

Ransomware & Incident Response Guide for Healthcare Practices

Quick-Reference Guide for Medical Practices

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

SECURITY & RISK

Small and mid-sized healthcare practices are attractive targets: patient records are valuable on the black market, and many practices run leaner IT defenses than a hospital system while holding the same category of sensitive data. This guide covers why practices like yours get targeted, the warning signs, and exactly what to do, and notify, in the first hours of a suspected incident.

Why Healthcare Practices Get Targeted

- Patient records (PHI) combine medical, financial, and identity data, more valuable on the black market than a stolen credit card number alone
- Practices are often more time-sensitive than other small businesses; a locked EHR during patient hours creates urgency attackers count on to pressure a fast ransom payment
- Attackers increasingly target IT providers and software vendors that serve many practices at once, since one compromised vendor can expose all of their clients
- Smaller practices frequently run without dedicated security staff, relying on whatever their EHR or general IT provider has set up by default

Warning Signs

- ☐ Files suddenly renamed, encrypted, or inaccessible, often with a ransom note file appearing in folders
- ☐ Unexpected password reset emails or MFA prompts you didn't trigger
- ☐ Unusual login times or locations flagged in your email or EHR admin console
- ☐ Computers running noticeably slower, or antivirus/EDR alerts you don't recognize
- ☐ Staff reporting phishing emails that impersonate your EHR vendor, bank, or leadership

The First Hours: What To Do

- 1. Isolate, don't shut down.** Disconnect affected devices from the network (unplug Ethernet, disable Wi-Fi) rather than powering them off. You may need what's in memory for the investigation.
- 2. Call your IT provider or internal IT lead immediately.** Don't wait to "see how bad it is." Early containment limits how far an attacker or malware spreads.
- 3. Don't negotiate with attackers on your own.** If a ransom note appears, don't engage, pay, or delete anything. That's a decision for your IT/security team, legal counsel, and often law enforcement together.

4. **Preserve evidence.** Don't reformat, reinstall, or "clean up" affected systems before your incident response team has captured what they need. You may destroy the evidence that determines whether PHI was actually accessed.
5. **Determine PHI involvement early.** This decides your notification clock (see below). Get your IT/security team and, if needed, breach counsel involved quickly to scope what was exposed.
6. **Loop in your cyber insurance carrier** if you have a policy. Many require notification within a specific window and can direct you to approved forensics and legal resources.

Your Notification Clock (HIPAA Breach Notification Rule)

Who	Timeline
Affected individuals	Without unreasonable delay, no later than 60 days after discovery
HHS Office for Civil Rights (500+ affected)	Within 60 days, same timeframe as individual notice
HHS Office for Civil Rights (under 500 affected)	Logged and reported annually, within 60 days of year-end
Media	Required if more than 500 residents of one state/jurisdiction are affected

"Discovery" starts the clock the day the breach is known or reasonably should have been known, not the day you finish investigating. Start documenting from hour one.

After the Incident

- ☐ Run a post-incident review: how did the attacker get in, and what would have stopped it?
- ☐ Update your Security Risk Analysis to reflect what you learned
- ☐ Reset credentials broadly, not just for the accounts you know were affected
- ☐ Confirm your backups actually restore cleanly before you consider systems "recovered"
- ☐ Refresh staff phishing training; most incidents start with a click, not a sophisticated exploit

Don't wait for an incident to find out your plan doesn't work.

SIM Technology Solutions builds and tests incident response plans, deploys EDR and immutable backups, and is who you call the moment something looks wrong. **Call 703-594-9226** or email **info@simtsolutions.com**, ideally before you need us in an emergency.