ComplyJet

# HIPAA BAA Template

A free, adaptable business associate agreement for a SaaS company acting as business associate: eleven clauses with sample wording, Exhibits A and B, a subcontractor flow-down rider, a one-page vendor-side checklist, a changes log and a customization checklist. Built around 45 CFR 164.504(e), 164.314(a) and 164.308(b).

**HOW TO USE THIS TEMPLATE**

Replace every [bracketed value] with a fact about your own deal, delete any option that does not apply, and fill Exhibits A and B from the PHI flows and vendors you actually run. Bracketed ranges for notice hours, windows and cure periods are examples only. HIPAA sets one breach-reporting number for a business associate, the 60-calendar-day outer limit in 45 CFR 164.410, and everything else in brackets is a commercial choice.

**BEFORE YOU SIGN**

This template is a starting point, not legal advice. HHS says its own sample provisions are only sample language, may not be sufficient for a binding contract under state law, and do not replace consultation with a lawyer. Have healthcare counsel review the final agreement.

## Business Associate Agreement

| | |
|---|---|
| **Covered Entity** | [Customer legal name], [address] |
| **Business Associate** | [Company legal name], [address] |
| **Services agreement** | [Name and date of the master services agreement or order] |
| **Effective date** | [Date] |

### Clause 1: Definitions and Roles

Needed to make it work | 45 CFR 160.103; HHS sample provisions (definitions)

"Business Associate" means [Company]. "Covered Entity" means [Customer]. "HIPAA Rules" means the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164. Capitalized terms not defined in this Agreement, including Breach, Designated Record Set, Disclosure, Minimum Necessary, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information and Use, have the meanings given in the HIPAA Rules. This Agreement applies to Protected Health Information that Business Associate creates, receives, maintains or transmits for Covered Entity in providing the services described in Exhibit A.

## Clause 2: Permitted and Required Uses and Disclosures

Required | 45 CFR 164.502(a)(3), 164.502(b), 164.504(e)(2)(i), (e)(2)(ii)(A), (e)(4)

Business Associate may use and disclose Protected Health Information only as necessary to perform the services described in Exhibit A, as permitted by this Agreement, or as Required By Law. Business Associate will not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except as permitted in this Section. Business Associate may use Protected Health Information for its own proper management and administration and to carry out its legal responsibilities. Business Associate may disclose Protected Health Information for those purposes only if the disclosure is Required By Law, or Business Associate obtains reasonable assurances from the recipient that the information will stay confidential and be used or further disclosed only as Required By Law or for the purpose for which it was disclosed, and the recipient agrees to notify Business Associate of any known breach of confidentiality. Business Associate will request, use and disclose only the minimum necessary Protected Health Information to accomplish the intended purpose. [Optional: Business Associate may provide data aggregation services relating to the health care operations of Covered Entity.] Business Associate will not de-identify Protected Health Information, or use it to train or improve its own products, unless Exhibit A expressly permits it.

## Clause 3: Safeguards and Security Rule Compliance

Required | 45 CFR 164.504(e)(2)(ii)(B), 164.314(a)(2)(i)(A), 164.308(b)

Business Associate will use appropriate administrative, physical and technical safeguards, and will comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement. Business Associate's current safeguards are described in [its security addendum / its most recent SOC 2 report available on request]. Business Associate will conduct and document a risk analysis and keep its safeguards reasonable and appropriate for the risks identified, and will train its workforce members on these obligations.

## Clause 4: Reporting Unauthorized Uses, Security Incidents and Breaches

Required, commercial number | 45 CFR 164.504(e)(2)(ii)(C), 164.314(a)(2)(i)(C), 164.410, 164.404(c)

Business Associate will report to Covered Entity: (a) any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware; (b) any Security Incident of which it becomes aware; and (c) any Breach of Unsecured Protected Health Information. Business Associate will report a Breach without unreasonable delay and in no case later than [__] calendar days after discovery, as discovery is determined under 45 CFR 164.410(a)(2), and in any event within [24 to 72] hours after Business Associate confirms the Breach. The report will identify, to the extent known, each individual whose Unsecured Protected Health Information was or is reasonably believed to have been accessed, acquired, used or disclosed, and will give Covered Entity the other information it needs to notify individuals under 45 CFR 164.404(c), supplemented as more becomes known. Unsuccessful Security Incidents, such as pings and port scans that do not result in unauthorized access, are reported by this sentence and require no further notice. Business Associate will cooperate with Covered Entity's investigation and mitigation.

