# The rules first, *then the list.*

*What HIPAA requires when an AI vendor touches patient information, and the four-part checklist to run before anything is signed.*

## What's inside

- **The rules.** How existing HIPAA obligations apply when AI touches patient information, cited to HHS throughout.
- **When a vendor becomes a business associate.** And what has to be signed before any patient information moves.
- **What the BAA must contain.** The required elements at 45 CFR 164.504(e), one at a time.
- **What the contract will not tell you.** Model training, retention, subcontractors, the breach clock, and how you get your data back.
- **A printable checklist.** Four parts and a disposition block. One copy per vendor.
- **Chart A.** All eighteen Safe Harbor identifiers, and the same clinical note before and after de-identification.

## How to use it

Read the first half once, before you vet anything. Then print the checklist and complete one copy per vendor, before signing and before any patient information flows. Keep the completed copy with the executed agreement. Bring what it raises to your attorney; that is what this document is for.

# HIPAA did not change for AI. Your exposure did.

## First principle: know your HIPAA status

HIPAA obligations sit with your practice, not with your vendors' marketing departments. A vendor saying "we're HIPAA compliant" transfers nothing. Compliance depends on what your practice signs, configures, and enforces.

## When an AI vendor becomes a "business associate"

Under HIPAA, a business associate is an entity that creates, receives, maintains, or transmits PHI on your behalf, including for "data analysis, processing or administration" (45 CFR 160.103). If an AI tool touches identifiable patient information on your behalf, it is almost certainly a business associate.[1]

**The consequence: when a vendor is acting as your business associate, PHI should not flow until an appropriate business associate agreement (BAA) is in place. The required contents are listed at 45 CFR 164.504(e), and Part B of the checklist in the second half of this document walks them one by one.[2]**

## Minimum necessary

Even with a BAA — and where the minimum necessary standard applies — an AI tool should receive only the PHI its task requires (45 CFR 164.502(b)).[3] A scribe, for example, needs the encounter audio. It does not need your whole chart export. Scope integrations deliberately.

## New tool, new risk analysis

The Security Rule requires an accurate, thorough risk analysis covering all ePHI your practice creates, receives, maintains, or transmits, explicitly including ePHI handled by vendors. OCR's guidance names incorporating new technology as a reason to review it.[4] Adding an AI tool is exactly that kind of change: assess and document the resulting risks as part of your ongoing risk-analysis and risk-management process, and update safeguards as appropriate. If your practice has never done a risk analysis, this is the moment; it is a required, foundational Security Rule element.

## The de-identification myth

Deleting the patient's name does not make data safe for a consumer AI tool. HIPAA recognizes exactly two de-identification methods: Safe Harbor, which requires removing all eighteen categories of identifiers and having no actual knowledge the remainder could identify the person; or Expert Determination by a qualified statistician (45 CFR 164.514).[5] A visit story with age, date, and rare diagnosis can identify a patient with the name long gone. Chart A at the end of this document lists all eighteen, and shows the same note before and after.

## Personal accounts are the leak

A particularly foreseeable and hard-to-control AI risk is not the vetted AI tool. It is PHI pasted into a free personal AI tool to complete a task. No BAA. No practice control. Your written policy and your training are what prevent it.

## State law can be stricter — and Part 2 is stricter still

HIPAA is a floor, not a ceiling. Your state may add requirements HIPAA does not: recording and consent, mental-health and behavioral-health records, substance-use records, minors, and how quickly a breach must be reported. Separately, and everywhere, substance-use-disorder records under 42 CFR Part 2 are stricter than HIPAA. Confirm what applies to you with counsel.

## The rules are moving

HHS proposed a significant HIPAA Security Rule update (published in the Federal Register January 6, 2025) that would tighten requirements around encryption, multifactor authentication, asset inventories, and business associate obligations.[6,7] As of this writing (2026) it remains a proposed rule — HHS has moved the rulemaking to its long-term agenda, with final action not expected in the near term — and the current Security Rule remains in effect. Have your attorney confirm status at your next policy review.

## The five-line summary

- If your practice conducts standard electronic transactions, it is almost certainly a covered entity, and the risk is yours. Confirm your status with counsel if unsure.
- An AI vendor that creates, receives, maintains, or transmits PHI on the practice's behalf is generally a business associate and ordinarily requires a signed BAA before PHI flows; confirm unusual arrangements with counsel.
- Minimum necessary, where it applies: the tool gets only what the task needs.
- New AI tool = review and, if needed, update the security risk analysis.
- Name-deletion is not de-identification, and personal AI accounts are never the place for PHI.

# Before patient data touches a vendor, run this list.

Print one copy for every vendor that will touch patient information, before you sign and before any patient information moves. Work through Parts A to D, then record your decision at the bottom and keep the completed copy with the signed BAA.

**Vendor / tool:** _____

**Completed by:** _____

**Date:** _____

## Part A. Does this vendor need a BAA?

☐ The tool will **create** PHI on our behalf (e.g., drafts clinical notes from encounter audio).

☐ The tool will **receive** PHI from us (uploads, integrations, dictation, message content).

☐ The tool will **maintain** PHI (stores recordings, transcripts, drafts, embeddings, logs).

☐ The tool will **transmit** PHI (sends data to its cloud, subcontractors, or the EHR).

If any box is checked and the vendor performs that function or service on the practice's behalf, the vendor is generally a business associate and a BAA is required before use; confirm unusual arrangements, such as treatment disclosures, workforce relationships, or conduit claims, with counsel (45 CFR 160.103; HHS Business Associates guidance).[1] No box checked? Document why, and re-check if the use changes.

