

WHITE PAPER

Strengthening Healthcare Cybersecurity: Protecting Patient Trust in a Digital Age

As healthcare continues to evolve into a technology-driven, data-centric ecosystem, leaders are challenged to lean into new innovations and embrace emerging technology while protecting their data at more secure levels. It's a fine balance to move quickly – get ahead of the curve and replace manual, outdated processes with a modern approach – and be diligent, bringing in new technology and applying advanced analytics to get the most value out of healthcare data without compromising an organization's data security.

Unfortunately, the risk of not having the right balance has never been greater.

Healthcare data breaches have surged in recent years. From January to August of 2024 alone, the healthcare sector experienced 491 data breaches that each affected 500 or more records, compromising over 58.6 million records in total.¹ Data breaches result in erosion of patient trust, operational disruptions, and significant financial losses – the average cost of a healthcare data breach is \$9.8 million, and healthcare is the most expensive industry for responding to and recovering from data breaches.²

The threat actors behind breaches appear in many forms, such as cybercriminals, hacktivists, nation state actors, and insider threats. Their motivations vary, but in healthcare, the impact of any breach cannot be overstated. Unlike other sectors, such as financial services or travel, healthcare records contain “one of one” data. Medical history cannot simply be replaced or revoked, making this data uniquely valuable threat to actors.

Furthermore, the COVID-19 pandemic underscored vulnerabilities within healthcare cybersecurity frameworks. Financially motivated hackers and insider threats exploited these gaps, targeting sensitive data ranging from patient records to vaccine research.

This white paper explores key challenges in healthcare data security and provides actionable solutions for organizational leaders across the care continuum. From ransomware defense to employee training, the following pages offer a roadmap to protect sensitive data, maintain compliance, and build organizational resilience.



\$9.8M

The average cost of a healthcare data breach²



491

Data breaches in the first three quarters of 2024¹



58.6M+

Records affected by these breaches¹

Cybersecurity threats: Who's behind the attacks?

Cyber threat actors are not all the same. Some are individuals working alone, while others are part of sophisticated groups that target various organizations at any given time. In healthcare, the most common cyber threat actors are listed in the following table.

Cybercriminals

An individual or a large group that targets an organization through extortion or the disclosure of compromised data for financial or personal gain; can orchestrate complex, sophisticated attacks.

Hackers

A hacker is an individual who conducts cyber threats in the name of some sort of activism. Their actions aim to cause significant reputational harm to their targets.

Nation State Actors

Nation state actors operate in the interest of advancing geopolitical objectives; their attacks may include building networks of compromised devices, financially motivated threat activity, and disrupting critical systems.

Insider Threats

A person or a contractor within a healthcare organization who has access to inside information regarding the organization's security guidelines, data, and systems. This could be a person who intends to cause harm in the form of a cybersecurity breach, or a negligent individual who unknowingly puts the company in risk of a breach.

Source: "Types of Cyber Threat Actors That Threaten Healthcare", U.S. Department of Health and Human Services, June 8, 2023, <https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf>

Challenges in healthcare data security, and recommendations to improve security

Just as the threat actors can vary, so can the methods they use in attempt to breach a healthcare organization. Some of the top healthcare cybersecurity threats are ransomware and multifaceted extortion, phishing schemes, and breaches that occur to third-party partners, which can negatively impact the organizations they are connected to.

#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.

Suffering a ransomware attack can come at a high cost. In 2024, 53% of healthcare organizations hit by ransomware paid the ransom to recover their data, with an average payment of \$4.4 million.³ Beyond the ransom, the impact to the organization and the patients they serve also comes at a cost. For example, the 2021 attack on Scripps Health disrupted patient care across multiple facilities and led to reported losses of \$113 million in revenue.⁴

53%

of healthcare organizations hit by ransomware paid the ransom to recover their data, with an average payment of \$4.4 million

Recommendation: Adopt a Zero Trust Architecture

[IBM defines](#) Zero Trust Architecture as, “a security strategy for modern multicloud networks. Instead of focusing on the network perimeter, a Zero Trust security model enforces security policies for each individual connection between users, devices, applications, and data.”

Zero Trust operates on the basis of never trust, always verify. This appears in the form of only giving role-based access to authorized users rather than granting all users within an organization the same level of access to their data and the systems that protect, analyze, and share data.

It also means limiting the connections between systems to only what is necessary. Zero Trust segments networks, protecting access to critical systems and applying advanced identity verification tools to authorize or deny access as users attempt to access an organization's data.

In a recent panel discussion, Paul Wilder, Executive Director, CommonWell Health Alliance, summarized Zero Trust as, “It should connect to nothing first. What is the minimal set of stuff it needs to do, to do its job?” He added, “Zero Trust is a must-have before a threat occurs. You can't respond to risks without a plan, and Zero Trust is the playbook every healthcare organization needs.”

#2 Phishing schemes

Phishing campaigns are no longer poorly written emails with “gotcha” links. They are sophisticated campaigns that closely mimic the entity they appear to be from – and threat actors are improving their tactics every day.

In the age of AI, when one- or two-sentence prompts can produce a well-written email (or a series of them), hackers have more tools at their disposal to craft better phishing schemes, faster. Just as security teams are exploring new tools, and AI may be one of them, offenders are using models to quickly build more sophisticated phishing tactics.