## Clause 5: Subcontractors

Required, commercial notice period | 45 CFR 164.504(e)(2)(ii)(D), (e)(5), 164.502(e)(1)(ii), 164.308(b)(2)

In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate will ensure that any Subcontractor that creates, receives, maintains or transmits Protected Health Information on its behalf agrees in writing to the same restrictions, conditions and requirements that apply to Business Associate with respect to that information. Business Associate will give Covered Entity a current list of such Subcontractors on request. [Optional: Business Associate will notify Covered Entity at least [15 to 30] days before engaging a new Subcontractor for the services in Exhibit A.]

## Clause 6: Individual Rights: Access, Amendment and Accounting

Required, commercial windows | 45 CFR 164.504(e)(2)(ii)(E)-(G), 164.524, 164.526, 164.528

Within [10 to 15] days after Covered Entity's written request, Business Associate will make available Protected Health Information in a Designated Record Set as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524, make any amendment to Protected Health Information that Covered Entity directs or agrees to under 45 CFR 164.526, and make available the information required to provide an accounting of disclosures under 45 CFR 164.528. If an individual sends Business Associate a request directly, Business Associate will forward it to Covered Entity within [5 to 10] business days and will not respond to the individual except as Covered Entity directs.

## Clause 7: HHS Access to Books and Records and Carrying Out the Covered Entity's Duties

Required | 45 CFR 164.504(e)(2)(ii)(H), (I)

Business Associate will make its internal practices, books and records relating to the use and disclosure of Protected Health Information available to the Secretary for purposes of determining compliance with the HIPAA Rules. To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164, Business Associate will comply with the requirements of Subpart E that apply to Covered Entity in the performance of those obligations. [Optional: Business Associate will cooperate with a reasonable audit by Covered Entity, no more than [once per year] unless a Breach has occurred, on [30] days' notice.]

## Clause 8: Return or Destruction of PHI at Termination

Required, commercial window | 45 CFR 164.504(e)(2)(ii)(J)

Within [30 to 60] days after this Agreement ends for any reason, Business Associate will return to Covered Entity, or, if Covered Entity agrees, destroy, all Protected Health Information it still maintains in any form, and will certify destruction in writing on request. If return or destruction is not feasible, including for encrypted backups and logs that are overwritten on a fixed cycle, Business Associate will notify Covered Entity of the reasons, extend the protections of this Agreement to the retained information, and limit further use and disclosure to the purposes that make return or destruction infeasible, for as long as it retains the information. These obligations survive termination.

## Clause 9: Term and Termination for Material Violation

Required, commercial cure period | 45 CFR 164.504(e)(2)(iii)

This Agreement takes effect on [effective date] and continues until the services agreement ends or this Agreement is terminated under this Section, whichever is earlier. Covered Entity may terminate this Agreement, and the services agreement to the extent it depends on Protected Health Information, if Covered Entity determines that Business Associate has violated a material term of this Agreement and Business Associate has not cured the violation within [30] days after written notice. If cure is not possible, Covered Entity may terminate immediately.

## Clause 10: Liability, Indemnification and Insurance

Commercial | Commercial term: not required by regulation

[Option A: Each party's liability under this Agreement is subject to the limitations in the services agreement.] [Option B: Business Associate's aggregate liability under this Agreement is capped at [amounts paid in the 12 months before the claim], except for liability arising from Business Associate's own gross negligence or willful misconduct.] [Option C: Business Associate will reimburse Covered Entity's reasonable, documented costs of notifying affected individuals, up to [cap], where a Breach results from Business Associate's failure to comply with this Agreement.] Business Associate will maintain [cyber liability] insurance of at least [amount] during the term.

## Clause 11: Order of Precedence, Amendment and Governing Law

Needed to make it work | Needed to make the agreement work: not required by regulation

If this Agreement conflicts with the services agreement on the handling of Protected Health Information, this Agreement controls. A reference to a section of the HIPAA Rules means that section as in effect or as amended. The parties will amend this Agreement as necessary to comply with the HIPAA Rules and other applicable law, and any ambiguity will be read to permit compliance with the HIPAA Rules. This Agreement is governed by the laws of [State], except where federal law controls. Nothing in this Agreement gives a third party any right.

