Annual Healthcare Cybersecurity Report
2025 Reality Check + 2026 Survival Guide

What 2025 taught healthcare

Cybercrime against healthcare didn't slow down — it became more precise and more financially aggressive. In 2025, more than 57 million patients had data exposed across 642 large healthcare breaches reported to HHS. Healthcare again ranked #1 for the most expensive data breaches, averaging $10.93 million per incident.

The biggest shift
Attackers stopped caring about just locking systems and started prioritizing stealing patient and billing data first, then extorting providers with both downtime and data exposure.

Who hit healthcare — and how
Healthcare was targeted primarily by financially motivated ransomware and cybercrime groups, not nation-states.

The dominant 2025 attack path was
Stolen credentials → remote access → data theft → ransom + threat to leak

Major groups driving healthcare attacks included
ALPHV / BlackCat, Qilin, Black Basta and similar ransomware-as-a-service crews.

They focused on
- EHR platforms
- Billing and claims vendors
- VPNs and remote desktop
- Email and payroll systems

Phishing and stolen passwords remained the #1 way attackers got inside healthcare networks.

The damage: why this is not just an IT problem

The modern benchmark for healthcare cyber disruption is still the 2024 Change Healthcare attack, which exposed data on 190 million Americans and shut down prescription processing and insurance payments nationwide for weeks. That event became a financial and operational blueprint for healthcare-focused attackers in 2025.

Throughout 2025, ransomware groups copied that playbook—steal massive volumes of patient and financial data first, then extort providers and their vendors.

The result

- Large healthcare operators such as DaVita reported significant breach fallout, including $13.5 million in disclosed costs and 2.7 million individuals affected
- Hundreds of hospitals and clinics experienced billing shutdowns, delayed prescriptions, and a return to manual charting

For small and mid-sized practices, a single cyber incident now routinely means:

- Weeks of lost revenue
- Claims backlogs
- Patients unable to receive care
- Six-figure recovery bills

Indiana reality

Indiana providers saw how modern healthcare breaches increasingly unfold — through vendors and shared systems. In 2025:

- Union Health System (Terre Haute) reported 263,000 patients affected due to a breach at Oracle Health (Cerner) — even though Union itself was not hacked.
- Woodlawn Hospital confirmed attackers accessed and copied internal files after breaching its network.

This is the new risk model: Your cybersecurity now depends on your EHR, billing, and cloud vendors — not just your own clinic. These patterns are not anomalies. They reflect a structural shift in how healthcare cyber risk propagates.

2026 Outlook: What healthcare should expect

Three trends likely will dominate this year:

1) **Data-theft extortion will keep growing.** Attackers steal records first, then threaten to publish them even if systems are restored.
2) **Email-based payment fraud will surge.** Fake invoices, stolen vendor email accounts, and fraudulent wiring instructions are now stealing billions from healthcare.
3) **Vendor breaches will keep hitting innocent clinics.** EHRs, revenue-cycle vendors, transcription services, and cloud platforms remain prime targets.

What actually protects healthcare in 2026

These controls stop most real-world attacks:

- Lock down how attackers get in
- Use phishing-resistant multi-factor authentication on:
  - VPN
  - Remote desktop
  - EHR portals
  - Admin and billing accounts
- Remove old employee and vendor logins.

Stop payment fraud

Require call-back verification for:

- Vendor payment changes
- Bank routing updates
- New ACH or wire requests

Make ransomware survivable

- Maintain offline or immutable backups
- Test restores quarterly
- Keep a paper-chart + downtime plan for:
  - Prescriptions
  - Labs
  - Scheduling
  - Billing

Treat vendors like clinical infrastructure

Ask EHR and billing vendors:

- Do you enforce MFA?
- How quickly must you notify us of a breach?
- Can you prove you have secure backups?

If they can't answer, they are now your largest cyber risk

What this means for healthcare leaders

Healthcare cyber risk in 2026 is an operational reality, not an abstract threat. It directly affects the ability to deliver care, maintain revenue continuity, and preserve patient trust when critical dependencies are disrupted.

Organizations that prioritize resilience over technical sophistication alone — those designed to withstand disruption and recover quickly — will be best positioned to reduce the impact of extortion and systemic outages.

TRUSTED CYBERSECURITY RESOURCES FOR HEALTHCARE

Guidance & Frameworks	Federal Resources	Collaboration & Tools
IECC Cyber in a Box 2.1 *(3.0 coming soon)*	Dept. of Health & Human Services	HHS 405(d) Program
NIST Cybersecurity Framework	HHS HC3	CISA Toolkit & Best Practices
Health Sector Coordinating Council	CDC	
	CISA #StopRansomware	
	FBI IC3	

Please contact David Ayers at: dayers@iot.in.gov for inquiries or to share your healthcare cybersecurity story or incident for potential inclusion in future quarterly newsletters. Anonymity is optional.