

BUSINESS ASSOCIATE AGREEMENT (BAA)

Version 2.1 | Last Updated: October 20, 2026

This Business Associate Agreement ("Agreement") is entered into between **OpenBots, Inc.** ("Business Associate") and the organization on whose behalf this Agreement is accepted electronically through the CoOrdio platform, as identified in the CoOrdio account at the time of acceptance ("Covered Entity"). This Agreement is effective as of the date and time it is accepted (the "Effective Date").

1. Definitions

1.1 HIPAA Rules: The Health Insurance Portability and Accountability Act of 1996, as amended, including the HITECH Act, and implementing regulations at 45 CFR Parts 160 and 164.

1.2 Protected Health Information (PHI): As defined under HIPAA, including electronic PHI ("ePHI"), limited to PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

1.3 Breach, Security Incident, Unsecured PHI: As defined under HIPAA.

1.4 Services: The CoOrdio platform and related services provided by Business Associate to Covered Entity.

1.5 Other Terms: Capitalized terms used but not defined in this Agreement have the meanings given to them in the HIPAA Rules.

2. Permitted Uses and Disclosures

2.1 Services: Business Associate may use and disclose PHI as necessary to perform the Services.

2.2 Limits: Business Associate shall not use or disclose PHI in any manner that would violate the HIPAA Rules if done by Covered Entity, except as permitted for a Business Associate under the HIPAA Rules and this Agreement.

2.3 Management and Administration: Business Associate may use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities. Business Associate may disclose PHI for these purposes only if (a) the disclosure is Required by Law, or (b) Business Associate obtains reasonable assurances from the recipient 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, and that the recipient will notify Business Associate of any instance of which it is aware in which the confidentiality of the PHI has been breached.

2.4 Required by Law: Business Associate may use or disclose PHI as Required by Law.

2.5 De-identification: Business Associate may de-identify PHI in accordance with 45 CFR 164.514(a)–(c). Information that has been de-identified in accordance with HIPAA is not PHI and is not subject to this Agreement.

2.6 No Sale or Marketing: Business Associate may not sell PHI or use PHI for marketing without written authorization as required by HIPAA.

3. Business Associate's Obligations

Business Associate shall:

3.1 Safeguards: Implement administrative, physical, and technical safeguards meeting applicable HIPAA Security Rule standards. Maintain policies, training, and access controls.

3.2 Reporting and Breach Notification: Report to Covered Entity any use or disclosure of PHI not permitted by this Agreement, any Breach of Unsecured PHI, and any Security Incident (other than an Unsuccessful Security Incident, as described in Section 3.4) of which it becomes aware, without unreasonable delay and no later than five (5) calendar days after discovery. Business Associate shall provide available information regarding the incident and supplement such information as additional details become available.

3.3 Content of Breach Notification: To the extent known and available to Business Associate, a notification of a Breach of Unsecured PHI shall include:

- (a) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed;
- (b) a brief description of what happened, including the date of the Breach and the date of discovery;
- (c) a description of the types of Unsecured PHI involved;
- (d) a description of what Business Associate is doing to investigate the Breach, mitigate harm, and protect against further Breaches; and
- (e) any other information Covered Entity reasonably requires to meet its notification obligations under 45 CFR 164.404.

3.4 Unsuccessful Security Incidents: The parties acknowledge that unsuccessful attempts to access information systems occur routinely, such as pings and other broadcast attacks on firewalls, port scans, unsuccessful log-on attempts, denials of service that do not result in a server being taken offline, and malware that is detected and neutralized ("Unsuccessful Security Incidents"), provided that no such incident results in unauthorized access, use, disclosure, modification, or destruction of PHI or interference with the operation of an information system containing PHI. This Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of Unsuccessful Security Incidents, and no further notice of such incidents is required.

3.5 Mitigation: Mitigate, to the extent practicable, any harmful effect known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement, and reasonably cooperate with Covered Entity's investigation of any such use or disclosure.

