OpenAI

HIPAA Implementation and Configuration Guide

Posted: March 27, 2026

This HIPAA Implementation and Configuration Guide ("HIPAA Guide") is part of the Business Associate and Healthcare Addendum and (the "BAA") between Customer and OpenAI. If you do not have a BAA with OpenAI, you may not use the Services with Protected Health Information. Capitalized terms used but not defined in this HIPAA Guide take their meaning from the BAA or Services Agreement. We may update or revise this HIPAA Guide from time to time, including to provide guidance for new features or services as they are released.

Overview

This HIPAA Guide provides general guidance regarding certain features to consider as Customer configures and uses the Eligible Services consistent with its HIPAA compliance obligations and risk analysis. The information in this HIPAA Guide does not constitute legal advice and adhering to this guidance does not ensure compliance or alignment with your specific HIPAA obligations. Customers are responsible for independently evaluating their own specific use of the Eligible Services as appropriate to support their legal compliance obligations, as the recommendations in the HIPAA Guide are for certain minimum product configurations and are not exhaustive. Please note this HIPAA Guide does not apply if you are using ChatGPT for Healthcare or ChatGPT Enterprise or Edu with the Regulated Workspace. If you use ChatGPT for Healthcare or ChatGPT Enterprise or Edu with the Regulated Workspace please review the guide available here.

General Implementation Guide

1. Users. Customer may not create End User Accounts directly on the OpenAI Services for patients, plan members, or their families or employer.
2. Support Requests. When initiating a support request to OpenAI through any means, Customer and its End Users may not include any PHI in the support request or attach any screenshots or documents that include PHI.
3. Designated Record Sets. Customer and its End Users may not use the Eligible Services to maintain PHI as a part of a designated record set (as defined in HIPAA).
4. Access Management. Customer is responsible for configuring use of single sign-on ("SSO") to manage access and authorization and for implementing other access management requirements for End Users when accessing the Services. Please see OpenAI's help articles regarding SSO for more information.
5. Mobile Device Management. Customer, and not OpenAI, is responsible for securing devices that are used to access the Services in accordance with HIPAA. The Services do not control the encryption, geolocation, remote wiping or other helpful or required security features of devices under HIPAA. OpenAI may store some data (such as message edits in progress) locally on a device running the OpenAI app or browser session. If Customer requires encryption of PHI at rest, Customer should encrypt all devices that run OpenAI applications or browser sessions.
6. Monitoring. Customer is responsible for implementing its own tools and processes for monitoring End Users' use of the Services.
7. Data Backup and Emergency Access. Customer is responsible for implementing backup and recovery procedures for emergency access and archival of PHI.
8. Multiple Covered Entity Data. OpenAI allows HIPAA-regulated customers to use the Eligible Services to manage the PHI of multiple Covered Entities. Customer is responsible for ensuring it has all necessary permissions and approvals, including from all relevant HIPAA-regulated entities, to use the Eligible Services for PHI. If, while using the Services, Customer no longer has permission to use one or more Covered Entity's data, Customer is responsible for deleting all Customer Content, including conversations and uploaded files, that contain that Covered Entity's PHI.

OpenAI API

1. Applicability. This portion of the HIPAA Guide applies if Customer has a BAA that includes OpenAI API Services as Eligible Services in the BAA. If Customer's BAA does not expressly specify OpenAI API Services are Eligible Services, Customer may not upload, transmit, or process PHI with the OpenAI API Services.

2. Modified Retention. Use of the OpenAI API Services in connection with this BAA is contingent on Customer's account being provisioned for a Modified Retention feature.

   2.1. Limited Use. Unless Customer has signed separate Modified Retention Terms, Customer must use Modified Retention with HIPAA Input and HIPAA Output only. If Customer wants to use Modified Retention for other use cases, Customer must submit these use cases to OpenAI in writing for review and approval and enter into Modified Retention Terms governing these additional use cases. If Input or Output ceases to include HIPAA Input or HIPAA Output, Customer will promptly inform OpenAI and submit the updated use case for review and approval.

   2.2. Activation. In order to transmit HIPAA Input to the API Services, Customer's account must show that a Modified Retention feature is activated for the associated Org ID and Project in the Account Console. If Customer has multiple Org IDs, Modified Retention must be activated separately for each Org ID. If Customer wishes to add additional Org IDs after execution of this Amendment, Customer must submit a written request to OpenAI identifying the Org IDs and Customer may be required to sign a written confirmation identifying each Org ID to document activation. Customer is responsible for ensuring all HIPAA Input for HIPAA Endpoints is transmitted only using Org IDs and Projects that have Modified Retention active.

   2.3. Platform Abuse. OpenAI may perform Safety Classification and generate Safety Classifiers that OpenAI retains for safety purposes, provided that the Safety Classifiers will not contain Customer Content. OpenAI may retain Safety Classifiers indefinitely. In the event the Safety Classifiers indicate persistent or material violations of law or OpenAI Policies, or OpenAI reasonably suspects that Customer is in violation of this provision, OpenAI may suspend or revoke approval for Modified Retention and terminate this BAA upon notice to Customer, suspend Customer's access to the Services, or take other action in its sole discretion. If OpenAI notifies Customer that its access to Modified Retention will be revoked or suspended, then Customer will cease, and will cause its users to cease, all transmissions, uploads, and communications of PHI through the API Services.

3. Definitions.

   "HIPAA Endpoints" means the endpoints listed at https://cdn.openai.com/osa/hipaa-endpoints.pdf.

