

SUPERWISE® LEARN KIT · OCTOBER 2026

HIPAA and AI: a checklist for using ChatGPT and Claude in a healthcare practice

Which plans carry a business associate agreement, the 18 identifiers to strip before anything leaves the practice, and the controls to put in place before staff paste patient details into a chat window.

Consumer ChatGPT and consumer Claude carry no BAA

No AI tool is HIPAA compliant on its own. A practice can send protected health information (PHI) to one only when three things are true: the vendor has a business associate agreement (BAA) with the practice, the plan is one the vendor names as eligible, and the feature in use is on the vendor's covered list.

No BAA available

- **ChatGPT Free, Plus, and Pro.** Absent from OpenAI's list of HIPAA eligible products.
- **ChatGPT Business.** OpenAI states it does not offer a BAA for this plan.
- **Claude Free, Pro, Max, and Team.** Anthropic states these plans "can't enable HIPAA."

A BAA is available

- **OpenAI.** ChatGPT for Healthcare, ChatGPT Enterprise with Regulated Workspace, ChatGPT for Clinicians, and the API with Modified Retention.
- **Anthropic.** Claude Enterprise once HIPAA is activated, the first-party Claude API, and Claude in Microsoft Foundry.
- **Both.** Only for the features each vendor lists as covered.

A signed BAA is the starting point

OpenAI's own help page says accepting its BAA does not, by itself, make an application HIPAA compliant [2]. Anthropic's BAA covers the single organization that accepted it, with configuration requirements and feature limits attached [4]. The practice still owns its policy, its risk analysis, its training, and its records. The checklist in part 4 of this kit covers each of them.

PLAIN ENGLISH • BUSINESS ASSOCIATE AGREEMENT

A contract in which a vendor that handles patient information for your practice agrees to protect it the way HIPAA requires. HHS treats a cloud service that processes or stores patient data for you as a business associate, even when it holds only encrypted data, and requires a BAA with it [7].

Not legal advice. This kit summarizes public vendor terms and HHS guidance for a practice deciding how staff may use AI. Confirm every decision with your compliance officer or counsel before you act on it.

Vendor terms move fast. OpenAI and Anthropic both updated their HIPAA pages in the week this kit was written. Every vendor fact in it carries the date it was read. Check the source before you rely on one.

Which plans carry a BAA, as of October 7, 2026

Read from each vendor's own pages. Numbers in the last column point to the sources at the end of this kit.

PLAN OR SERVICE	BAA	HOW, AND THE CONDITIONS	SOURCE
OPENAI · CHATGPT AND THE API			
ChatGPT Free, Plus, and Pro	None	Absent from OpenAI's HIPAA eligible products list.	1
ChatGPT Business	None	OpenAI: "We do not offer a BAA for ChatGPT Business."	2
ChatGPT Enterprise or Edu, sales-managed	Through sales	Contact OpenAI sales. The eligible product is named "ChatGPT for Enterprise with Regulated Workspace."	1, 2
ChatGPT for Healthcare	Available	OpenAI's route for a BAA covering several users, with central admin controls.	1, 3
ChatGPT for Clinicians	Individual	Free at launch for verified US physicians, nurse practitioners, physician assistants, and pharmacists. Each clinician signs under Settings > Agreements. It covers one person, so front-desk staff are outside it.	3
OpenAI API	Self-serve or email	An organization admin accepts the standard BAA in API Platform settings, which needs an established history of API usage, or emails baa@openai.com for custom terms. Modified Retention is required unless OpenAI specifies otherwise. Once enabled, it cannot be turned off in settings.	1, 2
ANTHROPIC · CLAUDE AND THE API			
Claude Free, Pro, and Max	None	Anthropic: these plans "can't enable HIPAA."	5
Claude Team	None	Named alongside the individual plans in the same statement.	5
Claude Enterprise, self-serve or sales-assisted	After activation	The Primary Owner turns on HIPAA under Organization settings > Data and privacy and accepts the BAA. A standard Enterprise plan has no BAA coverage until then. Anthropic calls it a one-way decision.	4, 5
Claude API, first-party	Through sales	The Primary Owner signs the BAA, then asks Anthropic sales to turn it on. Covered models need 30-day data retention and are unavailable with zero data retention unless Anthropic authorizes it.	4
Claude in Microsoft Foundry	Available	Listed by Anthropic as a HIPAA-ready service, with limits on the features available.	4
Claude Console, Cowork in the cloud, beta features	Excluded	Named exclusions, including the betas Claude in Office, Claude Design, Claude Slides, and Claude Docs.	4

