TEMPLATE · GOVERNANCE · KEYSTONE DOCUMENT

The AI policy your practice *should have had last year.*

A plain-language written AI policy template for a private medical practice. Written by a nurse, not a software vendor's legal team.

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 fill-in-the-blank AI use policy covering approved tools, prohibited uses, PHI rules, clinician review, patient notice, training, and incident reporting. Bracketed [ITEMS] are decisions your practice must make; the surrounding language is a starting point for your attorney, not a finished instrument.

HOW TO USE IT
Read it once fully. Fill the brackets with your attorney. Adopt it at a staff meeting (the Staff AI Conversation Script pairs with that meeting), collect signed acknowledgments, and calendar the review. A policy is useful only when it is adopted, communicated, trained, enforced, and kept current; signed acknowledgments document that staff received it.
Policy control — complete on adoption: Effective date _____ · Adopted by _____ · Policy owner _____ · Version _____ · Next review _____

1. Purpose and scope

[PRACTICE NAME] permits AI tools only as reviewed and approved under this policy when the use involves practice information — PHI, confidential or internal business information, patient communications, clinical content, employment or personnel information, credentials, or financial data — and prohibits all other AI use of that information. Public, non-confidential information (for example, already-published material) may be used only as the practice authorizes and subject to accuracy and intellectual-property requirements. This policy applies to every owner, clinician, employee, contractor, and student, on any device, personal or practice-owned, whenever practice information is involved.

This policy supplements and does not replace the practice's existing HIPAA Privacy, Security, sanctions, and breach-notification policies; where they overlap, the more protective requirement governs, and nothing in this policy waives any obligation under HIPAA or the practice's other policies. [ATTORNEY/PRACTICE: confirm precedence for our practice.]

2. Definitions

- **AI tool:** any software that generates, summarizes, transcribes, drafts, or decides using machine learning or a language model. This includes chatbots, ambient scribes, dictation with AI features, browser extensions, and AI features inside existing products (EHR, email, office suites).
- **PHI: individually identifiable health information protected by HIPAA when created, received, maintained, or transmitted by a covered entity or business associate. It may include names, dates, contact information, images, recordings, medical details, and combinations of information that identify or could reasonably identify an individual.**
- **Approved tool:** a tool listed on the practice's Approved AI Tools List, used within the limits written there.
- **Business associate agreement (BAA):** the written contract HIPAA requires before a vendor creates, receives, maintains, or transmits PHI on the practice's behalf.

3. The core rules

- **Rule 1.** No PHI enters any AI tool that is not on the Approved AI Tools List with "PHI permitted" marked yes and a signed BAA on file.
- **Rule 2.** Every AI-generated clinical note, letter, or message is reviewed and approved by the responsible clinician before it is signed, sent, or filed. The clinician must review the note for accuracy, completeness, and clinical appropriateness before approving or signing it, and remains responsible for the professional, documentation, billing, and organizational obligations that apply to the final note.
- **Rule 3.** No recording of patient encounters without the notice and consent procedure in Section 6.
- **Rule 4.** AI output never substitutes for clinical judgment. It drafts; it does not decide.
- **Rule 5.** Staff complete the training in Section 7 before receiving access to any approved tool. Training first, tools second.

4. Approved tools and the approval process

The practice maintains an Approved AI Tools List (template provided in this library) naming each approved tool, what it may be used for, whether PHI is permitted, the BAA date, and the review date. [ROLE, e.g., PRACTICE OWNER or PRIVACY OFFICER] owns the list. To request a new tool, staff submit the request to the list owner, who vets it using the practice's vendor checklist (BAA and Vendor-PHI Checklist, and the AI Scribe Vetting Checklist for documentation tools) before any use begins.

5. PHI and HIPAA requirements

- A vendor whose tool creates, receives, maintains, or transmits PHI on our behalf is a business associate, and a BAA meeting 45 CFR 164.504(e) must be signed before any PHI flows (see HHS sample provisions, cited below).
- Where the minimum necessary standard applies — and as a prudent data-governance default even where a technical exception may exist — an AI tool receives only the PHI its approved task requires (45 CFR 164.502(b)).

