



BUSINESS ASSOCIATE AGREEMENT (TEMPLATE)

DRAFT TEMPLATE - NOT LEGAL ADVICE. This document must be reviewed and finalised by qualified outside healthcare counsel, completed (every bracketed placeholder, including the Role-Mapping Schedule below), and executed by authorised representatives before it has any effect. Downloading this template, uploading a signed copy, or administrative approval of a partner application **does not** by itself execute an agreement or authorise any use or disclosure of protected health information (PHI). This template is not a certification of HIPAA compliance and may not satisfy state-law requirements.

Role-Mapping Schedule (complete BEFORE signature)

A business associate relationship depends on the actual data and services involved, not on the label "clinic" or "pharmacy". Counsel must complete this schedule. If counsel determines that no business associate relationship exists for a data flow (for example, where independent health care providers disclose PHI to each other for treatment purposes), that flow must **not** be papered with this BAA; document the determination instead. Do not use a "mutual" BAA as a substitute for this analysis.

Item	Completion
Upstream party (" Covered Party ")	[Partner legal entity] acting as: [] Covered Entity [] Business Associate of [identify covered entity]
Downstream party (" Business Associate ")	[TrueCore legal entity] acting as: [] Business Associate [] Subcontractor Business Associate
Services involving PHI	[describe exactly which Platform services create, receive, maintain or transmit PHI]
Categories of PHI	[e.g., demographics, contact details, intake responses, prescription/order status - list only what is needed]
Data flows excluded (counsel determination)	[e.g., treatment disclosures between independent providers - reference written determination]
Counsel reviewer and date	[name, firm, date]

The terms below apply only to the PHI and services listed in this Schedule.

This Business Associate Agreement (the "**BAA**") is entered into as of [Effective Date] by and between [**Covered Party legal entity**] ("**Covered Party**") and [**Business Associate legal entity**] ("**Business Associate**"), and supplements the Master Services Agreement dated [date] (the "**Underlying Agreement**").



1. Definitions

Capitalised terms not defined here have the meanings given in 45 C.F.R. Parts 160 and 164 (the "**HIPAA Rules**"), including Breach, Designated Record Set, Individual, Minimum Necessary, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor and Unsecured PHI. "PHI" is limited to PHI created, received, maintained or transmitted by Business Associate on behalf of Covered Party.

2. Obligations of Business Associate

Business Associate agrees to:

2.1 Permitted uses only. Not use or disclose PHI other than as permitted or required by this BAA or as Required by Law.

2.2 Safeguards. Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 (the Security Rule) with respect to electronic PHI, to prevent use or disclosure other than as provided by this BAA.

2.3 Reporting. Report to Covered Party: (a) any use or disclosure of PHI not provided for by this BAA, of which it becomes aware; (b) any Security Incident of which it becomes aware [the parties should specify, with counsel, how unsuccessful attempts (e.g., pings, port scans) are reported]; and (c) any Breach of Unsecured PHI as required by 45 C.F.R. § 164.410, **without unreasonable delay and in no case later than 60 calendar days after discovery**. The parties contractually agree to an earlier initial notice deadline of **[e.g., 24 hours / number] after discovery**, which controls where earlier. Notice will include, to the extent known, the identification of each affected Individual and other information Covered Party needs for its own notifications, supplemented as information becomes available.

2.4 Subcontractors. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any Subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions, conditions and requirements that apply to Business Associate, including compliance with the Security Rule.

2.5 Access. Make PHI in a Designated Record Set available to Covered Party within [number] business days of request as necessary to satisfy Covered Party's obligations under 45 C.F.R. § 164.524. If an Individual requests access directly from Business Associate, forward the request to Covered Party within [number] business days.

2.6 Amendment. Make amendments to PHI in a Designated Record Set as directed or agreed by Covered Party under 45 C.F.R. § 164.526, within [number] business days.

2.7 Accounting. Maintain and make available the information required for Covered Party to provide an accounting of disclosures under 45 C.F.R. § 164.528, within [number] business days.

2.8 Delegated obligations. To the extent Business Associate carries out any obligation of Covered Party under Subpart E of 45 C.F.R. Part 164 (the Privacy Rule), comply with the requirements of the Privacy Rule that apply to Covered Party in performing that obligation.

2.9 Books and records. Make its internal practices, books and records relating to PHI available to the Secretary for purposes of determining compliance with the HIPAA Rules.



2.10 **Minimum necessary.** Request, use and disclose only the minimum necessary PHI where the minimum necessary standard applies.

2.11 **Mitigation and cooperation.** Mitigate, to the extent practicable, any harmful effect known to Business Associate of a use or disclosure in violation of this BAA, and reasonably cooperate with Covered Party's investigation and notification obligations.

3. Permitted Uses and Disclosures by Business Associate

3.1 Business Associate may use or disclose PHI only as necessary to perform the services described in the Role-Mapping Schedule and the Underlying Agreement.

