Five things to do this week

Most break-ins at small practices start with a stolen password or a fake email. These five steps stop most of them. Each takes under an hour.

☐ 1. Turn on two-step login (MFA)

Start with email, then your records system (EHR), then banking. Use an authenticator app instead of text codes where you can. Email comes first: whoever controls your email can reset every other password.

☐ 2. Back up your records, and test it

Keep at least one copy that ransomware can't reach: offline, or locked so it can't be changed. If your records live in a cloud EHR, ask the vendor how they back up and how you would get your data out. Then restore one file to prove it works.

☐ 3. Turn on automatic updates

On every computer, phone and tablet used for work, and on your Wi-Fi router. Turn on disk encryption and a screen lock too, so a lost laptop is not a breach. Replace devices that no longer get security updates.

☐ 4. Slow down on money and login requests

Fake invoices and "please update our bank details" emails are the most common scam. Before changing payment details or sending money, call the person back on a number you already have, not one in the email. Never enter a password from a link you didn't expect.

☐ 5. Write down who to call

When something goes wrong, the first hour matters. Fill in the "Who to call" card (free on our site), print it, and keep a copy somewhere other than your computer.

Done all five?

You are ahead of most small practices. The next step is a written security risk analysis, which HIPAA requires of every covered practice.

General information for small practices, not legal advice. Free to copy and share with credit. © 2026 Edge Aspect. Version 1.0, November 2026.