COSMOS
Navigate the Compliance Universe

Healthcare Compliance Forms and Tools
Business Associate Agreement Checklist and Considerations

By Emma Trivax, Erin Whaley, Jim Koenig, Brent Hoard, Jonathan Ishee, and Kimberly Gillespie.[1]

Business Associate Agreement Background

In 2013, the U.S. Department of Health & Human Services (HHS) Office for Civil Rights announced a final rule that implemented a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to further strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[2] HIPAA requires that a covered entity enter into a business associate agreement (BAA) with a business associate. Among other things, the HITECH Act made business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements. The HITECH Act was needed to strengthen the HIPAA privacy and security protections for individual's health information maintained in electronic health records and other formats.

Definitions

Including applicable definitions into a BAA will clarify language and advise the writer/reader what terms mean. BAAs may include a statement with catch-all or specific definitions, as described below.

Catch-all Definition

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions

a. **Business associate**: "Business associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

b. **Covered entity**: "Covered entity" shall generally have the same meaning as the term "covered entity" at45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

c. **HIPAA Rules**: "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. §§ 160; 164.

d. **Breach**: This term means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E of this part which compromises the security or privacy of the protected health information.

e. **Unsecured protected health information**: This term means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

Checklist

This checklist sets forth contractual terms which must be included in a BAA and considerations for other terms which may be included. Please note: this checklist only provides the minimum requirements and considerations for a BAA. Every arrangement is different and has unique characteristics that may require additional customization to support the business objectives of the parties and provide appropriate protections. While a BAA may seem like a routine agreement, you should consult your attorney prior to executing any BAA.

Mandatory Provisions

These provisions **must** be included in every BAA:

- The business associate will not use or further disclose protected health information (PHI) other than as permitted or required by the BAA or as required by law.
- The business associate will use appropriate safeguards and comply, where applicable with Subpart C of 45 C.F.R. § 164 with respect to electronic protected health information (ePHI), to prevent use or disclosure of the information other than as provided for by the BAA.
- The business associate must report to the covered entity any use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of unsecured protected health information as required at 45 C.F.R. § 164.410.
- The business associate must report to the covered entity any security incident of which it becomes aware, however, notice of some security incidents may be addressed ahead of time for common unsuccessful events, such as: unsuccessful attempts at unauthorized use or disclosure such as pings and other broadcast attacks on a firewall, port scans, unsuccessful login attempts, denial of service attacks, or detection of malware.
- The business associate must, in accordance with 45 C.F.R § 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.
- The business associate must make available protected health information in a designated record set to the [choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 C.F.R § 164.524;
- The business associate must make PHI in a designated record set available for amendment and incorporate any amendments to protected health information in accordance with 45 C.F.R. § 164.526.
- The business associate must maintain and make available the information to the [choose either "covered entity" or "individual"] required to provide an accounting of the disclosures in accordance with 45 C.F.R. § 164.528.
- The business associate must, to the extent the business associate is to carry out a covered entity's

obligation under Subpart E of 45 C.F.R § 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s).

- The business associate must make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary of Health and Human Services for purposes of determining the covered entity's compliance; and
- At termination of the BAA, if feasible, return or destroy all protected health information 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.
- 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.

Optional Provisions

These terms may be included in your BAA. Whether or not the below terms are included in your BAA is generally analyzed on a case-by-case basis. Additionally, where a BAA is between a business associate and a subcontractor, the business associate must not extend rights to the subcontractor that the business associate was not granted from its BAA with the covered entity.

- The business associate may use PHI for the business associate’s proper management and administration and to carry out the legal responsibilities of the business associate.
- The business associate may disclose PHI for the business associate’s proper management and administration and to carry out the legal responsibilities of the business associate, provided that 1) the disclosure is required by law; or 2) the business associate obtains reasonable assurances from the person to whom the information 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 the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- The business associate may perform data aggregation services on behalf of the covered entity relating to the healthcare operations of the covered entity.
- The business associate may use PHI obtained from the covered entity to de-identify that PHI in accordance with the de-identification requirements of the Privacy Rule. Once properly de-identified, the data is not PHI and no longer subject to requirements and restrictions under HIPAA.
- The BAA shall terminate in the event that the underlying relationship, functions, or services that gives rise to the necessity of a BAA terminates for any reason.
- The business associate may use PHI to report violations of law to the appropriate state and federal authorities, consistent with 45 C.F.R. § 164.502(j).
- The covered entity shall notify the business associate of any restriction to the use or disclosure of PHI that the covered entity has agreed to in accordance with 45 C.F.R. § 164.522(a).

- The covered entity shall notify the business associate of any confidential communication requests which the covered entity has agreed to in accordance with 45 C.F.R. § 164.522(b).
- Determine whether the business associate and the covered entity agree on:
    - The time in which improper use or disclosure, a security incident, or breach of unsecured PHI must be disclosed.
    - The time in which PHI must be made available.
    - The time in which PHI must be amended.
    - The time in which an accounting of disclosures must be provided.
    - Non-HIPAA-specific provisions such as: indemnification, limitation of liability, required types of insurance, governing law, venue and other standard contractual clauses.
- Electronic Protected health information (PHI) will be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Valid encryption processes for data at rest and data in motion will be applied.
- Media on which the PHI is stored or recorded must be properly destroyed compliant with NIST standards.[3]

Four Additional Considerations

- With the prevalence of cloud services, it is possible that ePHI may be transferred and stored outside the United States (i.e., offshoring). Offshoring is permitted so long as there is a BAA (subcontractor) with the cloud service provider and all HIPAA requirements are met. However, it is not uncommon for a BAA to include a provision that expressly prohibits this practice. Permitted uses of PHI and BAAs with offshore companies conducting functions for covered entities or BAAs should be discussed in an annual HIPAA Risk Assessment.
- 42 C.F.R. Part 2 regulations are intended to safeguard the confidentiality of patient records regarding treatment for substance use disorders. Health providers that are both Part 2 providers and covered entities must ensure that their BAAs also meet the requirements for a Qualified Service Organization Agreement (QSOA) as required by Part 2.
- Several states have their own laws governing health information that include requirements in addition to or more stringent than those set by the federal standards implemented in HIPAA Rules. HIPAA does not preempt any state law that provides individuals with more rigorous protections or expanded rights of access to their health information than HIPAA does. As such, be aware that depending on your state's laws, you may have to include additional provisions into your BAA.
- In 2016, the 21st Century Cures Act (Cures Act) made sharing electronic health information the expected norm in healthcare by authorizing the Secretary of Health and Human Services to identify "reasonable and necessary activities that do not constitute information blocking."[4] Healthcare providers, certain health information technology vendors, and health information exchanges/health information networks are therefore prohibited from engaging in information blocking—actions that discourage or interfere with the access, use or exchange of health information. These information blocking actors should ensure that their BAAs do not require them, or their business associates, to act in a manner that could be construed as violating the information blocking rule.

1 Contributed by Troutman Pepper attorneys Emma Trivax, Erin Whaley, Jim Koenig, Brent Hoard, Jonathan Ishee, and Kimberly Gillespie.
2 45 C.F.R. §§ 160; 164, Modifications to the HIPAA Privacy, Security, Enforcement, and BreachNotification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rulehttps://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf
3 HHS, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
442 U.S.C. § 300jj–52(3).