COSMOS
Navigate the Compliance Universe

Compliance Today - March 2022
Business associates and their agreements: Almost twenty years later, and we're still messing this up

By Barry S. Herrin, JD, FAHIMA, FHIMSS, FACHE


Barry S. Herrin

Barry S. Herrin (barry.herrin@herrinhealthlaw.com) is Founder, Herrin Health Law PC in Atlanta, Georgia.

In 2003, the federal regulatory bureaucracy, acting in response to the mandate of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), created a special relationship between certain healthcare providers and certain of their vendors and contractors. This relationship relied on the vendor performing "certain functions or activities that involve the use or disclosure of protected health information [PHI] on behalf of, or provides services to, a covered entity."[1] This new, special kind of vendor was referred to as a business associate. And, as with any increase in the regulatory footprint, it was not sufficient that a healthcare provider covered by HIPAA (i.e., a covered entity) merely have a written contract with such a vendor; rather, the contract had to meet the requirements of the HIPAA regulations and qualify as a business associate agreement (BAA).

The regulatory requirements for BAAs are fairly onerous. To begin with—and these are nonnegotiable—the agreement must:

- Establish 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 information other than as permitted or required by the contract or as required by law;
- Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI;
- Require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI;
- Require the business associate to 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;
- To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation;
- Require the business associate to make available to the Department of Health & 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;
- At termination of the contract, if feasible, 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;

- 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 with respect to such information; and
- Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract.[2]

With the expansion of the HIPAA regulations in September 2013, the federal regulators now can hold business associates directly liable for certain violations of HIPAA and its regulations. These include:

- Failure to provide the HHS secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the secretary to information, including PHI, pertinent to determining compliance.[3]
- Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in a retaliatory investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA regulations.[4]
- Failure to comply with the requirements of the HIPAA Security Rule (which includes the requirement for the business associate to conduct a security risk analysis as required of covered entities in 45 C.F.R. § 164.308(a)(1)(ii)(A) .[5]
- Failure to provide breach notification to a covered entity or another business associate as required by the HIPAA Breach Notification Rule.[6]
- Impermissible uses and disclosures of PHI.[7]
- 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) to satisfy a covered entity's obligations regarding the form and format and the time and manner of access.[8]
- Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[9]
- Failure, in certain circumstances involving the business associate's maintenance of a "designated record set,"[10] to provide an accounting of disclosures.[11]
- 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.[12] Among other things, business associate subcontractor agreements must require the subcontractor to adopt the same or more restrictive policies than the business associate has or meet the same or a higher compliance burden than the business associate must meet in its relationship with the covered entity.
- Failure to take reasonable steps to address a material breach or violation of a subcontractor's BAA.[13]