“The reality is that threat actors are using some of the same tools that healthcare organizations are also leveraging for their own learnings and efficiencies. It’s a game of offense and defense; a race of gaining the greater advantage, and AI is in play on both sides,” shared Luke McNamara, Deputy Chief Analyst, Mandiant Intelligence (now part of Google Cloud), during the same panel mentioned above.

Plus, the growth of remote work means that bad actors have a bigger pool of people and devices to target. Every person using a home internet connection or their personal device to conduct work is a potentially new – and weaker – entryway to a healthcare organization’s valuable data.

Human error remains a leading cause of data breaches, and employees often underestimate how critical their role is in organizational security. One click in a phishing campaign or an improperly locked device is enough to open a risky door. In fact, phishing is among the most common causes of healthcare data breaches, and in 2024, 68% of healthcare breaches involved a non-malicious human error, including social attacks, errors, and misuse.⁵

“*The reality is that threat actors are using some of the same tools that healthcare organizations are also leveraging for their own learnings and efficiencies. It’s a game of offense and defense; a race of gaining the greater advantage, and AI is in play on both sides.*”

– Luke McNamara, Deputy Chief Analyst, Mandiant Intelligence (now part of Google Cloud)

Recommendation: Strengthen MFA protocols

How can healthcare organizations ensure every employee is doing their part to protect cybersecurity? By improving the sophistication of their multi-factor authentication (MFA).

MFA is evolving from a verification email or text message to more intricate forms of additional authorization, including facial recognition, hardware keys, or using a separate certificate-based system to confirm a code from the point of access. While not all employees may fully grasp the cybersecurity risk at stake, sophisticated MFA ensures all are held to the same level of security best practices.

In time, more stringent MFA may potentially improve employee awareness of threat actors, and organizations can also offer additional training on how to best protect their own data and devices, not just the company’s. Organization-sponsored cybersecurity training can further prepare staff for potential threats, and regular assessments and feedback loops can encourage appropriate responsiveness to threats such as reporting them to the organization’s security team.

#3 Third-party security – or lack of

In the midst of healthcare's technology and data-driven transformation, a push and pull is happening that cannot be ignored: organizations are striving to become more connected, faster – there's a growing desire to create complete patient profiles, understand longitudinal patient data, and apply advanced analytics to these more extensive datasets in order to deliver more personalized care – yet, every new connection is also a potential new access point for threat actors.

As healthcare is increasingly connected, verifying the strength of vendors' and partners' security is paramount. From billing portals to cloud storage solutions, every connection can become a potential threat if the vendor is impacted by a cybersecurity incident. In 2024, healthcare was the industry most affected by third-party data breaches, leading at 38.7% among all affected industries, according to a Black Kite report.⁶

So, what does this mean for business leaders who are eager to expand connections and access more complete healthcare datasets, while continuing to maintain the highest possible measures of security?

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. This ensures that both parties are clear on cybersecurity standards; there is no room for interpretation. It also sets expectations before any connections are established between the two parties' tech environments.



We are connected – patients, providers, payers, and more – and as we get more connected, we're also creating more access points in healthcare. Protecting these means serious audits along the way when establishing new connections, and maintaining the security of those connections with regular check-ins."

– Michael Quinn, VP, Strategic Partner Development, Inovalon

The contract becomes the guidelines for both set up and ongoing monitoring, which all healthcare organizations should do with their vendors. It's the Zero Trust principle of "never trust, always verify" in action. Organizations must conduct regular assessments of their vendors' security standards to ensure the contractual agreements are being upheld, and more importantly, that their environment and data are not at risk.

Michael Quinn, VP, Strategic Partner Development, Inovalon, summarized the value of verifying the security of third-party relationships as, "We are connected – patients, providers, payers, and more – and as we get more connected, we're also creating more access points in healthcare. Protecting these means serious audits along the way when establishing new connections, and maintaining the security of those connections with regular check-ins."



Looking ahead: 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. Implementing a Zero Trust architecture, enhancing MFA protocols, offering employee cybersecurity training, and building security requirements into contractual agreements are just some of the necessary, important steps organizations can take to establish and maintain a resilient cybersecurity framework.

No one strategy will be the protector of an entire tech environment or dataset. It's the thoughtful combination of many tactics working together that give organizations the best chance of stringent security. 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.

-
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. "\$3.5 Million Settlement by Scripps Health for Ransomware Attack Compromising Patient Information," Richard P. Kusserow, January 2023, Strategic Management Services, <https://www.compliance.com/resources/3-5-million-settlement-by-scripps-health-for-ransomware-attack-compromising-patient-information/>
 5. "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/>
 6. "Black Kite 2024 Third-Party Breach Report," Black Kite, March 2024, <https://blackkite.com/wp-content/uploads/2024/03/third-party-breach-report-2024.pdf>

About us

Inovalon is a leading provider of cloud-based SaaS solutions empowering data-driven healthcare. The Inovalon ONE® Platform brings together national-scale connectivity, real-time primary source data access, and advanced analytics into a sophisticated cloud-based platform empowering improved outcomes and economics across the healthcare ecosystem. The company's analytics and capabilities are used by over 50,000 active, licensed customers. For more information, visit www.inovalon.com.

Inovalon
4321 Collington Road
Bowie, MD 20716
(301) 809-4000

www.inovalon.com