*Scope note: this checklist covers federal HIPAA. State privacy, medical-records, and breach-notification laws may impose stricter vendor requirements; confirm your state's rules with counsel.*

## Part B. The offered BAA contains the required elements (45 CFR 164.504(e))

☐ States the permitted and required uses and disclosures of PHI by the vendor.

☐ Prohibits use or disclosure beyond the contract or as required by law.

☐ Requires appropriate safeguards, including Security Rule compliance for ePHI.

☐ Requires the vendor to report unauthorized uses and disclosures, including breaches of unsecured PHI.

☐ Makes PHI available for patient access, amendment, and accounting of disclosures.

☐ Requires compliance with Privacy Rule obligations the vendor performs for us.

☐ Makes the vendor's books and records available to HHS.

☐ Requires return or destruction of PHI at termination, if feasible.

☐ Flows the same restrictions down to the vendor's subcontractors.

☐ Authorizes termination for material violation.

## Part C. Questions the BAA alone will not answer

☐ **Training:** Is our data used to train or improve the vendor's models? Where is that stated in writing, and can we opt out?

☐ **De-identification rights:** Does the contract let the vendor de-identify our PHI and keep using it? (HHS model language treats this as an optional provision. It is a business decision, not a default. Strike it or price it.)

☐ **Retention:** How long are recordings, transcripts, and drafts kept? Can we set retention to the minimum our workflow needs?

☐ **Location and subcontractors:** Where is data stored and processed, and which subcontractors touch it? Are they under equivalent agreements?

☐ **Breach clock:** How quickly does the vendor notify us of a breach, in hours or days, in writing?

☐ **Exit:** At termination, how do we export our data, and what proof of destruction do we receive?

## Part D. Red flags requiring resolution before approval

- The vendor will not sign a BAA but says the product is "HIPAA compliant." Compliance claims without a BAA transfer nothing.
- The product permits or technically processes PHI on a tier for which the vendor will not execute a BAA.
- Consumer-grade terms of service govern clinical data.
- The vendor cannot say, in writing, whether your data trains their models.
- Nobody at the vendor can name their subcontractors that touch PHI.
- Patient data is stored or processed outside the United States, and the vendor cannot document adequate safeguards or contractual protection for it.

## Disposition

**Decision (approve / reject / conditions):**

_____

**BAA signed date:** _____

**Next review date:** _____

# Chart A. The 18 Safe Harbor identifiers

**45 CFR 164.514(b)(2)(i)**

## What must be removed

| | | | |
|---|---|---|---|
| **A** | Names | **J** | Account numbers |
| **B** | Geographic subdivisions smaller than a state | **K** | Certificate and license numbers |
| **C** | All elements of dates except the year | **L** | Vehicle identifiers and serial numbers |
| **D** | Telephone numbers | **M** | Device identifiers and serial numbers |
| **E** | Fax numbers | **N** | Web addresses (URLs) |
| **F** | Email addresses | **O** | Internet Protocol (IP) addresses |
| **G** | Social Security numbers | **P** | Biometric identifiers |
| **H** | Medical record numbers | **Q** | Full-face photographs and comparable images |
| **I** | Health plan beneficiary numbers | | |
| **R** | Any other unique identifying number, characteristic or code | | |

**Three carry conditions.** (B) the first three digits of a ZIP code may remain only where that three-digit area holds more than 20,000 people, otherwise it becomes 000. (C) all ages over 89, and any date element implying such an age, may be aggregated as "90 or older". (R) is the catch-all: a rare diagnosis or an unusual occupation identifies a person without appearing on this list by name.

## The same note, twice

Both notes below describe the same invented visit. Neither contains a real patient, a real practice, or real contact details.

**SCRUBBED OF THE OBVIOUS, AND STILL NOT DE-IDENTIFIED**

> Follow-up March 14, 2026. 91-year-old retired air traffic controller, referred in from the county clinic, first seen February 2. Treated for a rare connective-tissue disorder; the only patient in our panel with it. Tolerating the current regimen well. Next visit in April.

The name, the contact details, the record number and the photograph are already gone. Three categories remain, and only one of them looks like an identifier. The three dates and the age over 89 are all (C). The county is (B), because any geography below state level counts. The occupation and "the only patient in our panel with it" are both (R), the catch-all, and between them they would identify this person to anyone holding the panel.

**THE SAME VISIT, DE-IDENTIFIED UNDER SAFE HARBOR**

> Follow-up in 2026. Patient aged 90 or older, referred from an outside clinic, first seen earlier the same year. Treated for a connective-tissue disorder. Tolerating the current regimen well. Next visit later the same year.

**Eighteen is still not always enough.** If only one patient in your practice has this diagnosis, the second note may fail the actual-knowledge condition. The categories will not tell you that; your attorney will.

## REFERENCES

Check our work.

*Numbered in the order they are cited.*


1. US Department of Health and Human Services. Business associates. Accessed August 30, 2026. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates

2. US Department of Health and Human Services. Business associate contracts: sample business associate agreement provisions (45 CFR §164.504(e)). January 25, 2013. Accessed August 30, 2026. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions

3. US Department of Health and Human Services. Minimum necessary requirement. Accessed August 30, 2026. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement

4. US Department of Health and Human Services, Office for Civil Rights. Guidance on risk analysis. Accessed August 30, 2026. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis

5. US Department of Health and Human Services. Guidance regarding methods for de-identification of protected health information in accordance with the HIPAA Privacy Rule (45 CFR §164.514). Accessed August 30, 2026. https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification

6. US Department of Health and Human Services. HIPAA Security Rule NPRM. Accessed August 30, 2026. https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm

7. HIPAA Security Rule to strengthen the cybersecurity of electronic protected health information. 90 Fed Regist 898 (January 6, 2025) (proposed rule; document 2024-30983). Accessed August 30, 2026. https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information