

OpenAI Healthcare Addendum

This Healthcare Addendum (together with the BAA, this “Healthcare Addendum”) is entered into by OpenAI, LLC (“OpenAI”) and Customer as of the effective date of the OpenAI Business Terms or other agreement for services entered by OpenAI and Customer (“Services Agreement”). The Services Agreement and Healthcare Addendum together form the Agreement. Capitalized terms used but not defined in the Healthcare Addendum take their meaning from the Services Agreement.

1. **Definitions.** The following definitions shall apply for purposes of this Healthcare Addendum. Capitalized terms not defined below shall have the meanings ascribed to them under HIPAA, the BAA, or the Agreement.

“BAA” means the Business Associate Agreement attached as Exhibit A.

“Eligible Services” means (a) OpenAI’s Zero Retention API, (b) ChatGPT Enterprise and (c) any other services OpenAI explicitly identifies as Eligible Services under this Healthcare Addendum in writing from time to time. For the purposes of this Healthcare Addendum only, “Services” shall mean only the Eligible Services.

“HIPAA” means, collectively, the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 and the regulations promulgated thereunder.

“HIPAA Compliance and Implementation Guide” means the guide set forth at: <https://cdn.openai.com/osa/hipaa-compliance-and-implementation-guide.pdf>.

“HIPAA Input” means Input containing PHI that Customer transmits to OpenAI through the Eligible Services.

“HIPAA Output” means Output that OpenAI returns to Customer in response to the HIPAA Input.

“Personnel” of Customer means Customer’s employees, personnel, agents and contractors.

“Third Party Services” means any products, services, or content offered through OpenAI services by a third party. Third Party Services include, without limitation, Plugins, Actions, Third Party GPTs, and collaboration features such as shared links and templates (unless otherwise permitted in the HIPAA Compliance and Implementation Guide).

“Zero Retention API” means OpenAI’s solution for processing Customer Content without saving, retaining, or logging such content for human review. To access OpenAI’s Zero Retention API, Customer’s account must indicate that Zero Retention has been activated for the Org ID in question (each, an “Approved Org ID”).

2. **Obligations of the Parties.**

- 2.1. **Eligible Services and Implementation.** Customer (including its Personnel, Upstream Customers, End Users and other data custodians) may transmit and disclose PHI only through the Eligible Services and only in accordance with the terms and conditions of this Healthcare Addendum, including Sections 2 and 3 hereof and the HIPAA Compliance and Implementation Guide set forth at as Exhibit B. Without limiting the foregoing, Customer acknowledges and agrees that the following services are not Eligible Services and may not be used to transmit or disclose PHI: (i) Third Party Services; (ii) API use that is not through an Approved Org ID; and (iii) API use that is not to an endpoint eligible for Zero Retention (as set forth at: <https://platform.openai.com/docs/models/default-usage-policies-by-endpoint>).

- 2.2. **Customer Content.** Customer is solely responsible for: (i) the development, content, and integrity of the HIPAA Input; (ii) ensuring accurate matching (including patient matching) so that HIPAA Input is properly matched to HIPAA Output; and (iii) ensuring that HIPAA Output is returned to the appropriate Upstream Customer.

- 2.3. **Business Associate Agreement.** By executing this Healthcare Addendum, the parties agree to be bound by the BAA.

3. **Healthcare Restrictions and Requirements.**

- 3.1. **Healthcare Purposes Generally.** For any use of the Services or use or disclosure of HIPAA Output in connection with healthcare activities (including without limitation the practice of medicine, billing, coding, claims processing, or clinical research) (“Healthcare Activities”) Customer will: (i) test the Services for accuracy in Customer’s use cases and, to the extent that Customer provides any Upstream Customer with the HIPAA Output, disclose to such Upstream Customer any limitations associated with HIPAA Output; and (ii) ensure that only duly trained and qualified individuals who maintain licenses, certifications or other authorizations required to perform such Healthcare Activities will use the Services or use or disclose the HIPAA Outputs in connection with such Healthcare Activities.

- 3.2. **Upstream Customers.** Customer will enter into a written agreement with each Upstream Customer that requires such Upstream Customer to comply with all laws and regulations applicable to its use of the Services and HIPAA Output and, to the extent that Customer provides any Upstream Customer with the HIPAA Output, ensure such Upstream Customer understands and complies with Section 3.1(ii) above.

