Checklist for HIPAA Business Associate Agreements

Under the HIPAA Privacy and Security Rules, BAAs generally must contain the following terms.[6] To the extent the business associate enters a BAA with its subcontractors, those subcontract BAAs should also contain equivalent terms.[7]

1. Establish the permitted and required uses and disclosures of PHI by the business associate.[8] The BAA may not authorize the business associate to use or further disclose the PHI in a manner that would violate the Privacy Rule if done by the covered entity, except that the BAA may but is not required to:
    - ❑ Permit the business associate to use and disclose PHI for the proper management and administration of the business associate.
    - ❑ Permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
    - ❑ Permit the business associate to disclose PHI for the foregoing purposes if (1) the disclosure is required by law, or (2)(i) the business associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and (ii) the person notifies the business associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.
2. Provide that the business associate will:[9]
    - ❑ Not use or further disclose the PHI other than as permitted or required by the BAA or as required by law.
    - ❑ Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA.
    - ❑ Where applicable, comply with Security Rules with respect to electronic PHI.
    - ❑ Report to the covered entity any security incidents or use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of unsecured PHI as required by § 164.410.
    - ❑ Ensure that any subcontractors that receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI. Business associates may do so by requiring the subcontractors to execute a BAA with the business associate.
    - ❑ Make available PHI consistent with the patient's right to access PHI as set forth in § 164.524.
    - ❑ Make available PHI for amendment and incorporate any amendments to PHI in accordance with
    - ❑ § 164.526.
    - ❑ Make available the information required to provide an accounting of disclosures in accordance with
    - ❑ § 164.528, including certain information concerning disclosures of PHI in violation of the Privacy Rule.
    - ❑ To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligation. [*Note: this is a new requirement under the Omnibus Rule*].
    - ❑ Make 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 available to the Secretary of HHS for purposes of determining the covered entity's compliance with the Privacy Rule.

3. Include appropriate termination provisions[10] , i.e.:
    - ❑ At termination of the contract, if feasible, the business associate must return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such PHI.
    - ❑ If such return or destruction of PHI is not feasible, extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.
    - ❑ Authorize termination of the BAA by the covered entity if the covered entity determines that the business associate has violated a material term of the BAA.

Additional Terms. The OCR has published sample BAA language at its website. However, the OCR's sample language may not include additional terms that covered entities and business associates may want to include in their agreements. For example, **while not required by HIPAA**, covered entities may want to:

1. Confirm that the business associate is acting as an independent contractor and not as the agent of the covered entity.
2. Require business associates and subcontractors to carry appropriate insurance to cover HIPAA violations.
3. Require business associates and subcontractors to defend and indemnify the covered entity for violations of HIPAA or the BAA.
4. Require business associates, at their own cost, to respond to any potential HIPAA violation and provide any notice of privacy breaches or security incidents as mandated by the Privacy, Security or Breach Notification Rules.
5. Impose time limits or other conditions on the business associate's performance so long as such conditions do not establish an agency relationship as discussed below.
6. Coordinate the BAA with the underlying services agreement.
7. Include additional term or termination provisions.
8. Authorize termination of the underlying services agreement if the BAA is terminated.
9. Allow for amendment of the BAA as necessary to accommodate changes to the HIPAA Rules.
10. Include choice of law and venue provisions.

Business associates may want to include additional or alternative terms that minimize their exposure, such as:

1. Prohibit covered entities from asking the business associate to take any action that would violate the HIPAA Rules if done by the covered entity.
2. Prohibit covered entities from agreeing to restrictions on the use or disclosure of PHI that might adversely affect the business associate, or notify the business associate of such restrictions.
3. Authorize termination of the BAA if the covered entity agrees to restrictions that materially affect the business associate's ability to perform or costs of performance.
4. Allow the business associate to recover costs associated with such additional restrictions or requirements.
5. Eliminate or limit any insurance or indemnification agreement otherwise requested by the covered entity.
6. Waive or limit damages for which the business associate may be liable under the BAA.

Liability for Business Associate's Action. The HIPAA Privacy and Security rules confirm that a covered entity violates HIPAA if the covered entity knew of a pattern of activity or practice of a business associate that constituted a material breach or violation of the BAA unless the covered entity took reasonable steps to cure the breach, end the violation, or terminate the contract.[11] In addition, a covered entity may be vicariously liable for the business associate's misconduct if the business associate was acting as the agent of the covered entity.[12] The same rules apply to a business associates with respect to their subcontractors.[13] Accordingly, covered entities and business associates should ensure that their BAAs:

1. Confirm the business associate or subcontractor is acting as an independent contractor, and not as the agent of the covered entity or business associate; and
2. Confirm that the BAA does not give the covered entity or business associate such control over operational activities so as to make the business associate the agent of the covered entity, or the subcontractor the agent of the business associate.

Effect of No BAA. Covered entities and business associates violate HIPAA if there is no required BAA in place; however, business associates must still comply with the relevant HIPAA Rules even if there is no BAA.

---

[1]Under HIPAA, "business associates" are generally defined as those entities outside of the covered entity's workforce who create, receive, maintain or transmit PHI on behalf of a covered entity to perform certain enumerated functions, including claims processing; data analysis; utilization review; quality assurance; patient safety activities; billing; benefit management; practice management; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services; data transmission services if routine access to data is required; and subcontractors of business associates. 45 CFR § 160.103.
[2]*Id.* at §§ 164.402 and .404.
[3]*Id.* at §§ 164.308(b) and .502(e)(1)-(2).
[4]The Omnibus Rule extends the deadline to September 23, 2014, if (1) the BAA complied with HIPAA rules as they existed before January 25, 2013, and (2) the BAA is not renewed or modified prior to September 23, 2014. *See id.* at § 164.532(e).
[5]*Id.* at § 164.103.
[6]A covered entity need not execute a BAA if the covered entity disclosed only a limited data set (as defined by HIPAA) to the business associate and the covered entity has a data use agreement with the business associate that complies with §§ 164.514(e)(4) and 164.314(a)(1), if applicable. *See id.* at § 164.504(e)(3)(iv). If the covered entity and business associate are both governmental entities, the BAA may contain certain alternative or additional provisions. *See id.* at § 164.504(e)(3).
[7]*Id.* at §§ 164.314(a)(2)(iii) and .504(e)(5).
[8]*Id.* at § 164.504(e)(2)(i) and (4)(i)-(ii).
[9]*Id.* at §§ 164.504(e)(2)(ii) and .314(a)(2)
[10]*Id.* at § 164.504(e)(2)(ii)(J) and (iii). The covered entity may omit the provision authorizing termination if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate. *See id.* at § 164.504(e)(3)(iii).
[11]*Id.* at § 164.504(e)(1)(ii).
[12]*Id.* at § 160.402(c).
[13]*Id.* at §§ 160.402(c) and 164.504(e)(1)(iii).