## Signatures

| Covered Entity: [Customer] | Business Associate: [Company] |
|---|---|
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |

## Exhibit A: Services and Protected Health Information Covered

| Item | Your entry |
|---|---|
| Services provided | [Describe the product and services] |
| Permitted purposes for PHI | [List each purpose, narrowly. Delete data aggregation unless needed] |
| Categories of PHI | [For example: patient names, dates of service, clinical notes] |
| Systems where PHI is stored or processed | [Hosting region, databases, logs, support tools] |
| De-identification or product-improvement use | [Not permitted / permitted only as follows] |
| Breach report contact at Covered Entity | [Name, email, phone] |
| Security contact at Business Associate | [Name, email, phone] |

## Exhibit B: Current Subcontractors

| Subcontractor | Service | PHI handled | BAA signed (date) |
|---|---|---|---|
| [Cloud host] | [Hosting] | [Stored, processed] | [Date] |
| | | | |
| | | | |
| | | | |

## Subcontractor Flow-Down Rider

Attach this rider to a vendor's paper, or sign it as a stand-alone subcontractor business associate agreement. It carries the same restrictions down the chain (45 CFR 164.504(e)(5), 164.308(b)(2), 164.314(a)(2)(iii)).

> [Subcontractor] agrees to the same restrictions, conditions and requirements that apply to [Company] under its business associate agreement with [Customer] with respect to Protected Health Information, including the safeguards required by Subpart C of 45 CFR Part 164. [Subcontractor] will report to [Company] any use or disclosure not provided for, any Security Incident and any Breach of Unsecured Protected Health Information without unreasonable delay and in any event within [__] hours of discovery, so that [Company] can meet its own reporting obligations. [Subcontractor] will return or destroy Protected Health Information on termination as provided in Clause 8, and will ensure that any further subcontractor it engages agrees to these terms in writing.

**WATCH THE TIMING**

Your window to your customer must be longer than your subcontractor's window to you. If your hosting provider gets 72 hours and you promised your customer 48, you have breached your own clause before you have heard of the incident.

## Vendor-Side Checklist (One Page)

Run this on every BAA, yours or theirs, before you sign.

- ☐ Parties and effective date are correct
- ☐ Exhibit A describes the real services and PHI
- ☐ Permitted uses are listed, not "any lawful purpose"
- ☐ Every required Privacy Rule term is present (45 CFR 164.504(e)(2))
- ☐ Security incident and breach are both defined
- ☐ Breach window starts at a defined point and your team can meet it
- ☐ Subcontractor flow-down is present and your own vendors have signed
- ☐ Return or destruction covers backups and logs
- ☐ Termination for material violation is present, with a cure period if agreed
- ☐ Liability matches your services agreement
- ☐ The BAA prevails on PHI if it conflicts with the services agreement
- ☐ Healthcare counsel has read it

## Changes Log

| Date | Clause | Change | Reason | Approved by |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

## Customization Checklist

| Step | Done |
|---|---|
| 1. List your PHI data flows and name the parties and services (Exhibit A) | ☐ |
| 2. Set permitted uses narrowly and delete the data-aggregation option unless needed (Clause 2) | ☐ |
| 3. Choose your commercial numbers: breach-notice hours, forwarding window, return or destruction window, cure period (Clauses 4, 6, 8, 9) | ☐ |
| 4. Add the subcontractor rider and list current subcontractors (Clause 5, Exhibit B) | ☐ |
| 5. Choose a liability option and insurance amount with counsel (Clause 10) | ☐ |
| 6. Counsel review, sign, and file in your BAA inventory the same day | ☐ |
| 7. Keep the BAA and amendments for six years after it was last in effect (see 45 CFR 164.316(b)(2)(i)) | ☐ |

Free template from ComplyJet. Source guide: https://www.complyjet.com/blog/hipaa-baa-template. ComplyJet is not a law firm and does not draft, negotiate or sign contracts. This document is a starting point for review by healthcare counsel and is not legal advice. Sample wording follows the structure of HHS OCR's sample business associate agreement provisions (published January 25, 2013), which HHS says are not required for compliance with the HIPAA Rules.