- 3.3. Transparency. Customer shall not represent, to an Upstream Customer or to any other party, that the Services were performed by a human or that HIPAA Output was human-generated.
- 3.4. Training. Customer shall train its Personnel and other relevant data custodians on its and their obligations and responsibilities relating to this Healthcare Addendum and ensure compliance therewith.
4. Disclaimers. Notwithstanding any warranties or other terms in the Agreement, and without limiting any disclaimers set forth in the Agreement, the Services and HIPAA Output are not intended to substitute for the function or services of properly trained and licensed individuals, including without limitation physicians or other clinicians, billing, coding, or claims personnel, or clinical researchers. OpenAI is not responsible or liable for any advice, course of treatment, diagnosis, or any other information or services that any patient or other individual may obtain or receive; billing, coding, or claims activities conducted by Customer or its Upstream Customers; or for the accuracy, completeness, or suitability of any data or information used in any Healthcare Activities, including clinical research activities conducted by Customer or its Upstream Customers. The Services and HIPAA Output are not intended to be used in a manner that constitutes a medical device.
5. Limitation of Liability. Notwithstanding anything to the contrary in the Agreement, (i) except for any breach of Sections 2 (Obligations of the Parties) or 3 (Healthcare Restrictions and Requirements), neither party will be liable under this Healthcare Addendum for any indirect, punitive, incidental, special, consequential, or exemplary damages (including damages for loss of profits, revenue, customers, or data; business interruption; or costs of procuring substitute technology or services), even if such party has been advised of the possibility of such damages, and (ii) OpenAI's total aggregate liability under this Healthcare Addendum shall be capped at the greater of one million dollars (\$1,000,000) or three times (3x) the total amount paid (and payable) by Customer to OpenAI in the twelve (12) month period prior to the date of the claim. The foregoing limitations will apply notwithstanding any failure of essential purpose of any limited remedy and to the maximum extent permitted under applicable law.
6. Term and Termination. This Healthcare Addendum shall remain in full force and effect for as long as the Agreement remains in effect, unless otherwise terminated. The termination provisions set forth in the Agreement shall apply equally to this Healthcare Addendum. If this Healthcare Addendum expires or is terminated for any reason, Customer shall not, and shall ensure that its Upstream Customers do not, transmit or otherwise disclose PHI to OpenAI by any means or methods. Upon termination or expiration of this Healthcare Addendum, any provision of this Healthcare Addendum that (a) expressly states that it survives beyond the Term or (b) should survive following the Term to fulfill its essential purpose, will survive.
7. General. A reference in this Healthcare Addendum to a regulatory section means the section as in effect or as amended. In addition, any notification required in this Healthcare Addendum to be made to OpenAI (or that is otherwise provided to OpenAI in connection with this Healthcare Addendum) shall also be sent to hipaa@openai.com. The recitals and exhibits to this Healthcare Addendum are hereby incorporated by reference into this Healthcare Addendum and made a binding part of this Healthcare Addendum. The Agreement shall remain in full force and effect and, except as modified by this Healthcare Addendum, applies equally to this Healthcare Addendum, which is hereby incorporated by reference into the Agreement and made a binding part of the Agreement. In the event of a conflict between this Healthcare Addendum and the Agreement, this Healthcare Addendum shall prevail with respect to the subject matter of this Healthcare Addendum.

