care clearinghouses, and certain health care providers who transmit health information electronically in connection with certain HIPAA-covered transactions (such as claim submission).

A "business associate" is a person or entity (other than a member of the workforce of a covered entity) who performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to PHI. A "business associate" also includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate. Business associate functions and activities include: claims processing or

AUTHORS/ CONTRIBUTORS
Julie LaVille Hamlet
Ray H. Littleton

PRACTICE AREAS
Business Law
Health Care
HIPAA Privacy & Security Compliance

administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services can include: legal; actuarial; accounting; consulting; data aggregation; management; medical transportation, administrative; accreditation; and financial.

B. When is a Business Associate Agreement Required?

HIPAA requires that a covered entity must enter into a HIPAA-compliant business associate agreement with all of its business associates. Additionally, all business associates must enter into HIPAA-compliant subcontractor business associate agreements with any subcontractors who perform certain functions and will have access to the covered entity's PHI.

Therefore, any time a covered entity or business associate is contracting with another party to provide services that may involve the exchange of PHI, the parties should analyze the arrangement carefully to determine whether a business associate agreement is required.

C. What provisions must be included in a business associate agreement?

In order to comply with HIPAA, a business associate agreement must include a description of the permitted and required uses and disclosures of PHI by the business associate. The business associate agreement must also require, among other things, that the business associate:

1. not use or further disclose the information other than as permitted or required by the contract or as required by law;
2. implement appropriate safeguards to prevent the unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI;
3. report to the covered entity any use or disclosure of PHI not permitted by the business associate agreement, including incidents that constitute breaches of unsecured PHI;
4. disclose PHI as specified in its contract to satisfy a covered entity’s obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings;
5. to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, comply with the requirements applicable to the obligation;
6. make available to the U.S. Department of Health and Human Services ("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;
7. return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity at termination of the contract, if feasible; and
8. 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 with respect to such information.

In addition to the HIPAA-required provisions, a party may want to include additional protections. For example, a covered entity may want to include an indemnification provision to protect itself in the event that a business associate experiences a security breach involving the covered entity's PHI.

D. Takeaway

Both covered entities and business associates may be subject to penalties for failing to enter into a business associate agreement when required, and the penalties can be steep. For example, a physicians' group in Florida paid a $500,000 penalty when it failed to enter into a business associate agreement with its billing company. After the billing company improperly posted PHI on its website, the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services penalized the group for failing to take the proper steps to secure the PHI, including its failure to enter into a business associate agreement with the billing company.

Covered entities and business associates should also review the terms of their agreement to ensure that each is complying with statutory and administrative rules as well as the provisions of the contract itself. Companies need to make sure that they have taken steps to implement procedures and policies to comply with the necessary protections for PHI as well as obtain the agreed upon amounts of insurance coverage and required insurance policies as provided in the agreement.

Covered entities and business associates should review any arrangements that involve the exchange of PHI to ensure that business associate agreements are in place if required. Additionally, covered entities and business associates should carefully review any business associate agreements going forward to ensure that each agreement includes all of the HIPAA-required elements and adequately protects the applicable party. Finally, covered entities and business associates should ensure that they have adopted appropriate HIPAA policies and procedures to address the business associate agreement requirements.

If you have any questions regarding the HIPAA requirements that apply to a business associate, or if you'd like our assistance with drafting or reviewing a business associate agreement, please feel free to contact us. Our contact information is below.

Julie L. Hamlet
Phone: 616.796.2515
Email: jhamlet@fosterswift.com

Ray H. Littleton
Phone: 248.539.9903
Email: rlittleton@fosterswift.com