- Adding or materially changing an AI tool that creates, receives, maintains, or transmits ePHI requires the practice to assess and document the resulting risks as part of its ongoing Security Rule risk-analysis and risk-management process, and to update safeguards or the documented analysis as appropriate (45 CFR 164.308(a)(1)(ii)(A) and OCR risk analysis guidance).
- Removing patient names alone does not de-identify PHI. De-identification requires the Safe Harbor removal of 18 identifier categories or expert determination (45 CFR 164.514).
- Classify practice information before it goes near AI. A simple scheme works — public, internal, confidential, and restricted. PHI and any identifiable patient information is restricted: it never enters an AI tool that lacks the "PHI permitted" approval and a signed BAA, and never a personal or consumer account.
- **State law may be stricter than HIPAA.** State privacy, medical-records, breach-notification, and recording laws can impose requirements beyond HIPAA; confirm your state's rules, and any telehealth patient's state, with counsel.
- **Substance-use and behavioral-health records carry extra rules.** If the practice handles 42 CFR Part 2 substance-use-disorder records, or is subject to state behavioral-health or minor-consent confidentiality laws, additional restrictions apply before any such information reaches an AI tool — confirm with counsel.

6. Patient notice and consent for recording

Before any encounter is recorded for ambient documentation: [DESCRIBE PROCEDURE, e.g., verbal notice at the start of each visit plus posted signage, with consent documented in the record and an opt-out honored without affecting care]. Several states require all-party consent to record a conversation; this practice treats all-party consent as the default everywhere. [ATTORNEY: confirm requirements for OUR STATE and any state our telehealth patients are located in.]

7. Training

Before access, each user completes: how the approved tool works and its known failure modes (for scribes: omission errors are the most frequent error type found in validation research); what PHI may and may not enter it; the review-before-signing requirement; and how to report a suspected error or breach. Refreshed [ANNUALLY].

8. Good-faith incident reporting and non-retaliation

Anyone who suspects PHI entered an unapproved tool, or that an AI error reached a patient record, reports it to [PRIVACY OFFICER / OWNER] the same day. The practice prohibits retaliation against an individual because the individual made a good-faith report, requested guidance, or took part in an investigation; prohibited retaliation includes termination, demotion, suspension, reduced compensation, reassignment, or any other adverse action taken because of a good-faith report. That protection does not shield the underlying conduct: the practice may still evaluate it under its existing privacy, security, sanctions, and employment policies, considering intent, recurrence, and cooperation, and a knowingly false or malicious report is itself subject to discipline.

Nothing in this section alters the at-will employment relationship or creates any contractual right; only a written agreement signed by an authorized representative of the practice can do that. The goal of this policy is a managed practice, not a scared one. [ATTORNEY: confirm this non-retaliation and at-will language for our state and employment posture.]

A report under this section starts, and does not replace, the practice's breach-assessment process: promptly assess the nature and scope, contain it where practicable, and determine whether notification is required under 45 CFR 164.400–414 and any applicable state breach-notification law (for example, in Nevada, NRS Chapter 603A). Notify affected individuals, HHS, and any others as that assessment and those laws require.

9. Personal devices and personal accounts

Practice information never enters personal AI accounts (personal chatbot logins, free consumer apps) regardless of device. Approved tools are used only under practice-controlled accounts, so the practice can enforce settings, retention, and the BAA.

10. Review

This policy is reviewed on a set interval (for example, every 6 or 12 months, as the practice decides), and immediately upon: a new tool approval, a reported incident, or a change in law or guidance. Note: HHS has proposed updates to the HIPAA Security Rule (proposed rule published January 6, 2025); the current Security Rule remains in effect while rulemaking proceeds. Your attorney should confirm current status at each review.

Acknowledgment (each staff member signs)

I have read and understood the [PRACTICE NAME] AI Use Policy. I agree to use only approved AI tools, within their approved limits, and to report suspected incidents the same day I become aware of them.

Name: _____

Role: _____

Signature: _____

Date: _____

SOURCES · CHECK OUR WORK

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

HHS. Sample Business Associate Agreement Provisions. 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. hhs.gov/hipaa/for-professionals/special-topics/de-identification

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

AMA. Augmented Intelligence Development, Deployment, and Use in Health Care (principles). ama-assn.org/system/files/ama-ai-principles.pdf

AMA STEPS Forward. Governance for Augmented Intelligence. edhub.ama-assn.org/steps-forward/module/2833560

NIST. AI Risk Management Framework (AI RMF 1.0). nist.gov/itl/ai-risk-management-framework

Biro J, et al. Accuracy and Safety of AI-Enabled Scribe Technology. J Med Internet Res. 2025;27:e64993. jmir.org/2025/1/e64993