A covered plan can still carry uncovered features

- **OpenAI.** Inside an eligible ChatGPT workspace, improved memory, Sites, Codex in the cloud, and internet access in canvas and code blocks sit outside the BAA. OpenAI adds that features it has not listed are not automatically covered [1].
- **Anthropic.** On the API, the Batch API, Files API, code execution, computer use, and web fetch sit outside the BAA. In Claude Enterprise, sending data to third parties through connectors, MCP servers, or Claude in Chrome is outside it too [4].
- **Gateways and proxies.** Anthropic excludes Claude Code routed through an LLM gateway from its HIPAA setup. Part 5 covers what that means for a redaction gateway [4].

The 18 Safe Harbor identifiers

HHS recognizes two ways to de-identify health information. Safe Harbor is the one a practice can run itself: remove all 18 identifiers below, for the patient and for their relatives, employers, and household members, and have no actual knowledge that what remains could identify the person [6].

☐ **A** Names

☐ **B** Geographic units smaller than a state: street address, city, county, precinct, and ZIP code. The first three ZIP digits may stay where that area holds more than 20,000 people.

☐ **C** Every element of a date except the year, for birth, admission, discharge, and death dates. Ages over 89 fold into a single 90-or-older group.

☐ **D** Telephone numbers

☐ **E** Fax numbers

☐ **F** Email addresses

☐ **G** Social Security numbers

☐ **H** Medical record numbers

☐ **I** Health plan beneficiary numbers

☐ **J** Account numbers

☐ **K** Certificate and license numbers

☐ **L** Vehicle identifiers and serial numbers, including license plates

☐ **M** Device identifiers and serial numbers

☐ **N** Web URLs

☐ **O** IP addresses

☐ **P** Biometric identifiers, including finger and voice prints

☐ **Q** Full-face photographs and any comparable images

☐ **R** Any other unique identifying number, characteristic, or code

Where identifiers hide in a prompt

- **Pasted notes.** A visit note carries names, dates, and places inside its sentences, where a field-by-field review misses them.
- **Other people.** The rule covers a patient's relatives, employer, and household. "Her husband runs the pharmacy on Main Street" names a relative's employer and a street.
- **Rare details.** A rare diagnosis in a small town can point to one person with every listed identifier gone. That is what item R and the actual-knowledge test exist for.

PLAIN ENGLISH • DE-IDENTIFIED

Health information with all 18 identifiers removed and nothing left that the practice knows could point back to a person. HHS no longer treats it as PHI. Text with some of the identifiers removed is still PHI. The other HHS method, Expert Determination, needs a qualified expert to document that the risk of identification is "very small" [6].

Seven controls to have in place

Work through it with the person who owns compliance in your practice. Citations in gray point to the HHS rule summaries and vendor pages listed at the end of this kit.

Policy

- ☐ **Write an AI use policy.** Name the tools staff may use, and state that PHI goes only into a tool with a BAA on file and a covered feature. A copyable starting point is at superwise.ai/learn/ai-acceptable-use-policy/.
- ☐ **Name its owner.** The Security Rule requires a designated security official, and AI use belongs on that person's list.
HHS Security Rule summary, assigned security responsibility [8]
- ☐ **Add AI tools to your risk analysis.** Record which tools touch patient information, where the data goes, and what reduces the risk.
HHS Security Rule summary, security management process [8]

