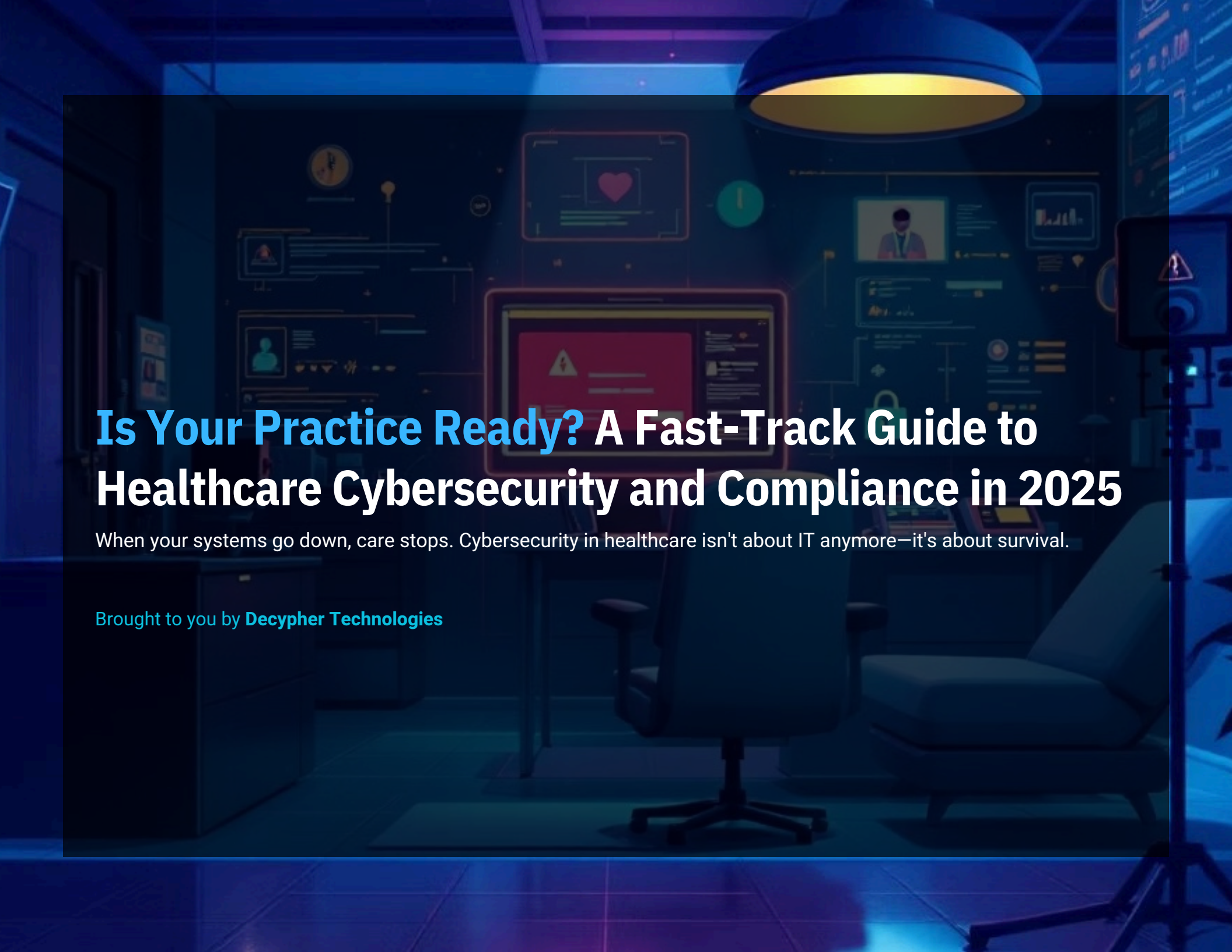


Is Your Practice Ready? A Fast-Track Guide to Healthcare Cybersecurity and Compliance in 2025

When your systems go down, care stops. Cybersecurity in healthcare isn't about IT anymore—it's about survival.

Brought to you by **Decypher Technologies**

What Keeps You Up at Night?

It's 2 a.m. Your staff can't access the EHR. Patient records are locked. A flashing red alert has replaced your morning schedule.

This isn't fiction. It's how healthcare breaches unfold—and small, mid-sized practices are now squarely in the crosshairs. Ransomware, phishing, system outages: these aren't just IT issues. They're clinical disruptions.

- **109M+ patients affected** by healthcare data breaches in 2023 alone (*HHS OCR*)
- Average breach cost: **$10.93M** (*IBM Cost of a Data Breach Report*)

For a deeper analysis of today's risk landscape, download the full white paper: "**The New Compliance Curve: How Healthcare Leaders Are Navigating Cyber Risk and Regulation**"

The New Standard of Care

Cybersecurity has become part of the standard of care—whether it's written into your chart or not. The days of HIPAA alone being “enough” are over.

