The State of **Health Security 2026**

Emerging Trends in Cybersecurity Across Healthcare

Thoropass™

Foreword

Healthcare cybersecurity is entering a new phase which is defined **less by intention** and **more by proof**.

Across the industry, expectations are shifting. Cyber incidents are having measurable financial and clinical impacts, AI is accelerating both opportunity and risk, and regulators are becoming more specific in their requirements. At the same time, healthcare remains highly complex, with fragmented data, legacy systems, and growing reliance on third parties.

This report brings together current data and research to highlight how these forces are reshaping healthcare security. The goal isn't just to understand threats, but to help organizations benchmark themselves and prepare for what comes next.

The data suggests a clear direction: organizations that succeed in 2026 will be those that move toward demonstrable resilience where controls are consistently implemented, tested, and verifiable.

AI Moves from Experimentation to **Infrastructure**

AI adoption in healthcare is accelerating, with many organizations moving from pilot programs into production environments. Clinical workflows, administrative processes, and security tools are increasingly incorporating AI to improve speed, operational efficiency, and decision-making.

However, governance and risk management are not advancing at the same pace. While organizations remain confident in AI's value, concerns around security, data protection, and responsible use continue to grow. In Thoropass' recent State of Audit and Compliance survey, 69% of respondents said AI adoption is outpacing their security and compliance controls, while 55% identified AI-related data exposure or misuse as their top breach concern - higher than ransomware, IAM failures, or cloud misconfigurations. Additionally, 57% believe AI incidents are the most likely cause of regulatory action or customer fallout in 2026.

AI adoption is widespread across all industries, but healthcare faces unique challenges due to sensitive data, regulatory requirements, and complex systems. This makes the gap between adoption and governance more consequential.

As we progress into 2026 and beyond, the key differentiator is no longer simply AI adoption, but the ability to manage AI systems in a **controlled**, **transparent**, and **auditable way**.

Thoropass™

AI Moves from Experimentation to **Infrastructure**

50%
of healthcare organizations have implemented generative AI[1]

19%
have implemented agentic AI[1]

51% are piloting

92%
expect AI to create competitive advantage[3]

72%
of organizations globally use AI in at least one function[4]

65%
of healthcare organizations say AI is redefining operations[3]

81%
of physicians report using AI in their practice[2]

vs. 38% in 2023

40%
of organizations plan to increase AI investment due to competitive pressure[5]

Healthcare breach costs are **67% higher than global average**[6]

Healthcare is the **most expensive industry for breaches** for 14 consecutive years[6]

Healthcare is the **5th most targeted industry**, with 10% of all cyber intrusions[7]

$7.42M
average cost of a healthcare data breach[6]

$4.45M
global average breach cost across industries[6]

74%
of hospitals reported patient care disruption from cyberattacks[8]

94%
reported financial impact[8]

33% lost >50% revenue

Average financial sector breach cost: **$5.9M vs. $7.4M healthcare**[6]

Thoropass™

Cybersecurity Becomes a **Financial** and **Operational Risk**

Cybersecurity incidents in the healthcare industry increasingly impact both financial performance and patient care delivery. Compared to many other sectors, healthcare experiences higher average breach costs and more direct operational disruption.

Recent incidents have demonstrated how cyber events can affect revenue cycles, delay care, and disrupt interconnected systems across providers and payers. These impacts extend beyond IT, making cybersecurity a core business risk.

At the same time, breach costs continue to rise globally, with healthcare consistently ranking as the most expensive industry for cyber incidents. This reflects both the sensitivity of healthcare data and the operational complexity of the sector.

As a result, organizations are shifting focus from prevention alone to ensuring continuity and recovery. In 2026, resilience - i.e. maintaining operations during disruption - has become as important as defense.

Third-Party and **Systemic Risk** Redefine the Threat Landscape

Healthcare's reliance on a network of third-party vendors and shared infrastructure continues to expand, increasing exposure to external risk. Cybersecurity incidents are no longer confined to individual organizations; they can affect entire networks of providers, payers, and partners.

Research shows that third-party breaches are common across industries, but their impact in healthcare can be particularly significant due to the sector's interconnected systems and dependence on shared services.

Recent large-scale incidents have highlighted how disruptions in a single vendor can cascade across the ecosystem, affecting operations, finances, and patient care. One example, a 2024 Russian-originated ransomware attack on a subsidiary of United Healthcare, caused widespread disruption nationwide. A survey of hospitals a month after the attack uncovered that 74% reported direct patient care impact, including delays in authorizations for medically necessary care, 94% reported the attack impacted them financially, and 33% reported the attack disrupted more than half of their revenue.

