CHECKLIST FOR BUSINESS ASSOCIATE AGREEMENTS

Background

A business associate is an entity or person (other than a member of the workforce of a covered entity) who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information ("PHI"). The term business associate also includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate, and a covered entity can be another covered entity's business associate. Generally, a covered entity may only disclose PHI to a business associate or allow a business associate to create, receive, maintain, or transmit PHI on its behalf if it has received satisfactory assurances in the form of a written business associate agreement ("BAA") that the business associate will appropriately safeguard the PHI. The business associate agreement ("BAA") also establishes the permissible uses and disclosures of PHI by the business associate. A business associate may use or disclose PHI only as permitted or required by the BAA or as required by law.

Terms Required under HIPAA

A BAA between the covered entity and a business associate must:[1]

1. Establish the permitted and required uses and disclosures of PHI by the business associate. 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:
    a. The BAA may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
    b. The BAA may permit the business associate to use and disclose PHI for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate 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:
    a. Not use or further disclose the PHI other than as permitted or required by the BAA or as required by law.
    b. Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA.

[1] 45 C.F.R. §164.504; 45 C.F.R. §164.314.

c. 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.
d. Ensure that any subcontractors that create, 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 information.
e. Make available PHI consistent with the patient's right to access PHI as set forth in §164.524.
f. Make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526.
g. 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.
h. To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation
i. 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.
j. Where applicable, comply with Security Rules with respect to electronic PHI.

3. Include certain termination provisions:
    a. At termination of the contract, if feasible, 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 information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
    b. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Sample Business Associate Agreement

The Department of Health and Human Services Office for Civil Rights has published a sample BAA (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html) for reference.

Additional Terms

BAAs that are compliant with HIPAA requirements (including the HHS sample BAA) may lack certain protective provisions for covered entities or business associates. However, a protective measure for a covered entity may not be in the best interest of the business associate, and vice versa. Thus, negotiation between the parties may be required. Below are terms that a covered entity or business associate may want to consider including in their BAA; however, it is important to note that this list is not exhaustive.

Covered Entity

a. Require that the business associate indemnify the covered entity for any HIPAA violations on the part of the business associate.
b. Require that the business associate maintain insurance to cover any HIPAA violations.
c. Require that the business associate responds to potential HIPAA violations and provides any breach notification required under HIPAA.
d. Impose notification time limits on the business associate (i.e., must notify covered entity within 2 days upon discovery of a breach).
e. Reference an underlying services agreement and authorize termination of the underlying services agreement if the BAA is terminated.
f. Allow for amendment of the BAA as necessary to accommodate changes to the HIPAA rules.
g. Include choice of law and venue provisions.

Business Associate

a. Eliminate or limit any insurance or indemnification agreement otherwise requested by the covered entity.
b. Eliminate or limit any requirement that the business associate responds to potential HIPAA violations and provides any breach notification required under HIPAA
c. Prohibit covered entities from asking the business associate to take any action that would violate the HIPAA Rules if done by the covered entity.
d. Prohibit covered entities from agreeing to restrictions on the use or disclosure of PHI that might adversely affect the business associate or allow termination of the BAA if the covered entity agrees to restrictions that would materially hamper the business associate's ability to perform the services necessitating the BAA.
e. Include choice of law and venue provisions.