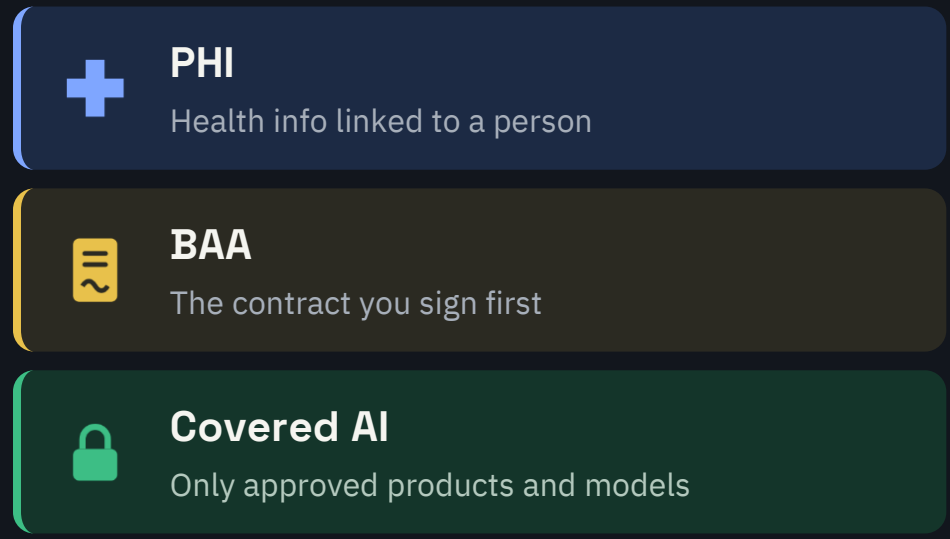
A BEGINNER'S GUIDE

HIPAA and AI

What counts as patient data, how BAAs work, and how to build with AI safely



Ibrahim Jaafar · Not legal advice

THE BASICS

HIPAA: the US law for patient data

The **Health Insurance Portability and Accountability Act** (1996) protects patients' health information in the United States. It has four main rules:

Privacy

Who may use patient data, and for what.

Security

How digital patient data must be protected.

Breach notice

Who must be told when data leaks.

Vendors (BAAs)

Outside companies must sign a contract first.

Outside the US? It applies to you only if you handle data for US healthcare organizations.

ROADMAP

What we'll cover

1	**Terminology**	The key words, and who is who
2	**What counts as PHI**	The 18 identifiers, and what isn't PHI
3	**HIPAA and AI**	Which AI tools can touch patient data
4	**Signing a BAA**	Step by step, provider by provider
5	**Your options**	Building apps and coding with Claude

1

PART 1 OF 5

Terminology

The words you’ll hear, in plain language

And who plays which role.

1 · TERMINOLOGY

Nine words you'll hear

PHI
Protected Health Information: health data linked to a person

ePHI
PHI stored or sent electronically, like in an app or AI

Covered entity
Hospitals, clinics, doctors, pharmacies, health insurers

Business associate
An outside company that handles PHI for them

BAA
Business Associate Agreement: the contract signed first

HIPAA-eligible
A product the provider's BAA actually covers

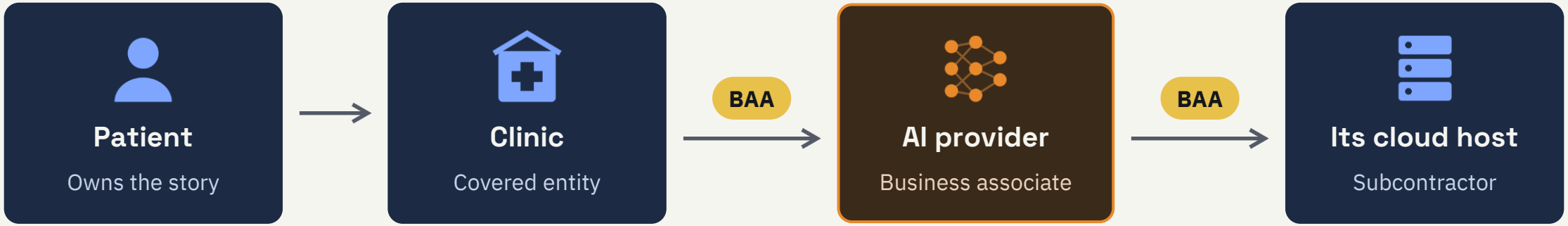
De-identification
Removing identifiers so data is no longer PHI

Minimum necessary
Use or share only the PHI a task really needs

Breach
PHI seen or taken by someone who shouldn't have it

1 · TERMINOLOGY

Who is who



The clinic

Responsible for its patients' data, wherever it goes.

