Healthcare Cyber Insurance at an Inflection Point

The cyber insurance market is reaching an inflection point where underwriting companies must differentiate healthcare from other industries in how the risk is evaluated, priced, and how claims are managed.

Healthcare cyber claims data tells a consistent and troubling story: attack frequency has surged dramatically in 2025, roughly a 90% increase from the prior year, while loss costs have more than doubled, driven by both ransomware and the near-automatic class action lawsuits that follow such incidents. In parallel, continued lawsuits tied to online tracking technologies increase exposure.

Even though it is clear that healthcare is being highly targeted, many underestimate the complexity of healthcare cyber exposure. This class cannot be priced or managed like retail, manufacturing, or construction; it demands specialization, underwriting discipline and strong risk management controls.

Healthcare Cyber - Standing Out from the Crowd

Claim data points to rising frequency and severity, with ransomware and litigation trends both deteriorating. Across the industry, healthcare organizations are facing ransomware attacks that are costing between two and three times more than those against non-healthcare entities.

While ransomware frequency in healthcare remained relatively flat from 2022 through 2024, loss ratios stayed elevated. Ransomware frequency in the healthcare sector has surged sharply in 2025, and severity continues to climb. Double extortion, where attackers not only encrypt a victim's data but also steal and threaten to publish patient data unless a ransom is paid, has become standard, triggering nearly every clause in a cyber policy: breach response, liability, business interruption, data recovery, and extortion payments.

The healthcare sector has consistently been featured among the top industries targeted by ransomware groups and it's not just direct attacks that threaten the industry. The February 2024 Change Healthcare attack disrupted 94% of US healthcare providers and impacted nearly half of the US population.

Healthcare networks are uniquely complex and interconnected. Legacy systems, vendor-managed devices, and limited cybersecurity resources expand the attack surface, making it one of the most challenging environments to secure. Also, when hospital systems are disabled, the consequences extend far beyond operational disruption. Patient care is delayed, safety is compromised, and the financial and human costs are intertwined.

The Legal Challenge

The legal aftermath of an attack is also quite challenging. When breaches must be disclosed under HIPAA and state privacy laws, it invites public scrutiny and rapid legal action. As a result, class actions often follow within days.

Meanwhile, litigation over website tracking tools has increased exposure for healthcare organizations, especially as some courts appreciate the sensitivity around personal medical data. One recent example was the use of Meta Pixel- a tool that helps analyze online traffic- in patient portals, not realizing the tool can share sensitive details with Meta, the social-media platform.

Although only about 200-300 of the roughly 3,000 cases filed so far on website tracking involved healthcare providers, those few accounted for around two-thirds of the total settlement costs. Data from published class action cases show healthcare settlements averaging $5–6 million.

Underwriting Complexity in a Dynamic Environment

Several factors converge to make healthcare organizations prime targets for cybercriminals. Healthcare organizations often have limited budgets and staffing for cybersecurity. At the same time, their IT environments are often complex and interconnected with numerous devices and endpoints.

This combination creates significant vulnerabilities that attackers are eager to exploit, especially given the value of healthcare data. A single medical record can sell for $50-$250 on the black market compared to just $1-$2 for a stolen credit card number, making healthcare data more lucrative.

One of the main vulnerabilities for healthcare organizations is their virtual private network (VPN). Most think their VPN / SSL VPN system is secure, but in reality, 50–60% of ransomware incidents come from VPN accounts that didn't have multi-factor authentication (MFA) properly enforced.

Attackers now commonly break into networks through VPN login portals using automated password-guessing tools. This is often called brute-force. To defend against this, it's critical to not only require strong and complex passwords and enforce the use of MFA on all accounts, but to also set up account lockouts after failed login attempts and block connections coming from anonymous or high-risk networks like public VPNs, proxies, or the onion router (TOR).

Regular software updates (patching) are still essential, but as seen in recent ransomware attacks like Akira's campaign targeting SonicWall devices, even fully patched systems can be compromised if MFA and secure remote access aren't enforced. Healthcare teams need to ensure remote access to patient data remains secure without sacrificing ease of access for staff.

These realities expose a persistent disconnect between underwriting assumptions and operational practice. Healthcare's distributed, multi-entity structure makes it uniquely difficult to assess and secure.

Generic underwriting checklists fail to capture the nuances of clinical systems, legacy infrastructure, and third-party dependencies that define healthcare risk. Carriers with smaller healthcare portfolios may view losses as isolated anomalies, but at scale, patterns are unmistakable: sustainable participation depends on underwriting models, controls, and claims management built specifically for healthcare.

The Call to Action

Healthcare cyber risk demands more than capacity; it requires accountability. Addressing this challenge depends on three critical elements: pricing, controls, and claims management built specifically for healthcare risk.

Firstly – introduce pricing with purpose. The healthcare segment should not be absorbed into the soft market. It needs underwriting that understands the sector's technical and legal realities, monitors meaningful measures of cyber hygiene, and prices risk accordingly. Without disciplined, data-driven pricing, the cyber market faces mispricing that weakens its foundation and long-term sustainability.

Secondly – introduce controls that strengthen defenses. Healthcare providers must invest in and demonstrate tangible improvements in their security posture. This means enforcing multi-factor authentication across all access points and all user accounts, modernizing legacy systems, tightening vendor management, and closing persistent gaps that attackers exploit. It also means being highly responsive when your insurer identifies a critical vulnerability that needs to be addressed.

Cyber resilience must be treated as inseparable from patient safety. It must be an operational necessity, not an optional investment. The same responsibility demanded in healthcare delivery must extend to safeguarding the systems that enable it.

Thirdly – ground claims management in partnership. Sustainable underwriting requires coordination between insurers and insureds to manage claims effectively and learn from every incident. The engagement must be ongoing with clear communication channels.

Healthcare cyber demands accountability from every stakeholder, including the underwriting company, broker organization, and insureds. Those who act with clarity, price with purpose, and demand progress on both sides of the risk equation will not only protect their portfolios but also help stabilize the market, strengthen critical infrastructure, and safeguard the people who depend on it. The strength of this market depends on shared accountability, disciplined underwriting and pricing, and a commitment to cyber security resilience that endures beyond the next renewal cycle.

TOKIO MARINE
HCC

tmhcc.com/pro

Cyber & Professional Lines Group

Tokio Marine HCC is the marketing name used to describe the affiliated companies under the common ownership of HCC Insurance Holdings, Inc., a Delaware-incorporated insurance holding company. Headquartered in Houston, Texas, Tokio Marine HCC is a leading specialty insurance group with offices in the United States, the United Kingdom and Continental Europe.