HIPAA

Business Associate Agreement

Free Template

Provided by Auditious.io, Compliance Automation for SOC 2, ISO 27001, HIPAA & GDPR

SAMPLE DOCUMENT, FOR REFERENCE ONLY

How to use this template

This document is a starting point, not a finished contract. Replace every bracketed placeholder with your actual details, remove any optional clauses that don't apply to your relationship, and have qualified legal counsel review the final version before either party signs. Requirements can vary depending on your specific data flows, subcontractor relationships, and state law.

This template reflects the core clauses OCR expects under the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule, including the changes introduced by the HITECH Act and the 2013 Omnibus Rule.

BUSINESS ASSOCIATE AGREEMENT

This is a sample template for reference purposes. Instructions to preparer are shown in gray italics like this. Delete instructional text before finalizing.

This Business Associate Agreement ("Agreement") is entered into as of

Effective Date: ____

Covered Entity ("Covered Entity"): ____

Covered Entity Address: ____

Business Associate ("Business Associate"): ____

Business Associate Address: ____

Covered Entity and Business Associate are each a "Party" and together the "Parties." This Agreement supplements and is made part of the underlying services agreement between the Parties dated ______________________ (the "Underlying Agreement"), under which Business Associate performs services that involve the creation, receipt, maintenance, or transmission of Protected Health Information on behalf of Covered Entity.

1. Definitions

Terms used but not otherwise defined in this Agreement have the meanings given in the HIPAA Privacy Rule (45 C.F.R. Part 160 and Part 164, Subparts A and E), the HIPAA Security Rule (45 C.F.R. Part 160 and Part 164, Subparts A and C), and the HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D), collectively referred to as "HIPAA." "Protected Health Information" or "PHI" means individually identifiable health information, including Electronic Protected Health Information ("ePHI"), created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

2. Permitted Uses and Disclosures of PHI

(a) Business Associate may use or disclose PHI only as permitted or required by this Agreement, the Underlying Agreement, or as required by law. Business Associate may not use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity, except as permitted under 45 C.F.R. § 164.504(e)(2)(i)(A) and (B) for Business Associate's own management, administration, or legal responsibilities.

(b) Business Associate may use PHI internally for its proper management and administration, or to fulfill its legal responsibilities, provided any disclosure for such purposes is required by law, or Business Associate obtains reasonable assurances from the recipient that the PHI will be held confidentially and used only for the purpose disclosed, and that the recipient will notify Business Associate of any instance in which the confidentiality of the PHI is breached.

(c) Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted under 45 C.F.R. § 164.504(e)(2)(i)(B), if applicable.

3. Safeguards

Business Associate will implement and maintain appropriate administrative, physical, and technical safeguards, consistent with the HIPAA Security Rule, to prevent the use or disclosure of PHI other than as provided for by this

Agreement. This includes safeguards to protect the confidentiality, integrity, and availability of any ePHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

4. Reporting of Breaches, Security Incidents, and Improper Disclosures

(a) Business Associate will report to Covered Entity, in writing, any use or disclosure of PHI not permitted by this Agreement, and any Security Incident of which it becomes aware, without unreasonable delay and in no case later than ______ business days after discovery.

(b) In the event of a Breach of Unsecured PHI, Business Associate will notify Covered Entity without unreasonable delay and in no case later than ______ business days following discovery of the Breach, and will provide the information required under 45 C.F.R. § 164.410, including the identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed.

5. Subcontractors

Business Associate will ensure that any subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees, in writing, to restrictions and conditions on the use and disclosure of PHI that are at least as restrictive as those that apply to Business Associate under this Agreement, including the requirement to implement reasonable and appropriate safeguards.

6. Access, Amendment, and Accounting of Disclosures

(a) Business Associate will make PHI maintained in a Designated Record Set available to Covered Entity, or as directed by Covered Entity, to an Individual, to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524, within ______ business days of a request.

(b) Business Associate will make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526, within ______ business days of a request from Covered Entity.

(c) Business Associate will document disclosures of PHI and make information available to Covered Entity as needed to satisfy Covered Entity's obligations to provide an accounting of disclosures under 45 C.F.R. § 164.528.

7. Availability of Books and Records

Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA.

8. Term and Termination

(a) This Agreement is effective as of the Effective Date and will terminate when all PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if return or destruction is infeasible, protections are extended in accordance with subsection (c) below.

(b) Covered Entity may terminate this Agreement and the Underlying Agreement if it determines that Business Associate has violated a material term of this Agreement, subject to any applicable cure period.

(c) Upon termination of this Agreement, Business Associate will return or destroy all PHI received from, or created or received on behalf of, Covered Entity. If return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the PHI for as long as it retains the PHI, and limit further uses and disclosures to those purposes that make return or destruction infeasible.

9. Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in HIPAA means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with HIPAA.

(c) Survival. The obligations of Business Associate under Section 8(c) survive the termination of this Agreement.

(d) Interpretation. Any ambiguity in this Agreement will be resolved in favor of a meaning that permits compliance with HIPAA.

(e) Governing Law. This Agreement is governed by the laws of the State of ______________________, without regard to conflict of law provisions.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

COVERED ENTITY	**BUSINESS ASSOCIATE**
____________________	____________________
Signature	Signature
____________________	____________________
Printed Name	Printed Name
____________________	____________________
Title	Title
____________________	____________________
Date	Date

Clause Checklist: What OCR Expects to See

Use this as a final review before signing. Each item below corresponds to a clause in the template above.

- ✓ Permitted and required uses and disclosures of PHI are clearly defined (Section 2)
- ✓ Prohibition on uses or disclosures that would violate the Privacy Rule if done by the covered entity (Section 2a)
- ✓ Requirement to implement Security Rule safeguards for ePHI (Section 3)
- ✓ Reporting timeline for security incidents and impermissible disclosures (Section 4a)
- ✓ Breach notification timeline and required content per 45 C.F.R. § 164.410 (Section 4b)
- ✓ Subcontractor flow-down requirements (Section 5)
- ✓ Individual access, amendment, and accounting of disclosures support (Section 6)
- ✓ Availability of books and records to HHS (Section 7)
- ✓ Return or destruction of PHI upon termination (Section 8c)
- ✓ Survival of obligations after termination (Section 9c)

This checklist and template are provided for general informational purposes and do not constitute legal advice. Consult qualified legal counsel before executing any Business Associate Agreement.