The AI provider

Signs a BAA and must protect the data it receives.

Down the chain

Every subcontractor that touches PHI needs a BAA too.

2

PART 2 OF 5

What is PHI?

What counts as patient data, and what doesn’t

The 18 identifiers, real examples, and de-identification.

2 · WHAT IS PHI?

The PHI formula

Health information

Condition, test result, treatment, payment

+

An identifier

Name, date of birth, phone, record number…

=

PHI

Protected by HIPAA

Example: “HbA1c 9.1%” + “Rami K., born 04/03/1980” = **PHI**

Health info alone, or a name alone, is usually not PHI. Together, held by a clinic or its vendor, they are.

The 18 identifiers

01	Names	07	Social Security numbers	13	Device IDs and serial numbers
02	Addresses smaller than a state	08	Medical record numbers	14	Web URLs
03	Dates (except year), ages over 89	09	Health plan numbers	15	IP addresses
04	Phone numbers	10	Account numbers	16	Fingerprints, voiceprints
05	Fax numbers	11	Certificate or license numbers	17	Full-face photos
06	Email addresses	12	Vehicle IDs and plate numbers	18	Any other unique ID or code

Rule of thumb: if it could point to one specific person, treat it as an identifier.

PHI or not?

Example	PHI?	Why
A clinic note: “Rami, 45, has diabetes”	PHI	Health info + name
A lab result with a medical record number	PHI	Record number is an identifier
A clinic’s appointment list with names	PHI	Shows a person is a patient
“40% of our patients have diabetes”	Not PHI	No individual person
Your step count in a fitness app you use	Not PHI*	App isn’t a covered entity
An employee’s sick-leave record at HR	Not PHI*	Employment record, not care
A properly de-identified dataset	Not PHI	Identifiers removed
Fake (synthetic) test data	Not PHI	Belongs to no real person

* Not covered by HIPAA, but other privacy laws can still apply.

Three ways to work without PHI

METHOD 1

Safe Harbor

✓ Officially recognized

Starts with real data

Remove all 18 identifiers, and have no reason to think the rest could still identify someone.

METHOD 2

Expert Determination

✓ Officially recognized

Starts with real data

A qualified expert confirms the risk of re-identifying anyone is very small.

ALTERNATIVE

Fake (synthetic) data

Not a HIPAA method

✓ No real data at all

Made-up patients with fake names and results. Never PHI, so ideal for building and testing.

Careful: removing names isn't enough. Dates, zip codes and rare conditions can still point to one person.

Also careful: fake data generated from real records can still leak real details.

3

PART 3 OF 5

HIPAA and AI

Which AI tools may touch patient data

And the catches people miss.

An AI provider is a business associate

Sending PHI to an AI service means sharing it with an outside company. So the rule is simple: **no BAA, no PHI.**

Not allowed

Free or personal chat apps

ChatGPT Free or Plus, Claude Pro or Max, consumer Gemini. No BAA is offered.

Allowed

Business plans or APIs with a BAA

Only on the products, features and models the BAA covers.

No BAA needed

A model on your own hardware

No outside company sees the data. You still protect it yourself.

Which AI products a BAA can cover

Provider	Can be covered	Not covered
Anthropic	Claude API Claude Enterprise (HIPAA-ready)	Free, Pro, Max, Team plans
OpenAI	OpenAI API ChatGPT Enterprise and Edu	ChatGPT Free, Plus, Business
Google	Vertex AI Workspace with Gemini (business)	Consumer Gemini, NotebookLM
Microsoft	Azure OpenAI Service	Check the product terms
Amazon	Bedrock (Claude, Llama and others)	Models not on AWS's eligible list

Cloud tip: on Bedrock, Vertex or Azure, one cloud BAA covers several models at once.

Checked October 2026. Coverage changes often: confirm on each provider's own HIPAA page.

3 · THE CATCHES

A signed BAA isn’t the finish line

It covers them, not you

Your own app, logs and staff access are still your job.

Not every feature

Some features stay uncovered or get switched off.

Not every model

On Bedrock, Claude Fable and Mythos models are excluded.

Settings aren’t automatic

Zero retention and audit logs often need switching on.

“HIPAA-certified” is a myth

No official HIPAA certification exists for any software.

