AI Self-Defense for Private Practice

The same qualities that make AI useful, that it is cheap, fast, and sounds like a person, make it the best fraud tool ever built. Physicians are a high-value target, with a public name and photo, an NPI, an office that moves money on emailed instructions, and aging parents. Everything on this page is free and can be done today.

THE THREE SCENARIOS THAT MAY REACH YOU

The voice that sounds like family. Sixty seconds of audio from a conference talk or a voicemail greeting is enough to clone anyone. The call goes to your spouse, your child, your parents, or your office manager. It is always urgent and it always needs money or a password.

The vendor who changed banks. A reply inside an existing email thread, in the vendor's real voice, with new wiring instructions. AI removed the typos that used to give these away. Your billing company and bank can get the same scam, sent in your name.

Your face, selling something. A video of you endorsing a supplement. A telehealth site with your name and headshot. A wave of one-star reviews written overnight. Your front desk hears about it from patients first.

> Urgency is the giveaway. A real emergency survives a hang-up and callback. A scam does not.

USE AI TO FIGHT BACK

The prompts on the back check an email or text for scams and draft your AI policy. No patient information goes into an AI tool without a signed business associate agreement (BAA). Personal accounts, free or paid, do not include one.

SAY THIS, THEN HANG UP

TO THE CALLER

"I am going to hang up and call you back at the number I have. What is our safe word?"

TO THE VENDOR

"Thanks. I will confirm the new account by phone with the contact on file before anything changes."

TO THE PATIENT ASKING ABOUT YOUR VIDEO

"That is not me. Please do not buy anything, and thank you for telling us."

FIVE THINGS TO DO TODAY

1. **Pick a family safe word.**
   One word, shared in person, never texted. Any call asking for money or secrets gets asked for it. Include your parents. If you have kids, turn on parental controls to limit screen time, filter content, and restrict chat rooms.
   2 minutes

2. **Post the callback rule.**
   No payment, wire, bank change, gift card, or password reset on a call or email alone. Someone calls back the number already on file.
   10 minutes, one page, on the wall

3. **Lock your key accounts and your credit.**
   Use a password manager. Turn on passkeys or a hardware key for email, bank, EHR, and payroll. Where those are not offered, use an authenticator app, not text codes. Turn on automatic updates for your computer, phone, and apps. Freeze credit at Equifax, Experian, and TransUnion. Also freeze ChexSystems, which blocks new bank accounts in your name. All free.
   30 minutes, once

4. **Protect your own name.**
   Google Alert on your name and your practice. Look up your NPI at npiregistry.cms.hhs.gov and check that the address is yours. If you bill Medicare, have whoever manages your PECOS login confirm the bank account has not changed. Bookmark the "report a fake account" page on Facebook, Instagram, LinkedIn, and Google so you can act within minutes.
   15 minutes

5. **Write the practice AI rule.**
   Which tools staff may use, that no patient information goes into any tool without a BAA, and what to do when someone slips. Have AI draft it, then read it.
   10 minutes

This handout is general information, not legal, financial, or compliance advice. Verify current state law with counsel.

DEEPER DIVE

Why each one works, and what to do if it already happened

Know why each defense works, and you will spot the scam even in a new disguise.

1. The safe word VOICE CLONES

A voice clone copies how someone sounds, not what they know. A safe word lives only in your family's heads and was never typed anywhere a scammer could find it. Cloning tools need less than a minute of audio, so if you have ever given a talk or recorded a voicemail greeting, assume you can be cloned. Older parents get these calls most because they are home and they answer. Talk with your parents this week and keep the rule simple: the caller says the word, or you hang up and call back.

