Gallagher

Insurance | Risk Management | Consulting

A Favorable Prognosis: Healthcare at the Forefront of Cyber Risk

Healthcare organizations continue to find themselves at the forefront of cyber risk. Exposures such as IT supply chain dependencies, website tracking litigation, ransomware attacks, new security regulations and data breach class actions put healthcare organizations of all sizes at high risk for cyber insurance claims. Understanding trends in cyber attacks as well as the evolving regulatory and litigation environment is critical to building resilience and maximizing insurance indemnification.

$2.87 billion

2024 anticipated cost of a healthcare ransomware attack (Source: The HIPAA Journal)

IT Supply Chain Dependencies

In February 2024, the breach of a healthcare technology provider impacted about 190 million people. Data exposed via the ransomware attack included personal, medical and financial information. The breach was particularly unique in its massive downstream effect on almost all touchpoints of the healthcare industry — hospitals, healthcare providers, pharmacies, drug companies, insurers and patients. This attack demonstrates the risk of IT supply chain exposures in the healthcare industry segment, and the considerations that healthcare companies should have as they engage with IT vendors and consider dependencies in running their operations.

$250 to $10,000 per violation

Potential statutory penalties related to website tracking technology

Website Tracking Litigation

Website tracking is the use of code, including pixels, cookies, or scripts, to capture data about how users interact with a website. Website tracking litigation is not a result of new regulations but rather the plaintiffs' bar's use of existing laws that never considered today's technology when they were enacted, such as 1967's California Invasion of Privacy Act, 1968's Federal Wiretap Act, and 1988's Video Privacy Protection Act. These laws carry statutory penalties ranging from $250 to $10,000 per violation. Healthcare organizations tend to be a bigger target for website tracking litigation than other industries, likely due to the highly regulated data that they collect and hold. According to a recent article in JD Supra, the increase in website tracking litigation for healthcare organizations may be correlated to a December 2022 bulletin by the US Department of Health and Human Services (HHS) Office for Civil Rights. This bulletin stated that information collected on a website constituted protected health information even if there was no relationship between the website user and the owner of the website and even if there was no billing or medical information collected. While a court later vacated a portion of this bulletin in June 2024, the plaintiff's bar continues to pursue website tracking litigation using the 1968 Federal Wiretap Act as a basis for privacy violations.

$1.9 million per day

Average financial loss from downtime due to ransomware attacks (Source: Comparitech)

Ransomware

Healthcare organizations remain a significant target for ransomware threat actors. According to Comparitech, there were 118 confirmed ransomware attacks and 147 unconfirmed ransomware attacks against the US healthcare sector in 2024, which resulted in an average of 18 days downtime. The healthcare industry tends to be targeted by ransomware threat actors given the large amounts of healthcare and financial data being processed, as well as the critical need for operational uptime to support patients. From 2018 to 2024, there were 654 individual ransomware attacks on medical organizations. During this period, ransom amounts varied from $4,000 to $10 million, with an average ransom demand of $1.18 million. On average, US healthcare organizations lose $1.9 million per day due to downtime from ransomware attacks. Ransomware attacks continue to be a scourge for the healthcare industry, and while improved cybersecurity controls have resulted in less ransoms being paid, the disruption that is caused by these attacks is significant.

Within 72 hours

Timeline for hospitals in New York State to report a breach

New Security Regulations

In December of 2024, HHS announced a proposed update to the HIPAA Security Rule that would require healthcare organizations to implement additional security controls, such as multifactor authentication (MFA), data encryption, vulnerability remediation, network segmentation, asset inventory and proactive security testing. This proposed rule update has not yet been finalized and now falls under the purview of the new federal administration. Various states have taken matters into their own hands in terms of requiring healthcare organizations to report breaches within a certain time period and improve cybersecurity controls. Effective October 2, 2024, hospitals in New York State must report incidents to the New York State Department of Health within 72 hours of discovery. Further, starting on October 2, 2025, New York State hospitals must implement additional cybersecurity controls, including but not limited to implementing MFA, conducting annual cybersecurity risk assessments, and employing a Chief Information Security Officer.

$9.77 million

Average cost of a healthcare data breach in 2024 (Source: IBM/Ponemon Institute Cost of a Data Breach Report 2024)

Data Breach Class Actions

Data breaches continue to impact healthcare organizations. According to The HIPAA Journal, there were thirteen data breaches in 2024 involving more than one million healthcare records. Eleven of these were a result of a cyber attack on the organization, and eight involved an attack on business associates of HIPAA regulated entities. As previously discussed, the 2024 ransomware attack on a healthcare technology provider resulted in the largest healthcare data breach on record, and associated class action lawsuits are ongoing. The healthcare industry is not new to dealing with class actions associated with data breaches, and in many cases, it is a ransomware attack that serves as a basis for not only a disruption in services but also a breach of HIPAA regulated data, typically resulting in costly class action litigation.

With such a challenging risk environment, how can healthcare organizations structure their cyber insurance to address the evolving claims environment? Insurance buyers should pay attention to the following:

- **Are limits adequate for the risk exposure?** Many healthcare organizations reduced limits during the 2020 to 2022 cyber insurance "hard market" while continuing to experience revenue growth. Only about 50% of those buyers increased limits when market conditions changed, leaving many healthcare organizations underinsured.
- **What vendors are in scope for dependent/contingent business interruption coverage?** Dependent/contingent business interruption coverage may include indemnification for net income loss and extra expenses associated with a disruption of a vendor on which the insured is dependent due to a security breach or technology failure. Many policies require that a contract be in place with the vendor to provide this coverage; however, coverage may be available or broadened to not require a contract.
- **Is coverage available for claims related to website tracking and the associated collection of data?** Many policies may exclude coverage for this "wrongful collection" peril or may limit coverage to defense costs only. Carriers have started underwriting for this exposure, and when controls are adequate, full limits may be available.

Having a broker with specific cyber insurance expertise and a consultative approach is key. The devil is in the details of cyber insurance coverage, and it is critical that healthcare organizations partner with a broker that can provide data and analytics to identify the potential quantum of loss, understand the nuances of available coverages across the market, and advocate through the claims settlement process. The prognosis for healthcare organizations that take this into consideration is favorable, and those organizations will be better positioned to maximize the value of their cyber insurance policy.

Stephanie Snyder Frenier is an SVP with Gallagher's Cyber Liability practice and National Director of Gallagher's Cyber Advantage panel. She has over 21 years of experience in the insurance industry as an underwriter, broker and cyber data and analytics vendor.

Recent Gallagher Cyber Webinars:

- Top Cyber Risk Predictions for 2025
- The Intersection of Artificial Intelligence, Regulation and Risk Management
- Deepfake Technology: A Demonstration of Video Manipulation

Gallagher Cyber Insights & Client Alerts:

- 2025 Cyber Insurance Market Conditions Outlook
- Risk Bulletin: The Emerging Threat of Quantum Computing
- The Chief Artificial Intelligence Officer: Leading AI Innovation and Risk Management
- Change Healthcare Cyberattack: Guidance and Insurance Implications