Business Associate Agreement

Effective August 6, 2026 · Version 2026-08-06 ·
Applies to United States workspaces

This Business Associate Agreement (this "BAA") supplements and is incorporated into the Terms of Use between **Underline.AI, Inc.**, a Delaware corporation ("Business Associate," "Underline," or "we"), and the clinician, practice, or entity accepting it ("Covered Entity" or "you").

This BAA applies to workspaces in the United States. You accept it when you create your workspace. It takes effect on that date and governs from the first moment any Protected Health Information is made available to us.

This BAA operates only where HIPAA applies to you — that is, where you are a Covered Entity, or a Business Associate of one, as those terms are defined in the HIPAA Rules. If HIPAA does not apply to your practice, this BAA imposes no obligations on either party and confers no rights, and our processing of your patient records is instead governed by the Terms of Use and by any data protection agreement we have separately entered into with you. Nothing in this BAA is a representation that accepting it satisfies a data protection obligation arising under the law of a jurisdiction other than the United States.

The parties intend this BAA to satisfy the requirements of 45 C.F.R. §§ 164.502(e) and 164.504(e).

1. Definitions

Capitalized terms not defined here have the meanings given in the HIPAA Rules.

- **HIPAA Rules** — the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended, including by the Health Information Technology for Economic and Clinical Health Act.

- **Protected Health Information** or **PHI** — as defined at 45 C.F.R. § 160.103, limited to information Business Associate creates, receives, maintains, or transmits for or on behalf of Covered Entity. **ePHI** means PHI in electronic form.
- **Breach**, **Designated Record Set**, **Disclosure**, **Individual**, **Required by Law**, **Secretary**, **Security Incident**, **Subcontractor**, **Unsecured PHI**, and **Use** have the meanings given in the HIPAA Rules.
- **Services** — the Underline.Health platform and related services provided under the Terms of Use.

2. Permitted uses and disclosures

2.1 Provision of the Services. Business Associate may Use and Disclose PHI only as necessary to perform the Services, as permitted or required by this BAA, or as Required by Law. Business Associate will not Use or Disclose PHI in any manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity.

2.2 Management and administration. Business Associate may Use PHI for its own proper management and administration and to carry out its legal responsibilities. Business Associate may Disclose PHI for those purposes only if the Disclosure is Required by Law, or if Business Associate obtains reasonable assurances from the recipient that the information will be held confidentially, used or further disclosed only as Required by Law or for the purpose for which it was disclosed, and that the recipient will notify Business Associate of any breach of confidentiality.

2.3 Data aggregation. Business Associate may Use PHI to provide data aggregation services relating to the health care operations of Covered Entity, as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

2.4 De-identification. Business Associate may de-identify PHI in accordance with 45 C.F.R. § 164.514(b) and may Use and Disclose the resulting de-identified information to operate, secure, evaluate, and improve the Services and to produce aggregate statistics. De-identified information is not PHI. Business Associate will not attempt to re-identify de-identified information or contact any Individual, and will not Use de-identified information to train, fine-tune, or otherwise improve any generative artificial intelligence model.

2.5 Minimum necessary. Business Associate will limit its Use, Disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose, consistent with 45 C.F.R. § 164.502(b).

2.6 No training of models. Notwithstanding anything else in this BAA, Business Associate will not Use PHI, and will not permit any Subcontractor to Use PHI, to train, fine-tune, or otherwise improve any generative artificial intelligence model.

2.7 No sale of PHI; no marketing. Business Associate will not sell PHI and will not Use or Disclose PHI for marketing or advertising purposes.

3. Safeguards

3.1 Security Rule compliance. Business Associate will comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, and will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI.

3.2 Current measures. Without limiting Section 3.1, Business Associate presently maintains: encryption of ePHI in transit using TLS 1.2 or higher and at rest under customer-managed keys for the primary database and its snapshots; verification of database server certificates against a pinned certificate authority; role-based access on a least-privilege basis with no long-lived static credentials; multi-factor authentication for administrative access; administrative access through session-recorded channels with no inbound shell access to production; tamper-evident, append-only audit logging of access to PHI, retained for six years; object-level logging of reads and writes on the clinical asset store; automated deletion of session audio following transcription; and point-in-time database recovery.

