

AI Acceptable-Use Policy - Small Healthcare Practice Template

Provided by Zabcore, maker of AI Leak Guard. This is a starter template you can adapt for your own practice. It is not legal advice; have your compliance advisor review before adopting.

Version: 1.0 (August 2026) **Effective:** [Insert date] **Applies to:** All workforce members of [Practice name], including physicians, dental providers, nurses, front-office staff, medical billers, and any contractors with access to practice systems or patient information.

1. Purpose

AI tools (ChatGPT, Claude, Gemini, Perplexity, Microsoft Copilot, and similar) are legitimately useful for drafting correspondence, summarising notes, writing insurance appeals, explaining procedures, and other administrative tasks. This policy sets clear rules for using them in a way that protects patients, complies with HIPAA and applicable state law, and preserves the practice's professional standing.

This policy does not ban AI tools. It defines how to use them safely.

2. Scope

This policy covers use of any generative AI service (chat interface, browser plugin, mobile app, or API) accessed on:

- Practice-owned devices
 - Personal devices used for practice work
 - Any account (personal or professional) used to interact with practice patients or their information
-

3. Definitions

- **Patient identifier** - any information that identifies a specific patient, including but not limited to: full or partial name, date of birth, address, phone number, email, medical record number (MRN), insurance member or subscriber ID, claim number, prescription number, Social Security number, license number, or any combination of two or more indirect identifiers that could reasonably identify the patient (e.g. "the 87-year-old male with pancreatic cancer we saw Tuesday").

- **Consumer AI account** - any AI service account created without a Business Associate Agreement (BAA) between the provider and the practice. OpenAI, Anthropic, Google, Microsoft, and Perplexity do not offer BAAs on consumer chat products (ChatGPT, Claude.ai, Gemini, standard Copilot, Perplexity) as of this policy's effective date.
 - **Approved AI tool** - an AI service or interface that the practice has formally approved for handling patient information, backed by a signed BAA or equivalent safeguard, and configured by the practice's IT contact.
-

4. Prohibited Uses

Workforce members must not, at any time:

1. Paste, type, upload, or dictate any patient identifier into a consumer AI account.
 2. Upload documents containing patient identifiers (referral letters, lab reports, EOBs, insurance denials, imaging reports, correspondence, or any other file) to a consumer AI account.
 3. Screenshot patient records or dashboards for the purpose of asking a consumer AI account to interpret them.
 4. Use a consumer AI account to draft any communication that references a specific patient by name, DOB, MRN, or other identifier.
 5. Use a consumer AI account to generate patient-facing content that appears to be authored by a licensed provider unless the content is reviewed and approved by that provider before sending.
 6. Configure AI tools with any browser extension, autocomplete, or dictation service that transmits captured text off-device without explicit approval from the practice's designated IT contact.
 7. Bypass, disable, or attempt to circumvent any tool the practice has deployed to detect or prevent patient information from being pasted into AI tools (including AI Leak Guard or equivalent).
-

5. Permitted Uses

Workforce members may use consumer AI accounts to:

1. Draft general correspondence that contains no patient identifiers (policy language, generic outreach emails, form letters with placeholders).
2. Explain a diagnosis, treatment, procedure, or medical concept in plain language, using only generalised or hypothetical patient details (e.g. "a 60-year-old with elevated A1c", not "John Miller, DOB 5/12/1948, with A1c 8.9").
3. Draft insurance appeals when patient identifiers have been replaced with placeholders (e.g. [PATIENT_NAME], [MRN], [INSURANCE_ID]) either manually or by a tool such as AI Leak Guard.

The clinical justification (CPT codes, denial reasons, comorbidities) may be included as long as it does not indirectly identify the patient.

4. Research CPT codes, ICD-10 codes, drug interactions, clinical guidelines, and reimbursement rules.
 5. Improve grammar, clarity, or tone of documents that contain no patient identifiers.
 6. Learn how to use practice software, spreadsheets, or general business tasks.
-

6. Recommended Safeguards

The practice recommends that workforce members using AI tools for permitted purposes:

1. Install a browser-based identifier detection tool such as **AI Leak Guard** (free at zabcore.com) on every browser used for practice work. This provides a second-line check before patient information reaches an AI tool, whether typed, pasted, or attached as a file. It also keeps a local activity view (counts, categories, site, time - never content or filenames) that individual workforce members can export to CSV or JSON on their own device for their own records.
 2. Use the placeholder pattern in prompts (e.g. [PATIENT_NAME], [MRN], [DOB]) as a habit, even for non-identifying context. Building the habit prevents mistakes.
 3. Review any AI-generated content before using it for patient communication, insurance filing, or clinical documentation. AI tools are known to fabricate confident-sounding but incorrect information.
 4. When in doubt, do not paste. Ask the practice's designated IT contact or compliance advisor.
-

7. Incident Reporting

If a workforce member believes they have pasted, uploaded, or transmitted patient identifiers to a consumer AI account, whether intentionally or by accident, they must:

1. Stop using the AI tool immediately.
2. Report the incident to [designated privacy officer / practice manager] within one business day.
3. Document what was shared (as best they can recall), when, and to which service.

The practice will assess whether the incident constitutes a breach under HIPAA and applicable state law, and will notify affected patients and regulators as required.

Good-faith reporting will not result in disciplinary action for the reporter. Failure to report a known incident may.

8. Enforcement

Violations of this policy may result in:

- Retraining
- Written warning
- Suspension of access to practice systems
- Termination
- Referral to the appropriate licensing board where relevant
- Referral to law enforcement where warranted

The specific consequence will depend on the nature and severity of the violation, whether it was intentional or accidental, whether it was reported voluntarily, and whether patient harm resulted.

9. Review

This policy will be reviewed at least annually and updated as AI tools, regulations, and industry practice evolve. Workforce members will be notified of material changes and asked to re-acknowledge the updated policy.

10. Acknowledgement

By signing below, I acknowledge that:

- I have read and understand this policy.
- I have received training on identifying patient identifiers and using AI tools safely in a healthcare setting.
- I understand that violations may result in disciplinary action up to and including termination.
- I will report incidents promptly.

Workforce member name: _____

Role: _____

Signature: _____ **Date:** ____

Practice representative: _____

Signature: _____ **Date:** ____

Appendix A: Quick Reference Card

A one-page checklist for daily use is provided separately: **"Before You Paste or Upload to AI: A 30-Second Check for Healthcare Staff."** Print it, tape it near the workstation, refer to it whenever prompting an AI tool.

Appendix B: About This Template

This template was provided by **Zabcore**, an independent studio focused on privacy-first tools for healthcare workers. Zabcore is the maker of **AI Leak Guard**, a free browser extension that catches patient identifiers in your browser: send-time protection (v1.3) on ChatGPT, Claude, and Gemini (checks your message the moment you send it), and paste checking plus document scanning (PDF, Word, Excel, PowerPoint, text) also on Perplexity and Microsoft Copilot (copilot.microsoft.com). Detection happens entirely in your browser. Your text and files are never uploaded, stored, or sent anywhere by the extension.

- Free extension: [Add to Chrome](#)
- Learn more: zabcore.com
- For practice deployment: zabcore.com/practice

This template is not legal advice. Adapt it to your practice's specific situation and have a qualified compliance advisor review before adopting.