3.2 Business Associate may use PHI for its proper management and administration or to carry out its legal responsibilities, and may disclose PHI for those purposes if the disclosure is Required by Law, or Business Associate obtains reasonable assurances that the recipient will hold it confidentially, use or further disclose it only as Required by Law or for the purpose disclosed, and notify Business Associate of any known breach of confidentiality.

3.3 **No other authorisation by default.** This BAA does **not** authorise: marketing; sale of PHI; data aggregation services; de-identification of PHI for Business Associate's own purposes or any licence to use de-identified data; or use of PHI to train or improve artificial-intelligence or machine-learning models. Any such activity requires a separate written amendment reviewed by counsel and compliant with the HIPAA Rules.

3.4 Business Associate will not use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Party, except as permitted by Sections 3.2.

4. Obligations of Covered Party

4.1 Notify Business Associate of any limitation in its notice of privacy practices, any change or revocation of an Individual's permission, and any restriction agreed to under 45 C.F.R. § 164.522, to the extent it may affect Business Associate's use or disclosure of PHI.

4.2 Not request Business Associate to use or disclose PHI in any manner not permissible under the Privacy Rule if done by Covered Party.

4.3 Disclose to Business Associate only the minimum necessary PHI for the services.

5. Term and Termination

5.1 **Term.** This BAA is effective on the Effective Date and continues until all PHI is returned or destroyed under Section 5.3, or protections are extended under Section 5.4.

5.2 **Termination for material breach.** Covered Party may terminate this BAA and the affected portions of the Underlying Agreement if Business Associate has violated a material term and has not cured the violation within [number] days of written notice (or immediately if cure is not possible). Where Business Associate is a Subcontractor, Business Associate may likewise terminate its subcontract for a Subcontractor's uncured material breach.



5.3 Return or destruction. On termination, Business Associate will, at Covered Party's direction, return or destroy all PHI (including PHI held by Subcontractors) and retain no copies, within [number] days, and certify completion in writing.

5.4 Infeasibility. If return or destruction is infeasible, Business Associate will notify Covered Party of the conditions that make it infeasible, extend the protections of this BAA to that PHI, and limit further uses and disclosures to the purposes that make return or destruction infeasible, for so long as Business Associate maintains the PHI.

5.5 Survival. Sections 2, 3, 5.3, 5.4 and 6 survive termination for as long as Business Associate or its Subcontractors maintain PHI.

6. Miscellaneous

6.1 Regulatory references. A reference to a section of the HIPAA Rules means the section as in effect or as amended. **6.2 Amendment.** The parties will amend this BAA as necessary to comply with changes in the HIPAA Rules or other applicable law. **6.3 Interpretation and precedence.** Ambiguity is resolved to permit compliance with the HIPAA Rules. This BAA controls over the Underlying Agreement with respect to PHI. **6.4 No waiver of duties.** Nothing in this BAA waives or limits either party's independent obligations under the HIPAA Rules or state law. **6.5 No third-party beneficiaries.** Nothing in this BAA confers, or is intended to confer, any rights, remedies, obligations or liabilities on any person other than Covered Party, Business Associate and their respective permitted successors and assigns. Individuals' rights under the HIPAA Rules exist independently of this BAA and are not limited by this Section. **6.6 Secure notices.** Privacy and security notices under this BAA must be sent to the secure-notice contacts below by [method, e.g., encrypted email and phone], and are effective on receipt.

	Covered Party	Business Associate
Privacy/security contact	[Name, title]	[Name, title]
Secure email	[]	[]
Phone	[]	[]



Data, Service, Retention, Access and Security Schedule

Item	Completion
Systems hosting PHI	[]
Data location / regions	[]
Retention period per data category	[]
Personnel/role access model	[]
Encryption in transit / at rest	[]
Audit logging and review cadence	[]
Subcontractors with PHI access	[name, service, BAA date]
Incident response contacts and escalation	[]

Signatures

	[Covered Party legal entity]	[Business Associate legal entity]
Signature	_____	_____
Name	[Name]	[Name]
Title	[Title]	[Title]
Date	[Date]	[Date]



Counsel Notes (non-operative; delete before execution)

- Required BAA content is drawn from 45 C.F.R. §§ 164.504(e), 164.314(a) and the breach-notification timing in § 164.410. Confirm current text before execution.
- HHS sample BAA provisions: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html> - HHS states the sample language is not a substitute for review by a lawyer and may need changes to reflect state law and the parties' relationship.
- HHS business associate guidance (including when providers exchanging PHI for treatment are not business associates): <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>
- Pharmacy compounding framework referenced in the Underlying Agreement:
<https://www.fda.gov/drugs/human-drug-compounding/human-drug-compounding-laws>
- State laws (e.g., health-data privacy statutes, breach statutes with shorter deadlines) may impose additional terms.