Secure Roots
info@secureroots.io · 310-421-8132 · www.secureroots.io

The 12-Point HIPAA Security Risk Analysis Checklist

What your EHR vendor does NOT cover, and what your practice is on the hook for

A HIPAA Security Risk Analysis is required, not optional, and it has to cover your whole practice, not just your electronic health record system. Your EHR vendor secures their platform. Everything below is your responsibility. Score yourself: for each item, can you show a document that proves it?

Administrative

1. A current, written Security Risk Analysis exists and was updated within the last 12 months.
2. One person is clearly designated as responsible for security and privacy.
3. Written policies exist for passwords, access, mobile devices, and remote work.
4. Staff receive security awareness training, and you can show they completed it.
5. Business Associate Agreements are signed with every vendor that touches patient data (billing, IT, cloud, shredding).

Technical

1. Multi-factor authentication is turned on for email, the EHR, and remote access.
2. Patient data is encrypted on laptops, phones, and backups.
3. Each staff member has a unique login, and access ends the day someone leaves.
4. You have endpoint protection on every device, and someone actually monitors the alerts.
5. Backups run automatically AND you have tested a restore in the last 12 months.

Physical and Response

1. Screens, servers, and paper records are physically protected from unauthorized view or access.
2. A written breach-response plan exists, and you know who you must notify and when.

> **How did you score?** Most small practices can prove five or six of these. The other half is exactly where OCR investigations, denied insurance claims, and ransomware find you.

A note on the road ahead: federal regulators have proposed making several of these controls (multi-factor authentication, encryption, regular testing) mandatory rather than optional. That change is proposed, not yet final, but the direction is set.

Want a real Security Risk Analysis done, the one the law requires? We deliver it as a fixed-fee package, and it doubles as your MIPS attestation evidence.

Book a free 30-minute readiness check: info@secureroots.io · 310-421-8132

This checklist is a general educational resource, not legal or compliance advice for your specific practice.