OpenAI

HIPAA Implementation and Configuration Guide

Posted: July 9, 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.

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 currently requires Customer's account being provisioned for a Modified Retention feature. Unless Customer has signed separate Modified Retention Terms

OpenAI may, in its discretion: (a) select the Modified Retention feature to apply; and (b) disable Modified Retention if it is no longer required for the BAA. To the extent Modified Retention remains required, the following terms apply.

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. In the event the Safety Classifiers indicate persistent or material violations of law, the Services Agreement, 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.

"Eyes Off" means that customer content will be retained in abuse monitoring logs and may be retained for application state, but such content will be excluded from human review unless required by applicable law for any API endpoint as specified and subject to the limitations at https://platform.openai.com/docs/guides/your-data.

"HIPAA Endpoints" means the endpoints listed at https://help.openai.com/en/articles/20001069-hipaa-eligible-products-and-functionality.

"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, Zero Data Retention, Safety Retention, or Eyes Off.

"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 or security 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.

"Safety Retention" means that Customer Content will not be logged for abuse monitoring and human review, unless OpenAI classifiers detect the Customer Content as potentially violating the OpenAI Policies or the Agreement (including Sections 3.3(d)-(f) therein) or as required by law, 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.

"Zero Data Retention" means that Customer Content (a) will not be logged for human review and (b) will not be 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

1. Applicability. This portion of the HIPAA Guide applies if Customer has a BAA that includes ChatGPT for Healthcare, ChatGPT for Clinicians, ChatGPT Enterprise / Education with the Regulated Workspace, or any other ChatGPT service identified as an Eligible Service in the BAA. If Customer is not using an Eligible Service, Customer may not upload, transmit, or process PHI with ChatGPT. For clarity, ChatGPT services for consumers (e.g., Free, Plus, Pro) and ChatGPT Business are not Eligible Services.
2. Limitations. When Customer uses the ChatGPT Eligible Services, Customer agrees that the Services will have preconfigured settings that may limit access to certain features that do not support HIPAA compliance. The current set of available features is available here. OpenAI may update that link to add additional features when available. Early access features when available in the workspace do not support HIPAA compliance and should not be used with PHI.
3. Adding Users. Before inviting a new End User to Customer's 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.
4. 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.
5. PHI-Prohibited Fields. Customer and its End Users may not include PHI in any of the following:
    5.1. User profile data, including:
        a. Name
        b. Email Address
    5.2. Workspace name and image
    5.3. Support tickets or any other support requests
6. Workspace Settings. The workspace Permissions & roles menu enables Customer to manage the following functionalities of the Eligible Services. Customer is solely responsible for evaluating and configuring the Eligible Services in a way consistent with its HIPAA obligations.
    6.1. Code on macOS - ChatGPT functionality to allow code edits (other other app connections) on macOS can involve transmitting information to outside of the ChatGPT workspace. Customer can disable these functionalities through the respective toggle on "Code on macOS".
    6.2. Sharing. 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 in conversations, projects or GPTs.

Codex Local

1. Applicability. This portion of the HIPAA Guide applies to Customer's use of Codex Local through either the API or using their account for ChatGPT Eligible Services. Codex Local involves installation of Codex Local Client on a local workstation. When the Codex Local Client transmits PHI to OpenAI for processing, OpenAI will protect the Customer PHI consistent with the BAA subject to the requirements below.
    1.1. API. Customer's use of Codex Local with a Customer-provided OpenAI API key for the OpenAI API Services will be covered by the BAA only if Customer has entered into a BAA with OpenAI that includes the API Services as an Eligible Service. The BAA will apply to the processing of PHI by the OpenAI API services in accordance with the "OpenAI API" section above.

1.2. Codex Local and ChatGPT. Customer use of Codex Local with Codex SiWC will be covered by the BAA only if the Codex Local workplace setting in Customer's ChatGPT account indicates that Codex Local is HIPAA-eligible. Customer must contact their Account Director to enable HIPAA coverage for Codex Local via Codex SiWC.

2. Customer Responsibility. The OpenAI BAA does not apply to the execution of the Codex Local Client on Customer's client machines or to any Third-Party Services accessed by the Codex Local Client due to Customer's use or instructions. Customer is responsible for evaluating the Codex Local Client installation, its operating environment, and establishing a managed configuration that meets their requirements for use with PHI. For more information on deploying Codex in your organization see https://developers.openai.com/codex/enterprise/admin-setup. For Codex Local configuration options see https://developers.openai.com/codex/enterprise/managed-configuration and our Codex Whitepaper on our Trust Portal at trust.openai.com.

3. Exclusions. Codex Cloud is not an Eligible Service and is not covered by the BAA, Customer may not upload, transmit, or process PHI using Codex Cloud.

4. Definitions.

4.1. "Codex Cloud" means the cloud-hosted version of the OpenAI Codex software engineering agent that is made available by OpenAI as a Service and any Codex functionality accessed via ChatGPT Enterprise via the web or applications.

4.2. "Codex SiWC" means the OpenAI-hosted services and infrastructure used to provide model inference, safety classification, authentication, authorization, service operation, and related support for Codex Local Clients when used with Sign-in With ChatGPT. For clarity, Codex SiWC does not include (a) Codex Cloud or any customer-selected connector, MCP server, third-party tool, third-party integration, customer-managed environment, customer device, local repository, terminal, log, cache, configuration file, history file, identity file, or other endpoint state; or (b) use of the Codex Local Client with a Customer managed OpenAI API account, in which case retention and data handling will be in accordance with the Customer's OpenAI API configuration.

4.3. "Codex Local Client" means Codex CLI, Codex Desktop, Codex IDE extensions, and substantially similar locally installed Codex surfaces made available by OpenAI to Customer under the Agreement that can be used to with Codex SiWC or with a customer-provided OpenAI API account.

4.4. "Codex Local" means the Codex Local Client used with the Codex SiWC Backend or the OpenAI API. Codex Local excludes Codex Cloud, cloud-hosted task execution, web search, connectors, MCP servers, and any Third-Party Services.