

The Practice Owner's Guide to **AI** — Without the Compliance Headache

What AI can actually do in your practice, what it can't, and the one obligation almost every practice overlooks before they start.

AI is coming into your practice whether you plan for it or not

Your front desk has already seen the ads. "AI scheduling." "AI notes." "AI phone answering." Some of your staff may already be pasting patient information into free AI tools to save time. That's the part that should concern you.

Here's the honest truth most vendors won't lead with: **the risk isn't adopting AI — it's adopting it without a compliance foundation underneath.** The moment an AI tool touches patient information, you've created new HIPAA obligations. Not "might have." Have.

Most practices discover this backwards — after a tool is already in use, after data has already moved, sometimes after an insurance renewal or an audit puts the question in front of them. This guide is about getting ahead of it: understanding what AI can genuinely do for a practice like yours, what it can't, and the single question to settle *before* you turn anything on.

ONE LINE TO REMEMBER

Adding AI to a practice that hasn't documented its security posture doesn't make you modern — it makes you the practice that adopted new patient-data risk without writing it down. The order matters: **foundation first, then AI.**

You don't need to become a technology expert. You need to ask a handful of the right questions and have someone accountable for the answers. The rest of this guide gives you exactly those questions.

What AI can actually do in a practice like yours

Set aside the clinical headlines for a moment. The AI that pays for itself in a small or mid-sized practice isn't diagnosing anything — it's giving your front office its hours back. Here's the grounded menu.

Patient engagement & communication

The front-desk load, handled around the clock.

- Intelligent scheduling and automated reminders that cut no-shows
- After-hours call capture — every new-patient call answered, triaged, and booked instead of going to voicemail
- Recall, follow-up, and review-request outreach that runs itself

Front-office workflow automation

The administrative hours nobody has time for.

- Intake processing — turning forms and calls into clean records
- Referral routing and insurance-verification prep
- Cutting repetitive data entry so staff focus on patients, not paperwork

Where we draw the line — on purpose

This guide is about **operational and administrative AI**: scheduling, intake, communication, front-office workflow. It is **not** about clinical AI — imaging analysis, diagnosis, or clinical decision-making. That's a different world with different regulation, different liability, and different vendors.

We're deliberately staying on the side of AI that saves your staff time and is safe to deploy in a well-governed practice. If a tool promises to practice medicine, that's a conversation for you and your clinical team — not an IT decision.

Notice what these have in common: every one is a **time-and-money** win, not a "look how advanced we are" win. That's the right lens. If an AI tool can't tell you which staff hours it gives back, it's a toy, not an investment.

03 • THE PART VENDORS SKIP

The compliance layer nobody puts on the sales page

Here's where "fun AI tool" quietly becomes "documented HIPAA exposure." When AI touches patient information, three things have to be true — and most practices can't confirm any of them.

1. The vendor must sign a Business Associate Agreement (BAA)

If an AI tool handles protected health information on your behalf, it's a business associate under HIPAA. No signed BAA means you're sharing patient data with a vendor that hasn't agreed to protect it the way HIPAA requires. Many popular consumer AI tools **will not sign one** — which alone rules them out for anything touching PHI.

2. The vendor must not train on your patients' data

"Where does our data go, and what do you do with it?" is not a rude question — it's a required one. Some tools use the data you feed them to train their models. For patient information, that's unacceptable, and it needs to be barred in writing.

3. It all has to show up in your Security Risk Analysis

Every system that touches PHI belongs in your HIPAA **Security Risk Analysis** — the annual, required assessment of where patient data lives and how it's protected. Adding an AI tool and *not* updating that analysis is exactly the gap an auditor or an insurer looks for.

THE UNCOMFORTABLE QUESTION

When was your last Security Risk Analysis — and could you produce it if your cyber-insurance carrier or a regulator asked tomorrow? If that question made you pause, that pause *is* the finding. It's also the right place to start, before any AI decision.

04 • KEEP THIS PAGE

5 questions to ask before you buy any AI tool

Print this. Tape it to the office manager's monitor. Any AI vendor who can't answer all five, in writing, isn't ready for a practice that handles patient data.

1

Will you sign a Business Associate Agreement?

If the answer is no — or "what's that?" — the conversation is over for anything touching PHI.

2

Where does our data physically go, and who can access it?

Cloud region, subprocessors, staff access. Vague answers are a red flag.

3

Do you train your models on the data we put in?

For patient data the only acceptable answer is a documented, contractual "no."

4

Can we get an audit trail of what the tool accessed and did?

If you can't see it, you can't defend it in an audit or after an incident.

5

Is this tool reflected in our Security Risk Analysis?

This one's on you, not the vendor — and it's the one most practices miss.

If you can't answer question five for the tools you *already* use, you've just found your starting point — and you're far from alone.

05 • THE SANE SEQUENCE

Where to start — without boiling the ocean

You do not need an "AI transformation." You need three steps in the right order. Ignore anyone selling you all of it at once.

1

Document your foundation first

Get a current Security Risk Analysis done. Know where patient data lives and how it's protected today. This is required regardless of AI — and it's the map for everything after.

2

Start with front-office AI, not clinical

Scheduling, reminders, after-hours call capture, intake. Low risk, fast payback, staff feel the relief in weeks. Prove the value where the stakes are lowest.

3

Expand deliberately, with compliance keeping pace

Every new tool goes through the five questions and into your risk analysis before it goes live. Growth with a paper trail, not growth you'll have to explain later.

The whole strategy in one sentence

Get your compliance foundation documented, adopt front-office AI where the payback is fast and the risk is low, and let your paperwork keep pace with your tools — so AI makes your practice more efficient **and** more defensible, not less.

THE RIGHT FIRST STEP

Before you add AI, know where you stand.

Everything in this guide starts from the same foundation: a current, honest picture of where your patient data lives and how it's protected. That's the HIPAA Security Risk Analysis — required anyway, and the natural first step before any AI decision.

TampaTeks HIPAA Security Risk Analysis

A fixed-fee, fixed-scope assessment delivered in 10 business days. You get the required report, a plain-English risk plan, and a clear picture of where you stand — including any AI tools already in use.

The fee credits back in full against a managed agreement signed within 60 days. Engage us, and the assessment was free.

No pressure, no jargon — a local Tampa team that shows up before there's a problem. Serving practices since 2005.

Book a conversation · **813-417-5349** · tampateks.com

This guide is general information for practice operators, not legal or compliance advice. HIPAA obligations vary by practice; a Security Risk Analysis provides the specifics for yours. TampaTeks provides IT, security, and operational AI services — not clinical or medical services.