Healthcare providers must now comply with:

- The **HIPAA Security Rule**
- The **FTC Safeguards Rule**
- **State privacy laws** like California's CCPA/CPRA or Colorado's CPA
- And follow **best practices like NIST CSF**

Your responsibilities go beyond patient charts. They include protecting employee data, vendor records, and any digital asset connected to your network.

> Being HIPAA-compliant doesn't automatically make you state-law compliant. If you're not protecting non-PHI (like HR records or marketing data), you're still at risk.

When Systems Fail, Lives Are Disrupted

Cyberattacks don't just cost money—they cost access, continuity, and trust.

Here's how that looks in real life:

Shutdown – ENT Clinic, Michigan

In 2019, Brookside ENT and Hearing Center in Battle Creek, Michigan, suffered a ransomware attack that encrypted all patient records, appointment schedules, and payment information. The attackers demanded a $6,500 ransom, which the practice refused to pay. Consequently, all files were deleted, and the practice was forced to close permanently.

Disruption – Miami Blood Transfusion Program

In 2024, a cyberattack on a blood transfusion coordination program serving multiple hospitals in Miami delayed surgeries and forced staff to revert to manual processes. Administrators described it as a "near miss" that exposed the fragility of digital health systems.

Lockout – Pain Clinic, Ohio

In August 2024, a small clinic in Blue Ash, Ohio was locked out of its systems overnight by a ransomware group called Helldown. Patients showed up to appointments the next morning—but the schedule, records, and prescriptions were inaccessible. The team scrambled to work offline for weeks.

> One click. One lost device. One missed patch. That's all it takes to shut down care—and sometimes, the business itself.

Your 5-Step Action Plan

1. Conduct a Real Risk Assessment

Use HHS's free tool or bring in a specialist. Identify what you're protecting, where the vulnerabilities are, and how to prioritize them.

2. Train and Equip Your Team

Annual training isn't enough. Simulate phishing. Explain data responsibilities in plain language. Keep everyone alert and accountable.

3. Harden Your Systems

Enable MFA. Encrypt devices. Patch everything. Separate guest Wi-Fi from medical devices. Backups are your lifeline4test them often.

4. Write and Practice Your Incident Response Plan

If a breach hits, you should know exactly who to call, what to disconnect, and how to communicate. Practice tabletop scenarios.

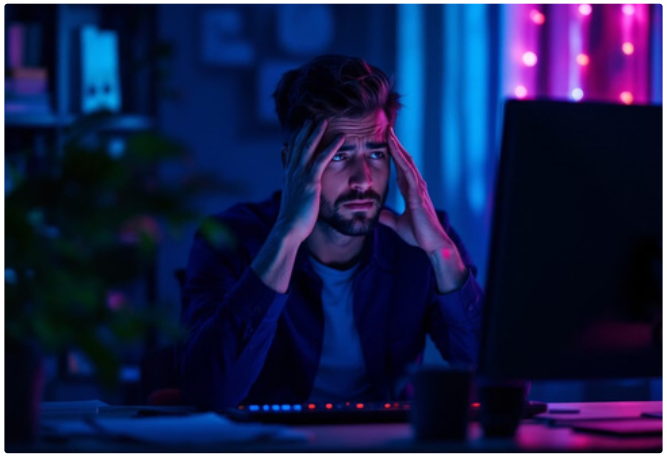
5. Document Everything

HIPAA, state laws, and insurers all require proof. No documentation? No defense.

🔎 See the full white paper for breakdowns of HIPAA, FTC, and NIST frameworks—and how they overlap.

Why Partnerships Matter

Going it alone



With a Partner

You don’t have to do this alone. The most successful healthcare organizations aren’t just compliant—they’re supported.

A partner like **Decypher Technologies** helps you:

- Conduct professional-grade risk assessments
- Monitor systems 24/7
- Train your staff with real-life simulations
- Stay compliant without drowning in paperwork
- Respond quickly if something goes wrong

Decypher works as an extension of your team. They bring the tools, the expertise, and the industry insight to help you lead with confidence.

> “They studied not just our tech—but our business culture. That’s why we trust them.” – Hospital IT Director, Colorado

Ready to Take the First Step?

The first step is often the hardest-but you don't have to take it alone.

Schedule a no-obligation risk consultation

Get an expert review of your current security posture

Call (855) 808-6920 or visit decyphertech.com

Want the full playbook? Download the complete white paper:
"The New Compliance Curve" – A Deep Dive for Healthcare Decision-Makers