OpenAI

OpenAI Business Associate and Healthcare Addendum
Effective: September 28, 2026

This Business Associate and Healthcare Addendum and (the "BAA") is entered into by OpenAI OpCo, LLC ("OpenAI") and the applicable healthcare provider or customer ("Customer") that has entered into an order form referencing this BAA or has otherwise accepted this BAA in connection with its purchase of the Eligible Services (as defined below). This BAA is governed by the OpenAI Services Agreement or other agreement for services entered by OpenAI and Customer ("Services Agreement") and applies to the Eligible Services only. The Services Agreement and BAA together form the Agreement. Capitalized terms used but not defined in the BAA take their meaning from the Services Agreement or HIPAA.

1. General.

   1.1. Background. OpenAI and Customer are entering into this BAA pursuant to which OpenAI provides Customer access to certain Eligible Services through which Customer may create, receive, transmit, or maintain PHI. For purposes of the BAA, 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.

   1.2. 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 BAA and the HIPAA Guide. Customer acknowledges and agrees that not all Services offered by OpenAI are Eligible Services and Customer represents and warrants that it will not transmit or disclose PHI to OpenAI through any Service other than the Eligible Services. For clarity, the following services are not Eligible Services and may not be used to transmit or disclose PHI: (i) the OpenAI API Services without Modified Retention enabled, unless otherwise specified by OpenAI in writing; (ii) ChatGPT Free, Plus, Pro, or Business; and (iii) any Beta Services, unless otherwise specified by OpenAI. Third Party Services are not Eligible Services covered by this BAA. Customer is responsible for ensuring its use of any Third Party Services complies with HIPAA.

   1.3. Updates. OpenAI may update this BAA by providing Customer with reasonable notice, including by posting the updated BAA at the provided URL. If OpenAI determines in its discretion that an update materially impacts Customer's rights or obligations, OpenAI will provide Customer at least thirty days' notice before the update is effective, unless the update is necessary for OpenAI to comply with applicable law, in which case OpenAI will provide Customer with as much notice as reasonably possible. Any other updates will be effective on the date OpenAI posts the updated BAA. Customer's continued use of, or access to, the Services after an update is effective constitutes acceptance of the update.

2. Use and Disclosure of PHI.

   2.1. 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 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.

   2.2. Management and Administration. OpenAI may use and disclose PHI for the proper management and administration of OpenAI or to carry out the legal responsibilities of OpenAI, provided any 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.

   2.3. 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.

   2.4. Use for Reporting of Violations. OpenAI may use PHI to report violations of law to appropriate federal and state authorities, consistent with applicable HIPAA requirements.

   2.5. 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. Safeguards and Reporting

3.1. 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.

3.2. 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; (ii) 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 reasonably cooperate with 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 Unsuccessful Security Incidents.

3.3. 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.

4. 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.

5. Access, Amendment, and Disclosures

5.1. Requests for Access. The parties acknowledge and agree that OpenAI does not maintain PHI as a designated record set for or on behalf of Customer or Upstream Customers. If 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.

5.2. Requests for Amendment. The parties acknowledge and agree that OpenAI does not maintain PHI as a Designated Record Set for or on behalf of Customer or Upstream Customers. If 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.

5.3. 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.

6. 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.

7. Responsibilities of Customer.

7.1. 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.

7.2. 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. Customer will notify OpenAI of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect OpenAI's use or disclosure of PHI, provided that Customer will be responsible for adjusting its use of the Services in order to comply with such change or revocation.

7.3. 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.

7.4. 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.

7.5. 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.

8. Healthcare Restrictions and Requirements.

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

8.2. Healthcare Activities. For any use of the Services or use or disclosure of Health Output in connection with 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 Health Output, disclose to such Upstream Customer any limitations associated with Health 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 Health Outputs in connection with such Healthcare Activities.

8.3. 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 Health Output and, to the extent that Customer provides any Upstream Customer with the Health Output, ensure such Upstream Customer understands and complies with Section 8.2(ii) above.

8.4. Transparency. Customer shall not represent, to an Upstream Customer or to any other party, that the Services were performed by a human or that Health Output was human-generated.

8.5. Training. Customer shall train its Personnel and other relevant data custodians on its and their obligations and responsibilities relating to this BAA and ensure compliance therewith.

8.6. Disclaimers. Notwithstanding any warranties or other terms in the Services Agreement, and without limiting any disclaimers set forth in the Services Agreement, the Eligible Services and Health 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 Health Output are not intended to be used in a manner that constitutes a medical device.