3.6 Subcontractors: Ensure that any subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to the same applicable restrictions, conditions, and requirements regarding PHI, including appropriate safeguards, as required under HIPAA.

3.7 Access, Amendments, and Accounting: To the extent applicable, make PHI in a Designated Record Set available to Covered Entity as necessary to satisfy 45 CFR 164.524, incorporate amendments to PHI as directed or agreed to by Covered Entity under 45 CFR 164.526, and maintain and provide information necessary for an accounting of disclosures under 45 CFR 164.528. Business Associate shall respond to Covered Entity's requests within five (5) business days.

3.8 Compliance Information and Audits: 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 compliance with the HIPAA Rules. Upon Covered Entity's reasonable written request, not more than once in any twelve (12) month period (except following a Breach of Unsecured PHI), Business Associate will provide Covered Entity with a copy of its most recent third-party security audit report (such as a SOC 2 report), where available, or responses to a reasonable security questionnaire, in each case subject to confidentiality obligations. On-site audits or inspections of Business Associate's facilities or systems may occur only by mutual written agreement of the parties.

3.9 Return/Destruction: Upon termination of this Agreement, comply with the return or destruction requirements set forth in Section 5.2.

3.10 Minimum Necessary: Limit PHI use/disclosure to the minimum necessary to accomplish permitted purposes, as applicable under HIPAA.

3.11 Privacy Rule Compliance: To the extent Business Associate performs any obligation of Covered Entity under the HIPAA Privacy Rule, comply with the requirements of the Privacy Rule applicable to such obligation.

4. Covered Entity's Obligations

Covered Entity shall:

4.1 Restrictions: Notify Business Associate of any restrictions on PHI use/disclosure that Covered Entity has agreed to, to the extent such restrictions may affect Business Associate's use or disclosure of PHI.

4.2 Permissible Requests: Not request Business Associate to use or disclose PHI in any manner that would violate HIPAA if done by Covered Entity.

4.3 Covered Features Only: Submit, store, or transmit PHI only through features of the Services that Business Associate has designated as covered by this Agreement, and not through any other feature, channel, or integration (including, for example, support tickets, feedback forms, or third-party integrations enabled by Covered Entity). Business Associate has no obligations under this Agreement with respect to PHI submitted in violation of this Section.

4.4 User Access: Be responsible for configuring and managing its users' accounts, roles, permissions, and access to PHI within the Services, including promptly removing access for users who no longer require it, and for safeguarding the credentials of its users.

5. Term and Termination

5.1 Term: This Agreement is effective as of the Effective Date and shall remain in effect for as long as Covered Entity uses the Services. This Agreement terminates when Covered Entity's CoOrdio account is closed or the Services otherwise end, subject to Section 5.2. The protections of this Agreement continue to apply to any PHI until it has been returned or destroyed in accordance with Section 5.2.

5.2 Effect of Termination: Upon termination of this Agreement, Business Associate shall, at Covered Entity's request made within thirty (30) days after termination, return or securely destroy all PHI received from Covered Entity or created, maintained, or received on its behalf, if feasible. If Covered Entity does not make such a request, Business Associate shall securely destroy the PHI where feasible. Business Associate will delete PHI from its active production systems within sixty (60) days after termination (or after completing any requested return). PHI residing in backup or archival systems will be destroyed in accordance with Business Associate's standard backup rotation schedule, generally within ninety (90) days after deletion from active systems; until destroyed, such PHI will remain subject to the protections of this Agreement and will not be restored or used except as necessary to complete destruction or as Required by Law. If return or destruction is infeasible, Business Associate shall extend the protections of this Agreement to retained PHI and limit further uses and disclosures to the purposes making return or destruction infeasible, for as long as such PHI is maintained.

5.3 Termination for Cause: If either party becomes aware of a material breach of this Agreement by the other party, the non-breaching party shall provide an opportunity to cure the breach or end the violation within a reasonable period, if feasible. If the breach is not cured within that period, the non-breaching party may terminate this Agreement.

