

BAAs made simple

Real-life examples for health insurance agents

By Kate Spilsbury, RSSA®, CMIP® • Founder of Mere Benefits

**Before client health information goes into a tool, ask:
“Is this exact account and feature covered by a BAA?”**

What is a BAA, in plain English?

A **Business Associate Agreement** is a written agreement about how another business can use and protect health information it handles for you. It also spells out responsibilities if something goes wrong. [1]

Think about what you do every day

- You save a client’s medication list in your CRM.
- Your phone system records a client discussing a diagnosis.
- An AI tool turns that conversation into notes.
- Your assistant opens an application or insurance card.

Each is a reason to check where the information goes and which agreements apply. When HIPAA applies to your work and a vendor handles protected health information for you, a BAA is generally required. [1]

What counts as protected health information?

Think **health or coverage details tied to an identifiable person**: a named medication list, claims, diagnoses, insurance records, or a recorded health conversation in a HIPAA-covered relationship. PHI is the short name. [2]

One important detail: Being an agent does not automatically make you a HIPAA covered entity. Your work may make you a business associate of a health plan. Confirm your role and carrier requirements. [1]

This guide gives practical examples, not a complete HIPAA program or legal advice. Sources and product information checked October 9, 2026.

Can I use ChatGPT or Gemini?

“Can I get a BAA with ChatGPT?”

Yes, for certain eligible offerings—not every ChatGPT plan. [3, 4]

What you use	What to know
ChatGPT Free, Plus, or Pro	These ordinary accounts are not listed as HIPAA-eligible products. Do not use them for PHI.
ChatGPT Business	OpenAI says it does not offer a BAA for this plan.
Eligible enterprise / healthcare offerings	BAAs are available for eligible offerings, including ChatGPT for Healthcare and Enterprise with a Regulated Workspace. Sales-managed Enterprise or Edu customers can contact sales about eligibility. Confirm the actual agreement and covered features.
OpenAI API	This is separate from your ChatGPT subscription. Eligible API organizations can obtain a BAA; covered services and required configuration still apply.

“I have a Google Workspace BAA. Can I use Gemini?”

Eligible Gemini use can be covered. Google lists Gemini in Workspace and the Gemini app among supported services, but excludes Gemini in Chrome. Use the covered organizational account and follow the required setup. A personal Gemini account is not covered by your organization’s Workspace BAA. [5, 6]

My agency example: I have a BAA with Google for my Google Workspace account. That gives me more options for using covered Workspace and Gemini services. I still need to check the account, feature, and settings—not assume everything with the Google name is covered.

Two very different AI requests

General content: “Write a post explaining what a deductible is.” No client PHI is involved.

Client work: “Summarize this named client’s prescriptions and diagnoses.” Verify the BAA and approved setup before uploading.

Paying for AI or turning off model training does not, by itself, give you a BAA. [3, 4]

Your everyday technology

These examples show **when to check**. They do not confirm that any particular vendor or account is covered. [1, 7]

Your CRM

Example: You enter “Client takes insulin” and attach a medication list to the client’s record.

Check: Does the BAA cover your CRM account, attachments, and any AI features? If the CRM sends notes to another service, review that service too.

Phone recordings and voicemail

Example: A client talks about cancer treatment during a recorded call. Or leaves health details in voicemail.

Check: Which company stores the audio? Is recording, storage, and transcription covered? A recording is client information even before anyone types notes.

Zoom plus an AI note-taker

Example: A tool such as Fathom joins your Zoom appointment and makes a transcript.

Check: Review both the meeting platform and the separate note-taker. A BAA with one company does not automatically cover the other. Verify each account’s terms before using PHI.

Email, Google Drive, and forms

Example: A client sends an insurance card. You save it in Drive or collect health details through a form.

Check: Use the covered business account and approved sharing settings. Google lists Gmail, Drive, and Forms within supported Workspace services. A Workspace BAA does not extend to your personal Gmail or outside add-ons. [5, 8]

Texting, fax, e-signatures, and backups

Example: You text a document, send an application for signature, or automatically back up recordings.

Check: Include each service that receives or stores PHI. Do not overlook the backup or the app connected to your main system.

