THE BUILDER'S TOOLKIT

Building with AI in healthcare

A working reference for shipping AI on protected health information without breaking HIPAA.

- Which AI providers sign a BAA
- How to turn on each provider's BAA
- A vendor-vetting checklist for any AI tool
- Safe patterns for running LLMs on PHI

paubox.com · Updated July 2026

PAUBOX

Which AI providers will sign a BAA

Most major providers will, but each hides it behind a specific plan or setting. Signing a BAA is only the first requirement.

> Verified July 2026. Provider terms and covered-service lists change often, so confirm the current agreement with each vendor before you rely on it.

Provider (surface)	Signs a BAA?	What it takes / conditions
Anthropic (Claude API)	Conditional	Org owner signs the BAA, then asks Anthropic to enable PHI. Some features stay out of scope.
Anthropic (Claude for Work)	Enterprise only	Activate HIPAA in Enterprise settings. Free, Pro, and Max are excluded.
OpenAI (API platform)	Yes	Request one from baa@openai.com. No enterprise contract required.
OpenAI (ChatGPT)	Enterprise/ Edu only	ChatGPT Business does not qualify.
Amazon Bedrock	Yes	Accept the AWS addendum in AWS Artifact. Free, any account. Process PHI only in HIPAA-eligible services.
Google Cloud (Vertex AI)	Conditional	Accept the Google Cloud BAA. Generally available services only; pre-GA excluded.
Google Workspace (Gemini)	Conditional	An admin accepts the amendment. Covered "included functionality" only.
Microsoft Azure OpenAI	Yes	Included by default via Microsoft's product terms and DPA. No separate contract.
Google Gemini API (AI Studio)	No	No BAA on this surface. Use Vertex AI instead when PHI is involved.
Cohere	Conditional	BAA for custom model development. For cloud-hosted access (Bedrock, Azure), the BAA is with the cloud provider.

How to turn on each provider's BAA

Most are self-serve. The mechanics differ by provider.

- [ ] **Anthropic:** the account's primary owner signs the BAA, then asks Anthropic to enable PHI handling. Keep PHI out of the features listed as out of scope.
- [ ] **OpenAI:** request a BAA from baa@openai.com for the API platform. No enterprise agreement required.
- [ ] **Amazon Bedrock:** accept the business associate addendum in AWS Artifact. Free, any account. Process PHI only in HIPAA-eligible services.
- [ ] **Google Cloud:** accept the Google Cloud BAA, then keep your work on generally available services.
- [ ] **Microsoft Azure OpenAI:** the BAA comes through Microsoft's product terms and data protection addendum. No separate document to chase.

Before you rely on any of them

- [ ] Confirm the BAA covers the **exact plan and configuration** you deployed, not a different tier.
- [ ] Turn on the provider's **PHI or HIPAA setting**, and keep PHI out of any feature listed as out of scope.
- [ ] Add your own **audit logging, access controls, and minimum-necessary limits** on top of the provider's controls.
- [ ] Route any **email or message your app sends** through a BAA-backed channel that encrypts by default.
- [ ] **Save the signed agreement** and note the exact plan and configuration it covers. An auditor will ask.

A vendor-vetting checklist for AI tools

Run these on every AI tool before it touches PHI. If a tool cannot or will not sign a BAA, it does not get PHI.

- [ ] Will the vendor **sign a BAA** for the exact plan and configuration you intend to deploy?
- [ ] What **data leaves your environment**, and how is it secured in transit and at rest?
- [ ] Which specific **features are inside the signed scope**, and which are excluded?
- [ ] Does the vendor **retain or train** on your data, and can you turn that off?
- [ ] Was the **infrastructure built for healthcare**, with certifications like HITRUST and SOC?

Safe patterns for running LLMs on PHI

- [ ] **Send the minimum necessary.** Strip identifiers the model does not need; pass a record ID your system can resolve, not a full patient profile.
- [ ] **Scrub PHI from logs and traces.** Prompt logs, LLM tracing, and error monitoring quietly capture whatever you send the model.
- [ ] **Treat your vector store as a PHI store.** Embeddings and retrieval indexes built on PHI need the same BAA, encryption, and access controls as your database.
- [ ] **Keep PHI out of uncovered features.** Provider BAAs are feature-specific; confirm the feature is inside the signed scope.
- [ ] **Constrain agents against prompt injection.** Limit the tools an agent can reach, scope its data access, and check its actions.
- [ ] **Log access and match retention to the workload.** Keep an audit trail, disable training where you can, and use zero-data-retention when the use case allows.