Exhibit A

Business Associate Agreement

1. Purpose. OpenAI and Customer entered the Healthcare Addendum, pursuant to which OpenAI provides Customer access to certain OpenAI products and services that implicate HIPAA. For purposes of the Healthcare Addendum, Customer is either a Covered Entity, or a Business Associate of its Upstream Customers. OpenAI is either a Subcontractor of Customer, or a Business Associate of Customer.
2. Definitions. The following definitions shall apply for purposes of this Business Associate Agreement.
 - “Business Associate” has the same meaning as the term “Business Associate” in 45 C.F.R. § 160.103.
 - “Covered Entity” has the same meaning as the term “covered entity” in 45 C.F.R. § 160.103.
 - “HIPAA Breach Notification Rule” means the Breach Notification for Unsecured Protected Health Information regulations, codified at 45 C.F.R. parts 160 and 164, as amended.
 - “HIPAA Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. parts 160 and 164, as amended.
 - “HIPAA Security Rule” means the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. parts 160 and 164, as amended.
 - “Protected Health Information” or “PHI” has the same meaning as under HIPAA, limited to such information that OpenAI receives from Customer.
 - “Required by Law” has the same meaning as the term “required by law” in 45 C.F.R. § 164.103.
 - “Security Incident” has the same meaning as the term “security incident” in 45 C.F.R. § 164.304.
 - “Subcontractor” has the same meaning as the term “subcontractor” in 45 C.F.R. § 160.103.
 - “Unsecured Protected Health Information” or “Unsecured PHI” have the same meaning as under the HIPAA Breach Notification Rule, limited to such information that OpenAI receives from Customer.
 - “Upstream Customer” is a customer of Customer that is either a Covered Entity or Business Associate.
3. OpenAI Requirements and Obligations.
 - 3.1. Prohibited Uses and Disclosures of PHI. OpenAI shall not use or disclose PHI other than as permitted or required by this BAA or the Agreement, or as Required by Law. OpenAI may not use or disclose PHI in a manner that would violate the HIPAA Privacy Rule if done by Customer or its Upstream Customers that are Covered Entities, except as provided in this BAA.
 - 3.2. Permissible Use and Disclosure of PHI. OpenAI is permitted to collect, receive, use, maintain, create, disclose, transmit, destroy, and otherwise process PHI (i) in connection with performing its obligations and exercising its rights under the Agreement, (ii) as permitted or required by this BAA, (iii) as Required by Law, (iv) as authorized by an Individual, and (v) as otherwise permitted by applicable law. OpenAI may use PHI for the proper management and administration of OpenAI or to carry out the legal responsibilities of OpenAI. OpenAI may disclose PHI for the proper management and administration of OpenAI or to carry out the legal responsibilities of OpenAI, provided the disclosures are Required by Law, or OpenAI obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and be used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies OpenAI of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.
 - 3.3. Minimum Necessary. To the extent that OpenAI uses, discloses, or requests PHI to provide the Services, OpenAI shall use reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, unless an exception to the minimum necessary requirements under HIPAA applies. Notwithstanding anything to the contrary, the parties acknowledge and agree that all PHI that is transmitted to OpenAI is the minimum necessary required by OpenAI to perform its obligations and exercise its rights under the Agreement.
 - 3.4. Incident Reporting. OpenAI will report to Customer (i) any use or disclosure of PHI by OpenAI that is not permitted under this BAA of which OpenAI becomes aware, including Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410, and (ii) any Security Incident of which OpenAI becomes aware. Any such report(s) must be made promptly after discovery by OpenAI of such impermissible use or disclosure, such Security Incident, or such Breach of Unsecured PHI. OpenAI will provide such reasonable cooperation as is reasonably requested by Customer in

responding to such event and will supplement such initial report with additional information, including all information reasonably available to OpenAI that is required to be included in notices to affected Individuals, regulators, the media, or other entities as required by HIPAA or applicable state laws. The parties agree that notice is hereby deemed given for all attempted, unsuccessful Security Incidents involving trivial and routine incidents such as port scans, attempts to log-in with an invalid password or user name, denial of service attacks that do not result in a server being taken off-line, malware, and pings, or other similar types of events that do not compromise the security or privacy of PHI.