Rules are changing

A stricter Security Rule is proposed, now expected in 2027.

4

PART 4 OF 5

Signing a BAA

Step by step, provider by provider

Claude first, then OpenAI, AWS, Microsoft and Google.

4 · SIGNING A BAA

Claude Enterprise: four steps

1. Get a **Claude Enterprise** plan through Anthropic sales
2. The **Primary Owner** opens Organization settings › Data and privacy
3. Under **HIPAA Compliance**, click Enable; read the BAA and guide
4. Click **“Accept and enable HIPAA”**: that’s your signature

Before you click

- The BAA is standard; it can’t be changed
- It can’t be undone from settings
- Some settings reset to defaults
- Use PHI only with features the guide lists as covered

Building on the **Claude API** instead? Ask Anthropic sales for a HIPAA-ready API organization (next slide).

4 · SIGNING A BAA

Getting a BAA everywhere else

Claude API

Contact Anthropic sales for a HIPAA-ready API organization.

Amazon Bedrock

Accept the BAA in AWS Artifact. Free, for any AWS account.

OpenAI

API: email baa@openai.com. ChatGPT Enterprise: via sales.

Azure OpenAI

Included in Microsoft’s product terms. No separate document.

Google Cloud

Accept the Google Cloud BAA. Generally available services only.

Whichever you pick

Read the implementation guide, then check each model and feature.

5

PART 5 OF 5

Your options

Building apps and coding with Claude

Plus a checklist before any PHI goes in.

5 · YOUR OPTIONS

Building an app that touches PHI

1	**Pick where Claude runs**	Anthropic’s API, or Bedrock, Vertex AI or Azure in your own cloud.
2	**Sign the BAA first**	Until it’s signed, test only with fake data.
3	**Use covered features and models**	Some are blocked or excluded for HIPAA accounts.
4	**Secure your own app**	Encrypt PHI, limit access, no prompts in plain logs, keep an audit trail.
5	**Send the minimum**	Strip names and IDs when the task doesn’t need them.

5 · YOUR OPTIONS

Coding with Claude Code near PHI

Remember: anything Claude Code reads (files, test data, query results) is sent to Claude.

Recommended

1. Keep PHI away

Build and test with fake data. Block real-data folders with “deny” rules in settings. Any plan, no cost.

Simplest BAA

2. Run it via Bedrock

Point Claude Code at Claude in your AWS account. Covered by the AWS BAA.

Most setup

3. Claude Enterprise

HIPAA alone doesn’t cover Claude Code. Needs zero retention or a special setup.

Not an option: a personal Pro or Max plan. No BAA is available.

5 · YOUR OPTIONS

Which option fits your situation?

If you want to...	Use
Give staff a chat assistant	Claude Enterprise with HIPAA enabled
Build an app that processes PHI	Claude via Bedrock, Vertex or Azure, or the API with a BAA
Code that app with Claude Code	Fake data only; or Claude Code via Bedrock
Analyze data or do research	De-identify first, then any tool
Keep PHI away from any outside company	A self-hosted model on your own hardware

5 · YOUR OPTIONS

Checklist before any PHI goes in

- [x] BAA signed with the provider
- [x] Product is on the covered list
- [x] Model is HIPAA-eligible
- [x] Every feature checked against the guide
- [x] Retention and logging settings set
- [x] Your app encrypts and limits access
- [x] Only the minimum PHI is sent
- [x] Tested end to end with fake data

RECAP

Five things to remember

1. PHI = health information + an identifier.
2. No BAA, no PHI. Free and personal AI apps are off-limits.
3. A BAA covers the provider, not your app.
4. Check every product, feature and model.
5. Build with fake data; real PHI only in the covered app.

SOURCES

Read more

Anthropic: HIPAA-ready Enterprise plans
support.claude.com › hipaa-ready-enterprise-plans

Paubox: AI healthcare HIPAA toolkit
paubox.com › ai-healthcare-hipaa-toolkit

John D. Cook: HIPAA compliant AI
johndcook.com › hipaa-compliant-ai

Respan: HIPAA BAAs for LLM engineering
respan.ai › hipaa-baa-llm-engineering

Anthropic: API and data retention
platform.claude.com › api-and-data-retention

Aptible: AWS Bedrock HIPAA compliance
aptible.com › aws-bedrock-baa

The AI Career Lab: AI BAAs in 2026
theaicareerlab.com › baa-vendor-guide

Paubox: Security Rule update delayed
paubox.com › security-rule-delayed-to-2027