As organizations continue to adopt external technologies and services, managing third-party risk requires **ongoing assessment** and **visibility** - not just point-in-time evaluation.

Thoropass™

Third-Party and **Systemic Risk** Redefine the Threat Landscape

Third-party risk management is a top healthcare cybersecurity investment priority[9]

61%
of organizations experienced a third-party breach in the past year[10]

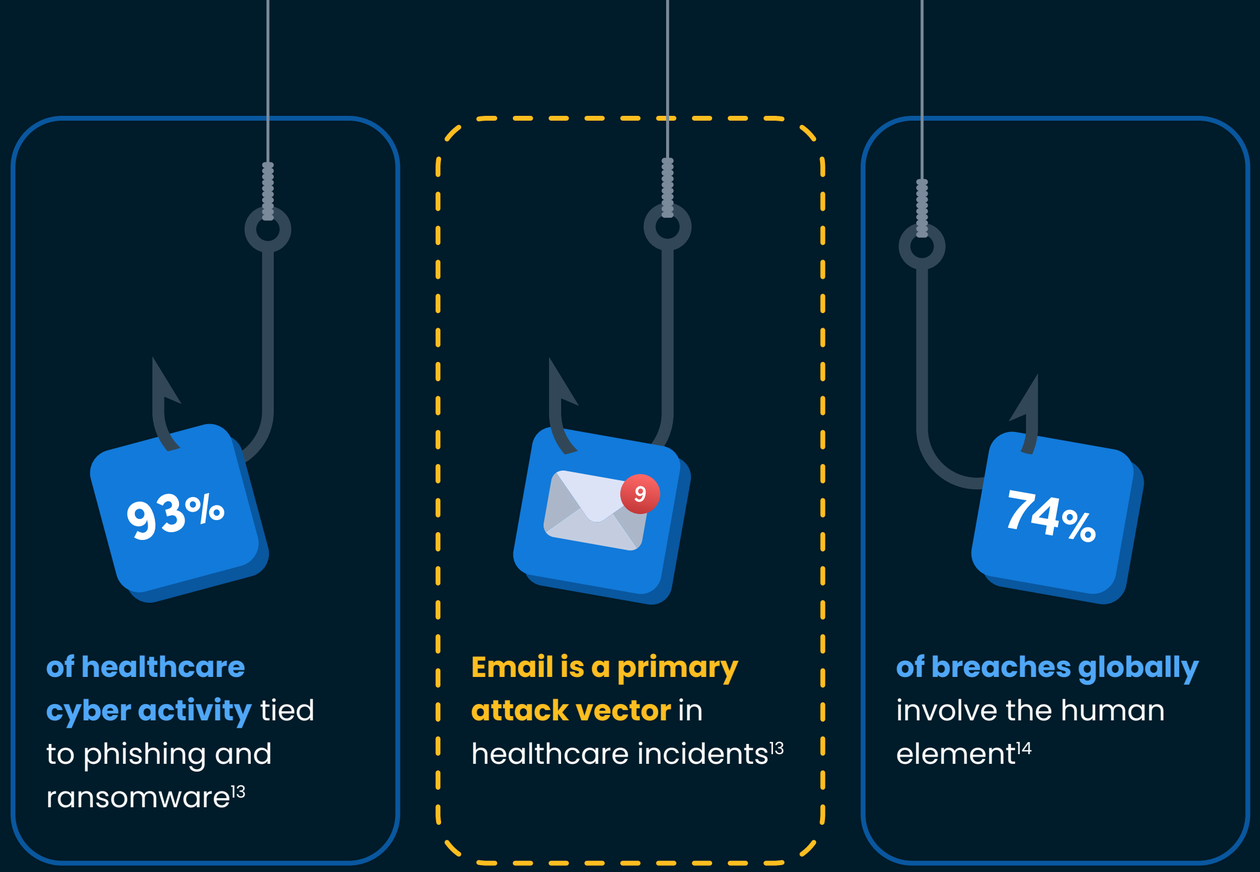
98%
of organizations globally have relationships with at least one breached vendor[10]

74%
of hospitals surveyed reported disruption linked to a recent cyber incident[8]

Top threats include ransomware, third-party breaches, and supply chain attacks[11]

