

Lead with Trust: Tips to Elevate Your Healthcare Cybersecurity

As healthcare evolves into a technology-driven, data-centric ecosystem, leaders are challenged to embrace emerging technology while protecting their data.

Getting ahead of the curve [without compromising cybersecurity](#) requires a fine balance — and the risk of not achieving it has never been greater.



491

data breaches in the first three quarters of 2024¹



58.6M+

records affected by these breaches¹

Data breaches are costly on multiple levels

- Erosion of patient trust
- Operational disruptions
- Significant financial losses

\$9.8M

The average cost of a healthcare data breach²

Data Security Challenges and How to Address Them

Threat actors use various methods to achieve their goals.

1 Ransomware and multifaceted extortion

Ransomware attacks have evolved from encryption to multifaceted attacks, and attackers now steal sensitive data before encrypting it — to then sell for financial gain or extort organizations.

In 2024, **53%** of healthcare organizations paid the ransom to recover their data, with an average payment of \$4.4 million.³

Recommendation: Adopt a Zero Trust architecture

- ☒ Operates on the basis of never trust, always verify
- ☒ Gives role-based access to authorized users
- ☒ Limits connections between systems to only what is necessary

2 Phishing schemes

Phishing campaigns are now more sophisticated, and threat actors are improving their tactics every day.

- Offenders use models to quickly build more effective phishing tactics
- Remote work creates a bigger pool of people and devices to target
- Human error remains a leading cause of data breaches

In 2024, **68%** of healthcare breaches involved a non-malicious human error, including social attacks, errors, and misuse.⁴

Recommendation: Strengthen MFA protocols

Healthcare organizations can better ensure every employee is protecting cybersecurity by improving the sophistication of their multi-factor authentication (MFA).

- ☒ MFA is evolving into more intricate forms of additional authorization
- ☒ Sophisticated MFA ensures all are held to the same level of security best practices
- ☒ Cybersecurity training can further prepare staff for potential threats

3 Third-party security — or lack of

Organizations are rapidly becoming more connected, and every new connection is a potential new access point for threat actors.

In 2024, **healthcare was the industry most affected** by third-party data breaches, leading at 38.7% among all affected industries.⁵

Recommendation: Enhanced vendor management

The best protection against a third-party security threat is to establish strict cybersecurity requirements for all vendors within the relationship's contractual agreement.

- ☒ Contract acts as the guideline for cybersecurity set up and ongoing monitoring
- ☒ Zero Trust principle of “never trust, always verify” in action
- ☒ Regular assessments of vendors' security standards a must

Raising the Bar on Cybersecurity

As cybersecurity threats continue to evolve, healthcare organizations must take decisive action to safeguard sensitive data and maintain operational integrity.

The time to act is now — to protect not only proprietary data and organizational assets, but also the trust and safety of every patient the healthcare system serves.

Elevate Your Cybersecurity

1. “August 2024 Healthcare Data Breach Report,” Steve Alder, The HIPAA Journal, September 23, 2024, <https://www.hipaajournal.com/august-2024-healthcare-data-breach-report/>
2. “Average cost of healthcare data breach nearly \$10M in 2024: report,” Emily Olsen, Healthcare Dive, August 1, 2024, <https://www.healthcaredive.com/news/healthcare-data-breach-costs-2024-ibm-ponemon-institute/722958/>
3. “Healthcare Ransomware Attacks Continue to Increase in Number and Severity,” Steve Alder, The HIPAA Journal, September 30, 2024, <https://www.hipaajournal.com/healthcare-ransomware-attacks-2024/>
4. “Verizon 2024 DBIR: 70% of Healthcare Data Breaches Caused by Insiders,” Steve Alder, The HIPAA Journal, May 1, 2024, <https://www.hipaajournal.com/verizon-2024-data-breach-investigations-report/>
5. “Black Kite 2024 Third-Party Breach Report,” Black Kite, March 2024,