3.3 Workforce. Business Associate will ensure that members of its workforce with access to PHI are subject to confidentiality obligations and are trained appropriately.

4. Subcontractors

4.1 Flow-down. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate will ensure that each Subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees in writing to restrictions and conditions at least as restrictive as those that apply to Business Associate under this BAA.

4.2 Disclosure. A current list of Subcontractors that may process PHI is published at https://underline.health/subprocessors/. Business Associate will update that list before a new Subcontractor begins processing PHI and will give Covered Entity at least thirty (30) days' notice of the addition by email or within the Services. If Covered Entity reasonably objects to a new Subcontractor on data protection grounds, Covered Entity may terminate the Services without penalty and receive a pro-rata refund of prepaid fees.

4.3 Urgent substitution. Where a Subcontractor must be replaced urgently to preserve the security, integrity, or continuity of the Services — including on a Subcontractor's service failure, security incident, or withdrawal of service — Business Associate may make the change without advance notice and will notify Covered Entity promptly afterwards, stating the reason. The written agreement required by Section 4.1 must be in place before the replacement creates, receives, maintains, or transmits any PHI, and Covered Entity's objection and termination rights under Section 4.2 apply equally to a change made on this basis.

4.4 Responsibility. Business Associate remains fully responsible to Covered Entity for the performance of its Subcontractors.

5. Reporting and breach notification

5.1 Reporting. Business Associate will report to Covered Entity any Use or Disclosure of PHI not permitted by this BAA, any Security Incident of which it becomes aware, and any Breach of Unsecured PHI, in accordance with this Section.

5.2 Initial notice. Business Associate will notify Covered Entity **without unreasonable delay and no later than five (5) business days** after Discovery of a

Breach of Unsecured PHI or of any Use or Disclosure not permitted by this BAA. The initial notice will state what is then known and need not be complete.

5.3 Full report. Business Associate will provide a complete report **no later than thirty (30) calendar days** after Discovery, containing, to the extent known: the identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed; a description of what happened; the date of the incident and the date of Discovery; the types of PHI involved; the steps Business Associate has taken to investigate, mitigate harm, and protect against recurrence; and any other information Covered Entity is required to include in a notification to an Individual under 45 C.F.R. § 164.404(c). Business Associate will supplement the report as further information becomes available.

5.4 Discovery. A Breach is treated as Discovered on the first day it is known to Business Associate, or by exercising reasonable diligence would have been known, in accordance with 45 C.F.R. § 164.410(a)(2).

5.5 Unsuccessful security incidents. The parties acknowledge that Business Associate's systems are subject to frequent unsuccessful attempts at unauthorized access that do not result in access to, or the Use or Disclosure of, PHI — including scans, probes, pings, denied connection attempts, and unsuccessful log-on attempts. This Section constitutes notice of such unsuccessful Security Incidents, and no further notice of them is required. Business Associate will report any Security Incident that results in unauthorized access to PHI under Sections 5.2 and 5.3.

5.6 Notification to Individuals. Covered Entity is responsible for notifying affected Individuals, the Secretary, and where applicable the media. Business Associate will not notify Individuals on Covered Entity's behalf unless Covered Entity instructs it in writing to do so, and will cooperate with and support Covered Entity's notification obligations.

5.7 Mitigation. Business Associate will mitigate, to the extent practicable, any harmful effect known to it of a Use or Disclosure of PHI in violation of this BAA.

6. Individual rights

6.1 Access. To the extent Business Associate maintains PHI in a Designated Record Set, it will make that PHI available to Covered Entity within ten (10) business days of a written request, so that Covered Entity may meet its obligations under 45 C.F.R. § 164.524. The Services also allow Covered Entity to retrieve and export this information directly at any time.

6.2 Amendment. Business Associate will make PHI in a Designated Record Set available for amendment, and will incorporate amendments directed by Covered Entity, as required by 45 C.F.R. § 164.526, within ten (10) business days of a written request.