Approved tools

- ☐ **List each approved tool exactly.** Vendor, plan, and the workspace or organization the BAA names. "ChatGPT" is a product family; "ChatGPT for Healthcare, workspace Smith Family Practice" is an approval.
- ☐ **Move practice work off personal accounts.** Free and individual paid plans from both vendors carry no BAA, whoever pays for them.
OpenAI [1], Anthropic [5]
- ☐ **Switch off features the BAA excludes.** Memory, connectors, browser extensions, and cloud agents are the usual ones. Re-check the vendor's list each quarter, since both lists changed this month.
OpenAI [1], Anthropic [4]

BAAs on file

- ☐ **Keep a copy of each BAA.** Record the date accepted, who accepted it, and the account it covers. OpenAI offers a download for the standard API agreement under View agreement.
OpenAI [2], Anthropic [4]
- ☐ **Record the configuration the BAA depends on.** Modified Retention for the OpenAI API, and HIPAA activated by the Primary Owner for Claude Enterprise.
OpenAI [1], Anthropic [5]
- ☐ **Check connected services separately.** Third-party GPTs, connectors, MCP servers, and website chat widgets have their own terms. OCR guidance on tracking technologies applies when a website tool collects PHI.
OpenAI [3], Anthropic [4], HHS OCR [10]

De-identification

- ☐ **Start from no PHI.** OpenAI notes that "many clinical tasks" need none. Template letters, policies, and patient education drafts can start from a blank page.
OpenAI [3]
- ☐ **Strip all 18 identifiers before using a tool without a BAA.** Use the Safe Harbor checklist in part 3, and include relatives, employers, and household members.
HHS de-identification guidance [6]
- ☐ **Treat partial removal as PHI.** A prompt with the phone number gone and the name left is still protected health information.

Staff training

- ☐ **Train every workforce member before access.** The Security Rule requires training all workforce members on security policies.
HHS Security Rule summary, security awareness and training [8]
 - ☐ **Show real examples.** Walk through a prompt that carries PHI and the same prompt with all 18 identifiers removed.
 - ☐ **Apply sanctions consistently.** The Security Rule requires sanctions against workforce members who violate the policy.
HHS Security Rule summary [8]
-

Logging and audit

- ☐ **Turn on the vendor's audit tools.** Both vendors list a Compliance API among the services their BAA covers.
OpenAI [1], Anthropic [4]
 - ☐ **Review the records on a schedule.** The Security Rule requires procedures to regularly review records that track access to ePHI and detect security incidents.
HHS Security Rule summary, audit controls [8]
 - ☐ **Write each review down.** Date, reviewer, what was found, and what changed as a result.
-

Incident response

- ☐ **Treat PHI in an unapproved tool as a possible breach.** HHS presumes an impermissible disclosure is a breach unless a four-factor risk assessment shows a low probability of compromise.
HHS Breach Notification Rule [9]
 - ☐ **Know the deadlines.** Affected individuals within 60 days of discovery at the latest. HHS within 60 days for 500 or more people, or within 60 days of the end of the calendar year for fewer.
HHS Breach Notification Rule [9]
 - ☐ **Record what you did to contain it.** The extent of mitigation is one of the four factors, so the chat deleted, the account closed, and the vendor contacted all belong in the file.
HHS Breach Notification Rule [9]
-

Keep patient work on a model you control

Two controls work together. Patient work goes to a model SUPERWISE hosts on its own equipment, under a BAA with the practice. For the outside tools staff keep using, a gateway on the PC replaces the identifiers it recognizes before a prompt leaves.

Patient work on a SUPERWISE-hosted model

- **Where it runs.** On SUPERWISE's own servers, in a locked cage in a datacenter. No outside AI vendor receives the prompts.
- **The models.** Open-weight models run on those servers: Qwen 27B and gpt-oss-120b. OpenAI publishes gpt-oss-120b, but OpenAI does not run it here and never sees the traffic.
- **How staff reach it.** Through SUPERWISE Chat, or through Sentinel configured to send a tool's traffic to the hosted model.
- **The agreement.** SUPERWISE signs a BAA with the practice. Available now under a custom contract, through superwise.ai/contact/.