Large-scale incidents have impacted **up to 1 in 3 patient records**[12]

Third-party breaches are among the most costly incident types[10]



of healthcare cyber activity tied to phishing and ransomware[13]

Email is a primary attack vector in healthcare incidents[13]

of breaches globally involve the human element[14]

- **Credential compromise** is a top breach vector across industries[14]
- Phishing accounts for **16% of global breaches**[14]
- **Legacy systems** remain common in healthcare environments[15]

Identity, Email, and Legacy Systems Remain **Core Vulnerabilities**

Common attack vectors such as phishing, credential compromise, and legacy system vulnerabilities continue to drive the majority of cybersecurity incidents. These risks aren't unique to healthcare, but they are amplified by the sector's complexity and reliance on distributed access.

Healthcare organizations often operate with a mix of modern and legacy systems, making it more difficult to enforce consistent security controls. Email remains a primary entry point for attackers, while compromised credentials enable lateral movement within networks.

Global breach data shows that human factors such as phishing and credential misuse are involved in the majority of incidents across industries. In healthcare, these risks are compounded by operational demands and system fragmentation.

Addressing these vulnerabilities requires consistent implementation and monitoring of identity and access controls across the organization.

Regulation Shifts Toward **Measurable Controls**

Regulatory expectations in healthcare cybersecurity are becoming more specific and measurable. Rather than focusing solely on policy requirements, regulators are increasingly emphasizing the need for implemented and tested controls.

Recent proposed updates to the HIPAA Security Rule reflect this shift, outlining expectations for multi-factor authentication, vulnerability management, and incident response planning. These changes align with broader trends across industries toward accountability and transparency.

Healthcare organizations must also manage multiple overlapping frameworks, increasing the complexity of compliance efforts. Compared to less regulated industries, this creates additional operational burden.

As regulations evolve, compliance is becoming a continuous process rather than a point-in-time exercise, requiring ongoing validation of controls.

HIPAA Security Rule updates which will become required in late 2026

- **Requirements include** MFA, vulnerability scanning, and IR testing[15]
- **72-hour breach reporting** requirement[15]

HIPAA HITRUST SOC 2

Healthcare organizations **manage multiple frameworks**[8]

45% of organizations say regulatory complexity is increasing[16]

Healthcare and financial services **rank among the most regulated industries**[16]

70–80%
of clinical data
is unstructured[17]

80%
of healthcare data
is unstructured[18]

Only 20% of enterprise data is structured globally[20]

42%
say poor data quality limits decision-making[19]

Healthcare data reached **4,200 exabytes in 2026** and is **growing at 63% annually**[21]

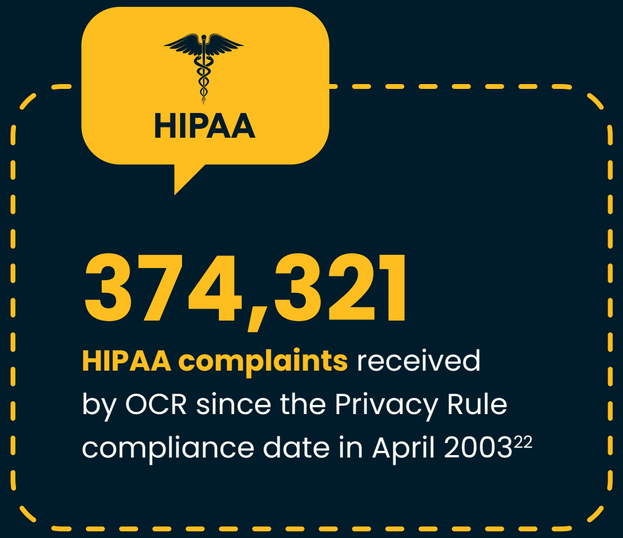
Data Growth Turns Governance into a **Security Imperative**

The volume of healthcare data continues to grow rapidly, driven by digitization, connected devices, and AI adoption. However, much of this data remains unstructured and fragmented, making it difficult to manage and secure.

Compared to many industries, healthcare deals with a higher proportion of unstructured data, increasing the challenge of maintaining visibility and control. This fragmentation affects both security and decision-making.

As healthcare providers rely more on data-driven technologies, governance becomes increasingly important. Without clear understanding of where data resides and who can access it, risks will only increase.

Effective data governance in 2026 and beyond requires both organization and oversight, ensuring that data is usable, secure, and compliant.



