

Before You Paste or Upload to AI: A 30-Second Check for Healthcare Staff

Print this. Tape it near your workstation. Take 30 seconds before you hit Enter.

The five questions

1. Is this about a specific patient?

If the prompt names a person, includes a date of birth, references an appointment, or would let someone identify who you are asking about, it is a patient prompt. Even one detail is enough.

2. Are you using a personal AI account?

ChatGPT (chatgpt.com), Claude (claude.ai), Gemini (gemini.google.com), Perplexity, Microsoft Copilot on a personal Microsoft account, and every free chat you can log into with a personal Google or Apple ID are personal accounts. They have no Business Associate Agreement with your practice. Do not paste patient information into them.

3. Are you about to upload a file?

Referral letters, lab reports, EOBs, insurance denials, imaging reports, patient correspondence, and screenshots almost always contain patient identifiers. Do not upload them to a personal AI account, even if you think the AI will "only look at the numbers."

4. Would you be comfortable if this prompt appeared in a subpoena?

ChatGPT and similar tools store history. That history is discoverable in litigation. If seeing this prompt exactly as you typed it, with your account name attached, would embarrass your practice or breach a patient's trust, do not send it.

5. Can you replace the identifiers with placeholders?

Instead of `John Miller, DOB 5/12/1948, MRN 003847`, write `[PATIENT_NAME], DOB [DOB], MRN [MRN]`. The AI can still write the appeal, referral, or summary. It just cannot identify the patient.

Two safe patterns

Pattern A: Ask about a diagnosis or process, no patient attached.

"Explain how prior authorization works for Ozempic for a Medicare Advantage patient with type 2 diabetes and BMI over 30, who has failed metformin and Jardiance at max doses."

No name. No DOB. No MRN. Still gets you a useful answer.

Pattern B: Draft with placeholders, fill in later.

"Draft an insurance appeal for [PATIENT_NAME], member ID [INSURANCE_ID]. Denied CPT 99215 as not medically necessary despite documented comorbidities including hypertension, type 2 diabetes, and CKD stage 3."

The AI writes the appeal. You paste the real name and IDs into the letter yourself, from your EHR or billing system, before sending.

When you are not sure

Ask the practice's designated privacy contact or compliance advisor. If they are not available and you are unsure, do not paste. Nothing you will draft with AI is so urgent that it justifies a HIPAA disclosure.

Safety net: install AI Leak Guard

AI Leak Guard is a free Chrome extension that catches patient identifiers in your browser. Send-time protection (checks your message the moment you send it) runs on ChatGPT, Claude, and Gemini. Paste checking and document scanning (PDF, Word, Excel, PowerPoint, or text files you attach) also cover Perplexity and Microsoft Copilot (copilot.microsoft.com). Send-time protection on Perplexity and Copilot is planned for a later release.

For paste, when it sees a name, DOB, MRN, phone, address, insurance ID, claim number, or similar identifier in what you are about to paste, it shows you a preview and lets you choose to send the safe version, send as-is, or cancel. For an attached file, it reads the file on your device and warns you which identifiers were found; you choose to upload anyway or cancel. The extension does not edit or redact your file, it just tells you what is in there before it leaves your device.

Microsoft 365 Copilot (the work or school version at m365.cloud.microsoft) is not covered for document uploads: those files are handled inside your organization's Microsoft 365 environment and are governed by your Microsoft 365 and Purview controls.

It runs entirely in your browser. Nothing goes to Zabcore's servers. Free forever for individuals.

Add to Chrome: zabcore.com/install

More at: zabcore.com

Zabcore, 2026. Not legal advice. Adapt to your practice's specific compliance requirements.