- 3.5. Mitigation. OpenAI will take reasonable steps to mitigate, to the extent practicable, any harmful effects known to OpenAI from any unauthorized use or disclosure of PHI by OpenAI in violation of HIPAA or this BAA.
 - 3.6. Subcontractors of OpenAI. OpenAI shall ensure that any Subcontractors of OpenAI that create, receive, maintain, or transmit PHI agree to the same restrictions and conditions that apply to OpenAI with respect to such information, to the extent required by HIPAA. If OpenAI learns of any pattern or activity that constitutes a material breach of a Subcontractor's obligations with respect to PHI, OpenAI will take reasonable steps to cure the breach, end the violation, or terminate the relationship with its Subcontractor.
 - 3.7. Requests for Access. The parties acknowledge and agree that OpenAI does not maintain a Designated Record Set for or on behalf of Customer or Upstream Customers. In the event that OpenAI receives a request for access to PHI under 45 C.F.R. § 164.524, OpenAI's sole responsibility shall be to promptly forward the request to Customer. If Customer or any Upstream Customer receives a request for access to PHI under 45 C.F.R. § 164.524, OpenAI shall have no obligations.
 - 3.8. Requests for Amendment. The parties acknowledge and agree that OpenAI does not maintain a Designated Record Set for or on behalf of Customer or Upstream Customers. In the event that OpenAI receives a request for amendment of PHI under 45 C.F.R. § 164.526, OpenAI's sole responsibility shall be to promptly forward the request to Customer. If Customer or any Upstream Customer receives a request for amendment of PHI under 45 C.F.R. § 164.526, OpenAI shall have no obligations.
 - 3.9. Accounting of Disclosures. If OpenAI discloses PHI in a manner that is required to be included in an accounting under 45 C.F.R. § 164.528, OpenAI shall maintain and, within ten (10) business days of a request from Customer, make available such information as Customer or Upstream Customer would be required to provide an Individual requesting an accounting of disclosures under 45 C.F.R. § 164.528.
 - 3.10. Customer Privacy Rule Obligations. The parties acknowledge and agree that OpenAI is not intended to carry out one or more of Customer's or any of Upstream Customer's obligation(s) under the HIPAA Privacy Rule.
 - 3.11. Availability of Books and Records. OpenAI will make its HIPAA policies and any other books and records that relate to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services (or his or her designee) for purposes of determining compliance with HIPAA.
 - 3.12. Privacy and Security Safeguards. OpenAI shall use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule (as codified in 45 C.F.R. §§ 164.302-164.318) with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this BAA.
4. Customer Restrictions and Obligations.
- 4.1. Compliance with Upstream Customer Business Associate Agreements. Customer shall comply with the terms and conditions of Customer's business associate agreements (entered into pursuant to 45 C.F.R. §§ 164.502(e), 164.504(e), 164.308(b), and 164.314(a)) with its Upstream Customers that are relevant to the Services.
 - 4.2. Upstream Customer Limitation(s) in Notice of Privacy Practices. Customer shall ensure that there are no limitation(s) in its own notice of privacy practices and that of any Upstream Customer under 45 C.F.R. § 164.520 that may affect OpenAI's use or disclosure of PHI pursuant to the Agreement.
 - 4.3. Permissions, Authorizations, and Consents. Customer represents and warrants that any permissions, authorizations (including authorizations under 45 C.F.R. § 164.508), or consents that may be required for OpenAI to provide Services, or to otherwise collect, receive, use, maintain, create, disclose, transmit, destroy, or otherwise process PHI as permitted or required under this BAA, have been obtained and reasonably documented.
 - 4.4. Restrictions on the Use and Disclosure of PHI. Customer shall ensure that Customer and Upstream Customers have not agreed to, or are not otherwise required to abide by, restrictions on the use or disclosure of PHI under 45 C.F.R. § 164.522 that may affect OpenAI's use or disclosure of PHI pursuant to the Agreement.
 - 4.5. Permissible Requests by Customer. Customer shall not ask OpenAI to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by Customer or any Upstream Customer. Customer shall

not request that OpenAI collect, receive, use, maintain, create, disclose, transmit, maintain, destroy, or otherwise process PHI in any manner that violates HIPAA or any other applicable law or regulation.

- 4.6. Mitigation. Customer shall take reasonable steps to mitigate, to the extent practicable, any harmful effects known to Customer of a breach of this BAA by Customer.
5. Term and Termination. The term of this BAA shall begin on the first date Customer transmits PHI to OpenAI pursuant to the Agreement and shall continue for as long as the Healthcare Addendum remains in effect. The Healthcare Addendum, including this BAA, may be terminated in accordance with Section 6 of the Healthcare Addendum. Following termination or expiration of this BAA for any reason, upon Customer's written request, OpenAI shall certify that all PHI has been returned or destroyed.
6. General. Except as modified by this BAA, the Healthcare Addendum applies equally to this BAA. In the event of a conflict between this BAA and the Healthcare Addendum, this BAA shall prevail with respect to the subject matter of this BAA.