6.3 Accounting of disclosures. Business Associate will document and, within fifteen (15) business days of a written request, make available to Covered Entity the information required for Covered Entity to respond to a request for an accounting of disclosures under 45 C.F.R. § 164.528.

6.4 Requests received directly. If Business Associate receives a request from an Individual concerning PHI, it will not respond directly. It will forward the request to Covered Entity within five (5) business days.

6.5 Restrictions and confidential communications. Covered Entity will notify Business Associate of any restriction on the Use or Disclosure of PHI agreed under 45 C.F.R. § 164.522, of any confidential communication request it has accepted, and of any change in or revocation of an Individual's authorization, to the extent any of these affects Business Associate's permitted Use or Disclosure. Notice must be sent to legal@underline.health.

6.6 Covered Entity obligations. Business Associate is not obliged to Use or Disclose PHI in a manner that would violate the HIPAA Rules if done by Covered Entity, except as permitted by Sections 2.2, 2.3, and 2.4.

7. Access by the Secretary

Business Associate will make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules. Business Associate

will notify Covered Entity of any such request unless prohibited from doing so by law.

8. Covered Entity obligations

8.1 Covered Entity will obtain any consent, authorization, or permission required by law for Business Associate to Use and Disclose PHI as contemplated by this BAA.

8.2 Covered Entity will not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

8.3 Covered Entity is responsible for the content and accuracy of the PHI it places in the Services, for its own Notice of Privacy Practices, and for its own record retention obligations.

8.4 Covered Entity will maintain appropriate safeguards over the credentials and devices used to access the Services and will promptly revoke access for workforce members who no longer require it.

9. Term and termination

9.1 Term. This BAA takes effect on the date you accept it and continues until all PHI is returned or destroyed in accordance with Section 9.4, or until the protections in Section 9.5 are extended.

9.2 Termination for cause by Covered Entity. Covered Entity may terminate this BAA and the Services if Business Associate materially breaches this BAA and fails to cure within thirty (30) days of written notice, or immediately if cure is not possible.

9.3 Termination for cause by Business Associate. Business Associate may terminate if Covered Entity materially breaches this BAA and fails to cure within thirty (30) days of written notice.

9.4 Return or destruction. On termination, Business Associate will return or destroy all PHI it maintains, including PHI held by Subcontractors, and will retain no copies. Covered Entity may export its data through the Services for thirty (30) days following termination. Business Associate will complete return or destruction **within sixty (60) days** after the end of that export period, and will confirm completion in writing on request. Requests should be sent to legal@underline.health.

9.5 Where return or destruction is infeasible. If return or destruction is infeasible, Business Associate will notify Covered Entity of the conditions making it so, will extend the protections of this BAA to that PHI for as long as it is retained, and will limit further Use and Disclosure to the purposes that make return or destruction infeasible. Retention in immutable backup media pending its scheduled expiry is an example of such a condition; that PHI remains encrypted and access-controlled and is not restored to production use.

9.6 Survival. Sections 2.6, 2.7, 5.7, 7, 9.4, 9.5, and 10 survive termination.

10. General

10.1 Regulatory references. A reference to a section of the HIPAA Rules means that section as in effect or as amended.

10.2 Amendment for compliance. The parties will take such action as is necessary to amend this BAA from time to time as required for Covered Entity to comply with the HIPAA Rules. Business Associate may amend this BAA where required by law or regulation on thirty (30) days' notice; any other amendment requires Covered Entity's acceptance.

10.3 Interpretation. Ambiguity is resolved in favour of an interpretation that permits compliance with the HIPAA Rules. In the event of a conflict between this BAA and the Terms of Use with respect to PHI, this BAA governs.

10.4 No third-party beneficiaries. Nothing in this BAA confers rights on any person other than the parties, their respective successors, and permitted assigns.

10.5 Governing law. This BAA is governed by the laws of the State of Delaware, United States, except to the extent preempted by federal law.

10.6 Notices. Notices to Business Associate under this BAA must be sent to **legal@underline.health** and are effective on receipt. Notices to Covered Entity are effective when sent to the email address on the account.

Underline.AI, Inc. legal@underline.health https://underline.health