Easy-to-miss example: Your covered CRM emails an appointment summary to your personal inbox. You have added another destination to review. Start with where the information ends up.

People, paper, and office access

Outside assistants and answering services

Example: A VA logs into your CRM to review medication lists or applications.

Check: An outside service handling PHI for you may need a BAA. People who qualify as your workforce generally do not need separate BAAs; they need training and access rules. Do not decide based only on the title “VA.” [1, 9]

IT support

Example: A technician can access client records while supporting your computers or backup system.

Check: Review what the service can access and what work it performs. A confidentiality promise alone does not replace a required BAA. [1]

Record storage and shredding

Example: A company picks up boxes of applications to store or destroy.

Check: Routine handling or destruction of PHI generally points toward a business-associate relationship. HHS notes a workforce option for some services under direct control. [9]

Cleaning crews and landlords

Example: Your cleaning crew vacuums the office, or your landlord has a key.

Usually: Office access alone does not mean they need a BAA. HHS says routine cleaning generally does not require one when PHI exposure is only incidental. Applying that same principle, renting office space alone generally does not either. [9]

Different example: Your shared office also provides a receptionist who handles client health records. Review that extra service separately.

A designer or marketing company

Example: Someone makes your logo using public information.

Usually: That task alone does not involve PHI. Giving that same company access to client health records changes the question. [1]

Good office habits still matter: Lock files, clear desks, secure screens, and limit access. Confidentiality agreements can help; use a BAA when the actual service requires one.

A simple review you can actually do

Start with five things

- ☐ Your CRM
- ☐ Your email and file storage
- ☐ Your phone / meeting recordings
- ☐ Your AI and transcription tools
- ☐ Your outside assistants and connected apps

For each one, answer these questions

- **What client information goes into it?** Include recordings and attachments.
- **Is a BAA required for this use?** Resolve uncertainty with compliance or counsel.
- **Do I actually have the BAA?** Save the accepted agreement and date.
- **Does it cover this account and feature?** Check the product, plan, and exclusions.
- **Where does the information go next?** Include integrations, exports, and backups.

Send this to the vendor

“We plan to use **[product and account]** for **[describe the task]**, which may involve protected client health information. Do you offer a BAA covering this use? Please send the agreement and tell us which features are covered, what is excluded, and which settings we must use.”

If you cannot confirm coverage

Hold the PHI workflow while you verify it or arrange an approved alternative. Use invented examples for demos. Removing only a client’s name does not establish that a real record is de-identified. [2]

Keep one small tracking list

Tool → account → BAA status → approved features → next action.

Update it when you change tools, plans, or integrations.

A BAA is part of protecting clients. Secure setup, appropriate access, staff training, and incident procedures still matter. If information reaches an unapproved service, promptly involve your incident contact instead of assuming deletion resolves it. [7, 10]

Sources, without the homework

You do not need to read every policy to use this guide. These official links let you check a rule or product detail when needed. Click a title to open the source.

[1] HHS: Business Associates

[2] HHS: PHI and de-identification

[3] OpenAI: Getting a BAA

[4] OpenAI: HIPAA-eligible products and features

[5] Google: Supported HIPAA services

[6] Google: Workspace with Gemini FAQ

[7] HHS: Cloud computing and BAAs

[8] Google: Workspace HIPAA requirements

[9] HHS: Cleaning crews and incidental contact

[10] HHS: Breach Notification Rule

A note about these examples

The examples apply official guidance to common agency tasks. They do not verify your particular Google, ChatGPT, CRM, recording, or other account. Named tools are examples, not endorsements. Product coverage can change; verify current terms before sharing PHI.

Whether HIPAA requires a BAA depends on your role and the service's work. Other privacy rules and carrier contracts may also apply. This educational guide does not replace legal advice or a full compliance review.

The question to remember:

"Before I put client health information here, have I checked the exact account, feature, and agreement?"

Kate Spilsbury, RSSA®, CMIP®

Mere Benefits • Simply For Your Benefit
KateSpilsbury.com • @katespilsbury

Version 2.0 • Simplified edition • October 9, 2026