8.7. State Law Requirements. Some state health information privacy and sensitive condition laws and other federal laws are more restrictive than HIPAA or impose additional requirements on the use and disclosure of identifiable health information. Customer is responsible for confirming that its use of the Services is consistent with applicable state and federal laws. By using the Services for processing or maintaining identifiable health information, Customer represents that: (i) such use, and disclosure of information to OpenAI through the Services, complies with applicable state and federal laws; and (ii) Customer has obtained all necessary consents, authorizations and permissions required by applicable law to share information with OpenAI in connection with the Services.

9. Term and Termination.

9.1. Term. The term of this BAA shall begin on the first date Customer transmits Health Input to OpenAI pursuant to the Agreement and shall continue until terminated as set forth in this BAA.

9.2. Termination. Either Party may immediately terminate this BAA, the Services Agreement, and any other related agreements if such Party makes a determination that the other Party has breached a material term of this BAA and has failed to cure that material breach within 30 days after written notice from the non-breaching Party. Without limiting the foregoing, the termination provisions set forth in the Services Agreement shall apply equally to this BAA.

9.3. Effect of Termination. If this BAA expires or is terminated for any reason, Customer shall not transmit or otherwise disclose, and shall ensure that its End Users and Upstream Customers do not transmit or otherwise disclose, PHI to OpenAI by any means or methods. Following termination or expiration of this BAA for any reason, OpenAI will return or destroy any PHI maintained by OpenAI within a reasonable period and, upon Customer's written request, OpenAI shall certify that all PHI has been returned or destroyed. If return or destruction of the PHI is not feasible, in OpenAI's reasonable judgment, OpenAI will extend the protections of this BAA to such information for as long as OpenAI retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible.

10. Limitation of Liability. Except for any breach of Section 1.2 (Eligible Services and Implementation) of the BAA or Section 8 (Healthcare Restrictions and Requirements), this BAA will be subject to the limitations of liability in the Services Agreement. The foregoing limitations will apply notwithstanding any failure of essential purpose of any limited remedy and to the maximum extent permitted under applicable law.

11. General. A reference in this BAA to a regulatory section means the section as in effect or as amended. In addition, any notification required in this BAA to be made to OpenAI (or that is otherwise provided to OpenAI in connection with this BAA) shall also be sent to hipaa@openai.com. The recitals and exhibits to this BAA are hereby incorporated by reference into this BAA and made a binding part of this BAA. The Services Agreement shall remain in full force and effect and, except as modified by this BAA, applies equally to this BAA, which is hereby incorporated by reference into the Services Agreement and made a binding part of the Services Agreement. In the event of a conflict between this BAA and the Services Agreement, this BAA shall prevail with respect to the subject matter of this BAA.

12. Definitions. The following definitions shall apply for purposes of this BAA. Capitalized terms not defined below shall have the meanings ascribed to them under HIPAA or the 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.

    "Eligible Services" means the eligible Services identified in Exhibit 1 attached to this BAA. For the purposes of this BAA only, "Services" shall mean only the Eligible Services.

    "Health Input" means Input containing PHI or other input related to Healthcare Activities that Customer transmits to OpenAI through the Eligible Services.

    "Health Output" means Output that OpenAI returns to Customer in response to the Health Input.

    "Healthcare Activities" means use of the Eligible Services in connection with healthcare activities, including without limitation the practice of medicine, billing, coding, claims processing, or clinical research.

    "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 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 Guide" means the implementation and configuration guide available at https://cdn.openai.com/osa/baa-hipaa-guide.pdf.

    "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.

    "Modified Retention" has the meaning given in the HIPAA Guide.

    "Personnel" of Customer means Customer's employees, personnel, agents and contractors.

    "Protected Health Information" or "PHI" has the same meaning as under HIPAA, limited to such information that OpenAI receives from Customer.

    "Regulated Workspace" means the preconfigured ChatGPT Enterprise or ChatGPT Edu workspace with the features listed at https://cdn.openai.com/osa/chatgpt-regulated-workspace.pdf.

    "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.

    "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, Web Search, Apple Intelligence and other connected third party applications, and collaboration features such as shared links and templates (unless otherwise permitted in the HIPAA Guide).

    "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.

"Unsuccessful Security Incidents" means attempted but 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.

"Upstream Customer" is a customer of Customer that is either a Covered Entity or Business Associate.

OpenAI

Exhibit 1: Eligible Services

Eligible Services	Notes
OpenAI API Services	• Customer must have accepted the BAA within their Account and, unless otherwise specified by OpenAI, Customer's account must be provisioned with a Modified Retention feature. • Customer may only use the HIPAA Endpoints listed at https://help.openai.com/en/articles/20001069
Specified ChatGPT Services	• Customer must have accepted the BAA within their Account or via an Order Form. • Only the ChatGPT Services and features accessible through ChatGPT listed at https://help.openai.com/en/articles/20001069 are Eligible Services (including, ChatGPT Enterprise or Edu with the Regulated Workspace, ChatGPT for Healthcare, and ChatGPT for Clinicians)