

Cyber Insurance Readiness Checklist for Medical Practices

For Doctors' Offices, Dental Practices & Med Spas

SIM Technology Solutions • Healthcare IT & Compliance Guide • Updated September 2026

RISK MANAGEMENT

Cyber insurance applications for healthcare practices have gotten a lot more specific in the last few years. Carriers that used to ask a handful of yes/no questions now want proof, screenshots, policy documents, vendor attestations, before they'll bind or renew a policy. This checklist covers what carriers are typically asking for today, so you're not caught off guard mid-application or, worse, denied a claim because a control you attested to wasn't actually in place.

Why this matters more than it used to: Insurers have paid out enough ransomware claims that many now audit controls before binding coverage, and some reserve the right to deny a claim if you attested to a control (like MFA) that turns out not to have been implemented.

Controls Carriers Commonly Require

- ☐ Multi-factor authentication (MFA) on email, remote access (VPN/RDP), and any admin/privileged accounts, the single most-asked-about control on nearly every application
- ☐ Endpoint Detection & Response (EDR) on all workstations and servers; traditional antivirus alone increasingly fails to qualify
- ☐ Encrypted backups, stored separately from your main network, with at least one copy that's immutable (ransomware-resistant) or offline
- ☐ A documented, tested incident response plan, not just a mental checklist
- ☐ Regular patching cadence for operating systems and critical software, with a defined timeframe (e.g., critical patches within 30 days)
- ☐ Email security filtering (anti-phishing, anti-malware) beyond your inbox provider's default spam filter
- ☐ Privileged access management: admin rights limited to who actually needs them, not shared broadly
- ☐ Employee security awareness training completed on a recurring basis, with records to prove it
- ☐ A written data retention and disposal policy; carriers increasingly ask whether you're holding more data than you need to

Healthcare-Specific Questions to Expect

- Do you have a HIPAA Security Risk Analysis on file, and when was it last updated?
- Do you have signed Business Associate Agreements with your EHR, billing, and IT vendors?

- Who has access to PHI, and is that access reviewed periodically?
- Have you had a breach or security incident in the last 3–5 years, and if so, how was it handled?

Before You Apply or Renew

1. Pull your most recent Security Risk Analysis; if it's more than a year old, update it first
2. Confirm MFA is actually enforced everywhere the application asks about, not just “available”
3. Test a backup restore, don't just confirm backups are “running”
4. Gather your BAAs into one folder so you're not hunting for them under deadline
5. Have your IT provider (or internal IT lead) sit in on the application. A lot of these questions are technical, and a wrong answer can mean a denied claim later, not just a rejected application

A Note on Accuracy

It's tempting to answer “yes” to a control question because it's mostly true, or because you plan to have it in place soon. Don't. Cyber insurers have increasingly denied claims after a breach when the post-incident investigation showed a control the policyholder attested to wasn't actually implemented. Answer based on what's true today, then fix the gaps: that's a faster path to both real coverage and a lower premium than papering over them.

Applying for or renewing cyber coverage soon?

SIM Technology Solutions can get your MFA, EDR, and backup posture where it needs to be before you apply, and put together the documentation carriers ask for. **Call 703-594-9226** or email info@simtsolutions.com.