GUIDE · HIPAA · PLAIN LANGUAGE

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

The rules of the road for putting AI tools anywhere near patient information, in plain language, with every claim cited to HHS itself.

PREPARED FOR YOUR LEGAL COUNSEL
This is a template prepared for you to take to your own attorney. Have your legal counsel review and adapt it for your state and your practice before you adopt it, use it in your practice, or put anything from it in front of patients. Laws vary by state; this is not a final legal instrument and is not legal advice.

WHAT THIS IS
A plain-language orientation to how existing HIPAA rules apply when a private medical practice adopts AI tools. It cites official HHS and OCR guidance throughout. It simplifies; the regulations control.

HOW TO USE IT
Read once before vetting any AI vendor. Keep it next to the BAA and Vendor-PHI Checklist when you do the vetting. Bring questions it raises to your attorney; that is what this document is for.

First principle: determine 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). HHS's own examples include an independent medical transcriptionist, the closest older cousin of an AI scribe. If an ambient scribe, transcription tool, or AI assistant touches identifiable patient information on your behalf, it is almost certainly a business associate.

The consequence: a business associate agreement (BAA) must be signed before PHI flows. When a vendor is acting as your business associate, PHI should not flow until an appropriate BAA is in place. The required contents of a BAA are listed at 45 CFR 164.504(e), and HHS publishes model language (cited below). The BAA and Vendor-PHI Checklist in this library walks the required elements one by one.

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)). A scribe 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. Adding an AI scribe 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 chatbot. HIPAA recognizes exactly two de-identification methods: **Safe Harbor**, removing 18 categories of identifiers (names, all dates more specific than year, full-face images, device identifiers, and more) with no actual knowledge the remainder could identify the person; or **Expert Determination** by a qualified statistician (45 CFR 164.514). A visit story with age, date, and rare diagnosis can identify a patient with the name long gone.

Personal accounts are the leak

A particularly foreseeable and hard-to-control AI risk is not the vetted scribe. It is PHI pasted into a free personal chatbot account to draft a letter. No BAA. No practice control. Some consumer health apps outside HIPAA may, depending on their functions, fall under the FTC's Health Breach Notification Rule, which is a rule about what happens after it goes wrong. Your policy and training (Stage 3 of this library) are what prevent it.

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

HIPAA is a floor, not a ceiling. State privacy, medical-records, breach-notification, and recording laws may impose requirements beyond HIPAA (for example, a state breach-notification statute such as Nevada's NRS Chapter 603A), and substance-use-disorder records under 42 CFR Part 2 — along with many state behavioral-health and minor-consent laws — carry their own limits before any information reaches an AI tool. Confirm your state's rules 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. 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 chatbot accounts are never the place for PHI.

SOURCES · CHECK OUR WORK

HHS. Business Associates. hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates

HHS. Sample Business Associate Agreement Provisions (45 CFR 164.504(e)). hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions

HHS. Minimum Necessary Requirement. hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement

HHS/OCR. Guidance on Risk Analysis. hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis

HHS. De-identification Guidance (45 CFR 164.514). hhs.gov/hipaa/for-professionals/special-topics/de-identification

HHS. HIPAA Security Rule NPRM. hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm

Federal Register, Jan 6, 2025. HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information. federalregister.gov/documents/2025/01/06/2024-30983

FTC. Health Breach Notification Rule. ftc.gov/legal-library/browse/rules/health-breach-notification-rule