   "Modified Abuse Monitoring" means that Customer Content will not be logged for abuse monitoring and human review for any API endpoint as specified and subject to the limitations at https://platform.openai.com/docs/guides/your-data. Customer may still save or retain Customer Content in the Services for application state, as configured by Customer.

   "Modified Retention" means, as applicable, Modified Abuse Monitoring or Zero Data Retention.

   "Modified Retention Terms" means an amendment, addendum, or other terms entered into by the Parties governing Customer's access to and use of endpoints with Modified Retention as specified here.

   "Org ID" means the organization identifier associated with Customer's account.

   "Project" means an API project created by Customer through the administrative functionality of the Services.

   "Safety Classification" means automated screening of the Customer Content for safety purposes.

   "Safety Classifier" means metadata (including classifier types, dates, counts, and confidence scores) that are generated by the Safety Classification process, excluding Customer Content (including summarizations of Customer Content) or any portion thereof.

   "Zero Data Retention" means that Customer Content (a) will not be logged for human review and (b) will not be saved to disk or retained by OpenAI when using the ZDR Endpoints and subject to the limitations, at https://platform.openai.com/docs/guides/your-data. If Customer uses an endpoint or Input type that is not eligible for Zero Data Retention, OpenAI will not log data, but data may be retained for application state.

   "ZDR Endpoints" means the endpoints eligible for Zero Data Retention, as specified at https://platform.openai.com/docs/guides/your-data.

ChatGPT Enterprise and Edu Configuration Guide.

1. Applicability. This portion of the HIPAA Guide applies if Customer has a BAA that includes the ChatGPT Enterprise or Edu Services as Eligible Services in the BAA. If Customer's BAA does not expressly specify ChatGPT Enterprise or Edu are

Eligible Services, Customer may not upload, transmit, or process PHI with the ChatGPT Enterprise and Edu Services. For clarity, ChatGPT Services for consumers (e.g., Free, Plus, Pro) and ChatGPT Business are not Eligible Services. Early access features when available in the workspace do not support HIPAA compliance and should not be used with PHI.

2. Adding Users. Before inviting a new End User to Customer's enterprise workspace, Customer should confirm that the End User is a part of its organization and is authorized to access PHI. Customer is responsible for ensuring that its organization members are familiar with the requirements in the BAA and this HIPAA Guide, as applicable, before provisioning access to them.

3. Data Retention. Unless earlier deleted by an End User or unless Customer has selected a shorter retention period, OpenAI will maintain Customer Content for the term of the Services Agreement. Customer is responsible for removing any data that needs to be removed using self-service tools provided in the Services, such as the ability to delete conversations.

4. PHI-Prohibited Fields. Customer and its End Users may not include PHI in any of the following:

   4.1. User profile data, including:

      a. Name

      b. Email Address

   4.2. Workspace name and image

   4.3. Support tickets or any other support requests

5. Workspace Settings. The workspace Permissions & roles and Apps & Connectors menus enable Customer to manage the following functionalities of Customer's ChatGPT workspace. Customer is solely responsible for evaluating and configuring its account in a way consistent with its HIPAA obligations and as set forth in this HIPAA Guide. Customer is solely liable for any breach of HIPAA arising out of its failure to disable any of the following features.

   5.1. Unsupported Features. The following features have not been evaluated by OpenAI for HIPAA compliance at this time and may not be used with PHI. It is recommended that Customer disable these functionalities.

      a. Codex - Customer can disable this functionality through the "Codex Local" and "Codex Cloud" toggles.

      b. Memories - Customer can disable this functionality through the "Memory" toggle.

      c. Search Agent mode - Customer can disable this functionality through the "Search>Agent mode toggle".

      d. ChatGPT Atlas - Customer can disable this functionality through the "ChatGPT Atlas" toggle.

   5.2. Features that Permit Transmission of Data. The following features may involve transmitting information to a third party that does not offer HIPAA-enabled Services. It is recommended that Customer disable these functionalities.

      a. Apps & Connectors- Apps & Connectors can involve transmitting information to third parties that do not offer HIPAA-enabled services as configured by Customer. Customer can disable individual connectors and apps functionality through the "Connectors & Apps" menu.

      b. Search and Deep Research - The use of the web browsing capabilities can involve transmitting information to third-party search providers and may not be used with PHI. Customer can disable these functionalities through the "Web search" toggle.

      c. Canvas code network access - Code execution and React/HTML rendering can result in external network requests to be made and may not be used with PHI. Customer can disable this functionality through the "Canvas code network access" toggle..

      d. Code on macOS - ChatGPT functionality to allow code edits (other other app connections) on macOS or enabling Apple Intelligence can involve transmitting information to outside of the ChatGPT workspace or third-parties that do not offer HIPAA-enabled services. Customer can disable these functionalities through the respective toggles on "Code on macOS".

      e. Third-Party GPTs. The use of GPTs developed by third parties can involve transmitting information to third parties that do not offer HIPAA-enabled services. If Customer enables this functionality, Customer is solely responsible for implementing internal policies with respect to review and use of each third-party GPT in accordance with its legal obligations under HIPAA. Customer can choose to disable this functionality by

selecting “Allow all third party GPTs - Don’t Allow” under “Third Party GPTs.”

5.3. Sharing. The Sharing, GPT and Project settings allow Customer to control how End Users can share their content within the workspace, including chats, projects, and GPTs. Customer is solely responsible for evaluating and configuring these tools in accordance with its legal obligations under HIPAA. For example, Customer should only choose to enable sharing with workspace members if it has made the determination that all End Users of its workspace are authorized to access any PHI shared over chats, projects or GPTs.