# Business Associate Agreement — Clinitect.ai

Clinitect.ai · compliance/BAA-template.md

**Template version:** 1.0 (2026-04-24) **Pending:** legal review by Clinitect.ai counsel before first execution. **Adapted from:** HHS Sample Business Associate Agreement Provisions, 45 CFR § 164.504(e), HITECH Act amendments.

---

This Business Associate Agreement (this "**Agreement**") is entered into as of the date last signed below (the "**Effective Date**") between:

**Clinitect.ai, Inc.** (or the legal entity operating Clinitect.ai at the time of execution), a [Delaware] corporation with its principal place of business at [Address to be provided], hereafter "**Business Associate**" or "**BA**",

and

**[Customer Name]**, a [State] [entity type] with its principal place of business at [Address], hereafter "**Covered Entity**" or "**CE**".

## Recitals

WHEREAS, the parties have entered into a Services Agreement (or similar) under which BA provides services to CE that involve the use or disclosure of Protected Health Information;

WHEREAS, CE is a "Covered Entity" as defined under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), and BA is a "Business Associate" of CE as defined under HIPAA;

WHEREAS, the parties intend for this Agreement to satisfy the requirements of 45 CFR §§ 164.504(e) and 164.314(a) for Business Associate Agreements;

NOW THEREFORE, the parties agree as follows.

---

## 1. Definitions

Terms used but not defined in this Agreement have the meanings given in the HIPAA Rules (45 CFR Parts 160 and 164). Specifically, but without limitation:

- "**Breach**" has the meaning given in 45 CFR § 164.402.
- "**Designated Record Set**" has the meaning given in 45 CFR § 164.501.
- "**Electronic Protected Health Information**" or "**ePHI**" has the meaning given in 45 CFR § 160.103, limited to information that BA creates, receives, maintains, or transmits on behalf of CE.

- "**HIPAA Rules**" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and 164.
- "**Individual**" has the meaning given in 45 CFR § 160.103.
- "**Protected Health Information**" or "**PHI**" has the meaning given in 45 CFR § 160.103, limited to information that BA creates, receives, maintains, or transmits on behalf of CE.
- "**Required by Law**" has the meaning given in 45 CFR § 164.103.
- "**Secretary**" means the Secretary of the U.S. Department of Health and Human Services (HHS) or his/her designee.
- "**Security Incident**" has the meaning given in 45 CFR § 164.304.
- "**Subcontractor**" has the meaning given in 45 CFR § 160.103.

## 2. Obligations of Business Associate

### 2.1 Permitted uses and disclosures

BA may use and disclose PHI only as:

(a) necessary to perform the services set forth in the Services Agreement; (b) required by law; or (c) permitted by this Agreement.

BA will not use or further disclose PHI other than as permitted or required by this Agreement or as required by law.

### 2.2 Safeguards

BA will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Rule) with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this Agreement.

### 2.3 Minimum necessary

BA will, to the extent practicable, limit its use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose (45 CFR § 164.502(b)).

### 2.4 Reporting

BA will report to CE:

(a) Any use or disclosure of PHI not provided for by this Agreement, of which BA becomes aware, without unreasonable delay and in no event later than ten (10) business days after discovery.

(b) Any Security Incident of which BA becomes aware, in accordance with the timing in §2.4(a) above. The parties acknowledge that the ongoing, typically unsuccessful attempts to probe or scan BA's systems (e.g., pings, port scans, unsuccessful login attempts) constitute Security Incidents within the meaning of 45 CFR § 164.304, but do not require individual reporting provided BA maintains records of such attempts as part of its ordinary course of security operations and provides a summary to CE upon reasonable request.

(c) Any Breach of Unsecured PHI in accordance with 45 CFR § 164.410: without unreasonable delay and in no event later than sixty (60) calendar days after discovery (BA's internal target is seventy-two (72) hours; see Clinitect.ai Breach Notification Procedure).

Each Breach report will include, to the extent available at the time of the report: the identification of each Individual whose PHI was accessed or disclosed; a description of the nature of the event; the date of discovery; the types of PHI involved; and the remediation steps BA has taken or plans to take.

### 2.5 Subcontractors

BA will ensure that any Subcontractor to whom BA provides PHI agrees in writing to the same restrictions and conditions that apply to BA under this Agreement (45 CFR § 164.502(e)(1)(ii)).

BA represents that its current Subcontractors with access to PHI are:

- **Amazon Web Services, Inc.**, under the AWS standard Business Associate Addendum, which is in effect for all AWS services used by BA.

BA will not introduce a new Subcontractor into the PHI processing path without first ensuring that an equivalent written agreement is in place.

### 2.6 Access by Individuals

If BA maintains PHI in a Designated Record Set, BA will provide access to such PHI to CE (or, at CE's direction, to the Individual) within ten (10) business days of CE's written request, in order to enable CE to meet its obligations under 45 CFR § 164.524. BA's current architecture does not maintain customer PHI in a Designated Record Set beyond the minimum required to provide the service; any PHI stored by BA at CE's direction is retrievable for this purpose.