What SUPERWISE Sentinel does

As described on superwise.ai/sentinel/, read October 7, 2026 [11]:

- **Placeholders.** It replaces emails, phone numbers, account and card numbers, government IDs, and API keys with placeholders before a prompt reaches ChatGPT or Claude.
- **A record.** Every inspected interaction lands in an Activity Log the practice can show.
- **Platforms.** Windows 10 and 11 with no admin rights, a CLI for macOS and Linux, and a browser extension in preview for Chrome and Edge.

Limits to plan around

- **Coverage decides the result.** Its PII redaction guardrail covers phone numbers, email addresses, Social Security and other government ID numbers, account and card numbers, IP addresses, vehicle numbers, and, when labeled in the text, dates of birth and medical record numbers (docs.superwise.ai, PII redaction, read October 7, 2026) INFERRED OVERLAP. Names, street addresses, dates such as admission or service dates, and unlabeled record numbers are not redacted. A prompt that holds any of them still carries PHI.
- **It makes no tool HIPAA compliant.** Compliance is the practice's program: policy, training, BAAs where PHI is shared, and audit. Sentinel is one control within it.
- **Vendor BAAs and gateways.** Anthropic states that Claude Code sessions routed through an LLM gateway or custom base URL fall outside its HIPAA configuration [4]. Because names and dates pass through, a gateway cannot stand in for that configuration. Keep patient work on a covered plan or on the hosted model.

Trying it. SUPERWISE Sentinel is free for 30 days with no card, then \$10, \$25, or \$50 a month per deployment, as listed on superwise.ai/pricing/ on October 7, 2026 [11]. Details are at superwise.ai/sentinel/.

Sources

All read on October 7, 2026. Vendor pages show a relative update date only; the one shown on the day is recorded with each.

- 1 OpenAI Help Center, *HIPAA eligible products and functionality*. Eligible products, covered and uncovered ChatGPT features, eligible API endpoints. Marked "Updated: yesterday." help.openai.com/en/articles/20001069
- 2 OpenAI Help Center, *Getting a Business Associate Agreement for the OpenAI API*. API BAA process, ChatGPT Business exclusion, Enterprise and Edu through sales. Marked "Updated: 2 days ago." help.openai.com/en/articles/8660679
- 3 OpenAI Help Center, *ChatGPT for Clinicians*. Eligibility, the individual BAA, and ChatGPT for Healthcare for several users. Marked "Updated: last month." help.openai.com/en/articles/20001202
- 4 Anthropic Privacy Center, *Business Associate Agreements (BAA) for Commercial Customers*. HIPAA-ready services, exclusions, feature coverage, retention, and gateway coverage. Marked "Updated this week." privacy.claude.com/en/articles/8114513
- 5 Claude Help Center, *HIPAA-ready Enterprise plans*. Eligible plans, activation steps, and the one-way decision. Marked "Updated this week." support.claude.com/en/articles/13296973
- 6 HHS Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information*. Safe Harbor identifiers and Expert Determination. hhs.gov/hipaa/for-professionals/special-topics/de-identification/
- 7 HHS, *Guidance on HIPAA & Cloud Computing*. Business associate status of cloud services, including those holding only encrypted data. hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/
- 8 HHS, *Summary of the HIPAA Security Rule*. Security official, risk analysis, training, sanctions, and audit controls. hhs.gov/hipaa/for-professionals/security/laws-regulations/
- 9 HHS, *Breach Notification Rule*. Breach presumption, the four factors, and notification deadlines. hhs.gov/hipaa/for-professionals/breach-notification/
- 10 HHS Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*. Part of this bulletin was vacated by a federal court on June 20, 2024, as the page itself notes. hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/
- 11 SUPERWISE, *Sentinel and Pricing*. Product claims and prices used in part 5. superwise.ai/sentinel/ · superwise.ai/pricing/

Further reading on superwise.ai

- **HIPAA and AI answers.** superwise.ai/learn/is-chatgpt-hipaa-compliant/ and [/learn/is-claude-hipaa-compliant/](https://superwise.ai/learn/is-claude-hipaa-compliant/)
- **AI in healthcare.** superwise.ai/healthcare/ and the Renova Health case study