6. Indemnification and Limitation of Liability

6.1 Indemnification: Each party shall be responsible for its own acts and omissions arising from a breach of this Agreement or violation of applicable HIPAA Rules. Neither party shall be required to indemnify the other except as expressly agreed in writing between the parties.

6.2 Limitation of Liability: To the maximum extent permitted by law: (a) each party's total aggregate liability arising out of or related to this Agreement, whether in contract, tort, or otherwise, shall not exceed the fees paid by Covered Entity to Business Associate for the Services during the twelve (12) months immediately preceding the event giving rise to the claim; and (b) neither party shall be liable to the other for any indirect, incidental, consequential, special, exemplary, or punitive damages, or for any lost profits, revenue, or data, arising out of or related to this Agreement, even if advised of the possibility of such damages.

7. Electronic Acceptance and Authority

7.1 Electronic Acceptance: This Agreement is accepted electronically. By clicking "I Accept" (or a similar button or checkbox), the individual accepting this Agreement agrees to it on behalf of Covered Entity. Electronic acceptance has the same legal effect as a handwritten signature under the federal Electronic Signatures in Global and National Commerce Act (E-SIGN) and applicable state laws based on the Uniform Electronic Transactions Act (UETA).

7.2 Authority: The individual accepting this Agreement represents and warrants that they have the authority to bind Covered Entity to this Agreement. An individual who does not have such authority must not accept this Agreement.

7.3 Acceptance Record: Business Associate will maintain a record of each acceptance, including the name of Covered Entity, the name and email address of the accepting individual, the date and time of acceptance, the IP address from which acceptance was made, and the version of this Agreement accepted. This record shall serve as evidence of Covered Entity's acceptance and of the Effective Date.

8. Versions and Updates

8.1 Versioning: This Agreement is identified by the version number and Last Updated date shown at the top of this Agreement.

8.2 Updates: Business Associate may update this Agreement from time to time. Business Associate will notify Covered Entity of any material update by email to Covered Entity's account administrator or by notice within the Services at least thirty (30) days before the update takes effect, unless an earlier date is required to comply with law. The updated version takes effect on the date stated in the notice. Covered Entity's continued use of the Services to create, receive, maintain, or transmit PHI after that date constitutes acceptance of the updated version. If Covered Entity does not agree to an update, it must stop using the Services to process PHI and may terminate this Agreement before the update takes effect. Each version governs the period during which it is in effect.

8.3 Automatic Amendment for Changes in Law: This Agreement shall be deemed automatically amended to the extent necessary for the parties to comply with any amendment to the HIPAA Rules, effective as of the compliance date of such amendment.

9. Miscellaneous

9.1 Governing Law: This Agreement shall be governed by and construed in accordance with the laws of the State of Delaware, except where preempted by HIPAA.

9.2 Survival: Obligations relating to PHI survive termination.

9.3 Interpretation: Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules. A reference to a section of the HIPAA Rules means that section as in effect or as amended.

9.4 No Third-Party Beneficiaries: Nothing in this Agreement confers, or is intended to confer, any rights, remedies, or obligations upon any person other than the parties and their respective successors and permitted assigns.

9.5 Severability: If any provision of this Agreement is held invalid or unenforceable, the remaining provisions shall remain in full force and effect, and the invalid or unenforceable provision shall be enforced to the maximum extent permitted by law.

9.6 Notices: Notices to Business Associate under this Agreement shall be sent by email to legal@openbots.ai. Reports of Security Incidents or suspected Breaches, and other security-related communications, shall be sent to security@openbots.ai. Notices to Covered Entity shall be sent to the email address of Covered Entity's account administrator on file in the Services, and Covered Entity is responsible for keeping that address current. Email notices are effective when sent, unless the sender receives notice of non-delivery.

BY CLICKING "I ACCEPT," YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS BUSINESS ASSOCIATE AGREEMENT, THAT YOU AGREE TO IT ON BEHALF OF THE ORGANIZATION IDENTIFIED IN YOUR COORDIO ACCOUNT, AND THAT YOU ARE AUTHORIZED TO BIND THAT ORGANIZATION TO THIS AGREEMENT.