### 2.7 Amendments

BA will make any amendments to PHI in a Designated Record Set as directed by CE or the Individual, within thirty (30) days of CE's written request, in order to enable CE to comply with 45 CFR § 164.526.

### 2.8 Accounting of disclosures

BA will document disclosures of PHI and information related to such disclosures as would be required for CE to respond to an Individual's request for an accounting under 45 CFR § 164.528. BA will provide such information to CE within thirty (30) days of written request.

### 2.9 Access to records by the Secretary

BA will make its internal practices, books, and records available to the Secretary upon request, for purposes of determining CE's compliance with the Privacy Rule.

### 2.10 Compliance with Covered Entity obligations

To the extent BA is to carry out one or more of CE's obligations under Subpart E of 45 CFR Part 164, BA will comply with the requirements of Subpart E that apply to CE in the performance of such obligations.

### 2.11 Use of PHI by Business Associate

BA may use PHI to provide Data Aggregation services relating to the health care operations of CE (as defined in 45 CFR § 164.501) if the Services Agreement so provides. Otherwise, BA will not use PHI for any purpose other than as specifically permitted by this Agreement.

BA may use PHI for BA's own proper management and administration, and to carry out BA's legal responsibilities, provided that the use is either required by law, or BA obtains reasonable assurances from the person to whom the PHI is disclosed that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed.

### 2.12 Prohibition on use for training AI models

BA expressly warrants that it does not and will not use PHI received under this Agreement to train, fine-tune, or otherwise improve any machine learning model, whether proprietary or third-party, unless CE has provided specific, written consent for a particular use. The third-party services BA relies on (AWS Bedrock, Comprehend Medical, Textract) are contractually prohibited from using PHI for model training under the AWS Business Associate Addendum.

### 2.13 Prohibition on sale or marketing

BA will not sell PHI or use PHI for marketing purposes except as expressly permitted by HIPAA and as consented to by CE.

## 3. Obligations of Covered Entity

### 3.1 Permissible requests

CE will not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by CE (except for Data Aggregation activities as defined in 45 CFR § 164.501).

### 3.2 Restrictions

CE will notify BA of any restriction on the use or disclosure of PHI that CE has agreed to or is required to abide by, if such restriction may affect BA's use or disclosure of PHI.

### 3.3 Changes in authorization

CE will notify BA of any changes in, or revocation of, the permission by an Individual to use or disclose the Individual's PHI, if such changes affect BA's permitted or required uses and disclosures.

## 4. Term and Termination

### 4.1 Term

This Agreement becomes effective on the Effective Date and remains in effect until terminated as described below.

### 4.2 Termination for cause

Either party may terminate this Agreement if it determines that the other party has materially breached this Agreement and has failed to cure the breach within thirty (30) days of written notice. If cure is not possible, the non-breaching party may terminate immediately.

### 4.3 Termination for convenience

Either party may terminate this Agreement upon sixty (60) days' written notice to the other party.

### 4.4 Effect of termination — return or destruction of PHI

Upon termination of this Agreement, BA will, if feasible, return or destroy all PHI received from CE, or created, maintained, or received by BA on behalf of CE, that BA still maintains in any form. BA will not retain any copies of PHI, except as required by law.

If BA determines that return or destruction is not feasible, BA will extend the protections of this Agreement to the PHI and limit further uses and disclosures to those purposes that make the return or destruction infeasible, for so long as BA maintains the PHI.

BA will certify to CE, in writing, the return or destruction of the PHI (or the reasons why such return or destruction is not feasible) within thirty (30) days of termination.

## 5. Miscellaneous

### 5.1 Regulatory references

Any reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

### 5.2 Amendment

The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the parties to comply with the requirements of HIPAA and any other applicable laws.

### 5.3 Interpretation

Any ambiguity in this Agreement will be interpreted to permit compliance with the HIPAA Rules.

### 5.4 Survival

The provisions of §§ 2.4, 2.9, and 4.4 survive termination of this Agreement.

### 5.5 Entire agreement

This Agreement constitutes the entire understanding between the parties with respect to the treatment of PHI and supersedes all prior or contemporaneous agreements, whether oral or written. The terms of the Services Agreement remain in effect to the extent they do not conflict with this Agreement.

### 5.6 Governing law

This Agreement will be governed by and construed in accordance with the laws of [State — typically the state of the CE's primary operations, to be negotiated], without regard to conflicts-of-laws principles.

### 5.7 No third-party beneficiaries

Nothing in this Agreement confers any rights, benefits, or remedies on any person or entity other than the parties hereto.

---

## Signatures

**Covered Entity:**

---

Name: [Printed name] Title: [Title] Date: _____

**Business Associate (Clinitect.ai):**

---

Name: Deep Patel Title: Co-Founder and Security Officer Date: _____

---

*This Agreement was drafted from the HHS Sample BAA Provisions and reviewed by [Law Firm Name] on [Date]. Counter-signed templates are available at* `clinitect.ai/baa` *(pending domain provisioning).*

---