2. The callback rule FAKE PAYMENT EMAILS

An email proves nothing about who sent it. Calling back a number you already had on file forces the scammer to fake a second channel, which they almost never can. Having two people approve every payment works for the same reason: the scam is built to rush one person. Put the rule in writing so a new hire follows it on day one, and tell your bank and billing company to follow it too.

```
Is this email or text a scam? List the warning
signs and what to do. [paste the message or attach
a screenshot, no patient information]
```

3. Locking your accounts PASSKEYS AND FREEZES

A password or texted code typed into a fake login page can be passed straight to the real site. A passkey only works on the real website, so a fake page gets nothing, which is the whole reason to switch. Where passkeys are not offered, an authenticator app is next best. A credit freeze works the same way for your identity, since no lender can open an account in your name until you unlock it, and it is free. ChexSystems is the freeze most people miss, and it covers new bank accounts, where stolen identities become cash.

4. Protecting your name LIKENESS AND LICENSE

You cannot stop someone from making a deepfake of you, but you can catch it sooner. A Google Alert tells you early, and a profile on each platform, even one you never post on, gives you a verified account to report from. Your NPI and DEA numbers are worth more to a scammer than your credit card. Once a year, check your NPI address and, if you bill Medicare, your PECOS bank details. Watch your state PDMP for prescriptions you did not write, and read your payment statements for services you never provided. Most states let you sue when someone uses your face to sell something. Have an attorney's name ready before you need one.

aiforprivatepractice.com/rppa

5. The practice AI rule HIPAA AND YOUR STAFF

Your staff will use AI whether or not you have a policy. Free chatbots do not sign business associate agreements, so if a staff member pastes a patient note into one, your practice is responsible for the breach. Preventing it takes a one-page policy, not a big program. Name the approved tools, state the rule, and say what to do the moment someone slips. Also read the AI section of every EHR, scribe, and billing contract, because some vendors train their AI on your data unless you opt out. Start with this prompt, then edit what it gives you.

```
Draft a one-page AI acceptable-use policy for
a small rheumatology practice. Cover which
tools are approved, who our privacy officer
is, the rule that no patient information
enters any tool without a signed BAA, how
staff report an accidental disclosure, and how
every staff member signs it at hire and each
year. Plain English, no legalese.
```

Also on the horizon

Scammers are using deepfake video to apply for remote billing jobs, so check ID in person for anyone who will handle money or charts. Before you sign with an AI scribe, read the contract and find out whether your state requires you to tell patients. For cyber insurance, ask your malpractice carrier and any broker, in writing, whether you have cyber coverage, what the limit is, and whether it covers scams that trick staff into sending money. Many malpractice policies include a small cyber add-on that does not.

If it already happened

If a scammer is on the line or on your computer, stop talking, end any remote access session, and unplug the desktop, close the laptop lid, or pull the battery. **If money was wired,** call your bank's fraud line immediately, ask them to recall the wire, and report it at ic3.gov the same day. **If a clone or deepfake of you is spreading,** report it to the platform as impersonation, save screenshots with links and dates, and tell your state medical board if it makes claims about your practice. **If a password was stolen,** change it from a different device, sign out of all other sessions, turn on passkeys, and check your email for forwarding rules, which scammers add to keep reading your mail. **If patient information went into a chatbot,** do not panic. Delete the chat, write down what was shared and when, and tell your privacy officer that day. A short risk assessment decides whether it must be reported, and a small slip often ends with a note in the file. **If a relative sent money to a voice clone,** call their bank first, then file a police report, then report it at ic3.gov. While shame keeps people quiet, speed gets money back. **In every case,** save the messages and transaction records, and report at reportfraud.ftc.gov and ic3.gov, plus identitytheft.gov if your identity was used.

Sources worth your time

FBI IC3 annual report (ic3.gov) · FTC consumer alerts on voice cloning and impersonation (consumer.ftc.gov) · HHS Office for Civil Rights guidance on AI and business associates (hhs.gov/hipaa) · NPPES (nppes.cms.hhs.gov) and PECOS (pecos.cms.hhs.gov) · NCMEC Take It Down for minors (takeitdown.ncmec.org) · Your state medical board and PDMP.