31,191

cases required **corrective action**, **privacy-practice changes**, or **technical assistance** for covered entities and business associates[22]

152

cases resulted in **settlements** or **civil money penalties**, totaling $144.9 million in fines[22]

67,873

cases were addressed through **early intervention** and **technical assistance**, avoiding the need for a full investigation[22]

Thoropass™

HIPAA Violations: Enforcement Trends and Risk Areas

HIPAA enforcement remains a significant operational risk for healthcare organizations, health plans, pharmacies, and business associates. Since the Privacy Rule compliance date in April 2003, the HHS Office for Civil Rights has received almost 400,000 HIPAA complaints and initiated more than a thousand compliance reviews.

While most cases are resolved without financial penalties, OCR's enforcement record shows that confirmed noncompliance often leads to corrective action, changes in privacy practices, technical assistance, or settlement agreements. The data also highlights recurring failure points: improper use or disclosure of protected health information, insufficient safeguards, and barriers to patient access. As healthcare organizations continue digitizing workflows and expanding vendor ecosystems, HIPAA compliance remains both a regulatory requirement and a core patient trust issue.

Recommendations for Healthcare Cybersecurity Leaders

Healthcare organizations can take practical steps to strengthen resilience while aligning with evolving risks and regulatory expectations.

01 **Prioritize** identity and access controls

Credential-based attacks remain a leading entry point. Enforcing multi-factor authentication and regularly reviewing access can reduce exposure.

02 **Improve** data visibility and governance

Understanding where data resides and who can access it reduces both security and compliance risk.

03 **Strengthen** third-party risk management

Vendors expand the attack surface. Continuous assessment and validation of third-party security posture is critical.

04 **Move toward** continuous validation

Organizations should shift from periodic reviews to ongoing validation of controls, ensuring readiness for both audits and real-world threats.

05 **Operationalize** incident response

Plans must be tested regularly. Simulations and exercises help ensure effective response during real incidents.

Thoropass™

Conclusion

Healthcare cybersecurity is no longer a background function whose only stakeholders are in the IT department. It is central to **delivering care**, **maintaining financial stability**, and **sustaining trust**.

The data is clear: healthcare faces higher breach costs, greater operational disruption, and deeper third-party dependencies than most industries. At the same time, expectations are rising and government regulators, boards, and patients are all demanding greater accountability.

What's changing most is the standard of success. It is no longer enough to have policies or tools in place. Organizations are being judged on whether their controls actually work - under pressure, in real-world conditions.

The key questions for CISOs throughout the healthcare industry are straightforward:

- Can systems withstand disruption?
- Can incidents be contained quickly?
- Can organizations prove their security posture and not just describe it?

Those organizations that succeed will shift from periodic compliance to continuous validation - ensuring controls are consistently implemented, tested, and effective.

The healthcare industry cannot eliminate cyber risk, but it can build resilience to emerging threats and mitigate against them through smart policy and the right tools and processes in place. In today's environment, resilience is what ultimately determines whether organizations can continue to operate - and deliver care - when it matters most.

Thoropass™

References

1. McKinsey & Company. *Generative AI in Healthcare* (2025)
2. American Medical Association. *AI Usage Among Doctors* (2026)
3. KPMG. *Intelligent Healthcare Report* (2025)
4. McKinsey. *State of AI Global Survey* (2025).
5. PwC. *AI Business Survey* (2025)
6. IBM Security. *Cost of a Data Breach Report* (2025)
7. Crowdstrike. *2026 Global Threat Report* (2026)
8. AHA. *Change Healthcare Cyberattack Report* (2025)
9. KLAS Research. *Cybersecurity Solutions for Healthcare* (2025)
10. Ponemon Institute. *Third-Party Risk Report* (2025)
11. Health-ISAC. *Threat Landscape Report* (2025)
12. AHA. *Same Change Healthcare Report* (2025)
13. Microsoft. *Rural Hospital Cybersecurity Report* (2025)
14. Verizon. *Data Breach Investigations Report* (2025)
15. U.S. HHS. *HIPAA Security Rule NPRM* (2025)
16. Thomson Reuters. *Cost of Compliance Report* (2025)
17. Institute for Health Metrics (2025)
18. Applied Clinical Trials (2025)
19. KPMG. *Future of Risk* (2024)
20. IDC. *Global DataSphere Forecast* (2024–2025)
21. Capgemini. *Healthcare Trends Report* (2025)
22. U.S. Dept of Health and Human Services. *Enforcement Highlights* (2024)