RYAN SPECIALTY

FINANCIAL LINES CYBER

Healthcare

Innovative Insurance Solutions for Complex Cyber Risks

Cyber Exposures in Healthcare

Unique Exposures

Healthcare organizations are encountering a growing number of cyberattacks targeting their critical infrastructure. These attacks can lead to substantial data breaches in digital health information systems, jeopardizing both patient safety and privacy. The healthcare sector is exceptionally exposed to privacy breaches not only because of the extremely sensitive nature of the patient data being stored and managed, but also because many global healthcare organizations are grappling with vast volumes of digital data housed in outdated legacy systems. These systems often lack robust monitoring and security protocols, creating critical points of potential exposure. These vulnerabilities were starkly highlighted in February 2024, when multiple U.S. healthcare facilities were compromised during the UnitedHealth Group cyberattack.[i]

Another example of cyber exposures specific to the healthcare sector is the widespread use of the vendor Change Healthcare, which facilitates revenue and payment cycle management, connecting providers and patients across the U.S. healthcare ecosystem. Today, most healthcare operations rely on such platforms in some capacity, and this digital dependency has introduced a new level of vulnerability. Hospitals have never been more exposed to operational disruptions caused by system outages.

Regulatory and Third-Party Litigation

Given the highly sensitive nature of the data handled by healthcare organizations, the industry has traditionally prioritized regulatory compliance, often at the expense of proactive security measures. However, regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union have shifted the landscape, placing data protection and cybersecurity squarely at the forefront. Failure to safeguard patient information can trigger regulatory investigations, hefty fines, and third-party legal claims. Importantly, security risks extend beyond cyberattacks to include physical threats, such as the theft of paper records and even low-tech breaches like dumpster diving. In today's environment, security must address both digital and physical vulnerabilities.

Data Privacy and Business Interruption

While threat actors actively target personally identifiable information (PII), medical data remains a top target for cybercriminals. In 2023, 1,220 of the 1,378 reported security incidents in healthcare were data breaches.[ii] The financial toll is staggering. Each breach cost an average of $10.93 million, which is more than double the average in the next most affected industry, finance.[iii]

As healthcare records are increasingly digitized and electronic protected health information (ePHI) flows more freely online, the industry is under immense pressure to achieve more with fewer resources, balancing limited budgets while staying at the cutting edge of innovation. In response, healthcare providers have invested heavily in digital infrastructure, particularly in systems like Hospital Management Information Systems (HMIS). These systems function as the central nervous system of modern hospitals, automating critical functions such as bed allocation, pharmacy logistics, staffing, and patient flow. Interruptions to HMIS can have costly and far-reaching impacts on physicians, staff, and patients.

Healthcare is more connected than ever. Cybersecurity must be more proactive.

Healthcare is moving toward integrated care, and the rise of interconnected systems has introduced new vulnerabilities, especially through Internet of Things (IoT) medical devices. Devices like drug-infusion pumps and pacemakers have been found susceptible to cyber threats, posing serious risks to patient safety.

The scale of the threat is growing. According to *The HIPAA Journal*, the number of healthcare data breaches has steadily increased over the past 14 years, with over 133 million records compromised in 2023.[iv] The Q1 2024 breach of UnitedHealth Group's Change Healthcare environment further underscored the danger, putting 6,000 hospitals, 1 million physicians, 125,000 dentists, 39,000 pharmacies, and 700 laboratories at risk.[v]

From radiology imaging software and patient data archives to telehealth platforms connecting doctors across the globe, Ryan Financial Lines ("RFL") understands the complex digital ecosystem healthcare professionals rely on. With these technologies come significant risks, ranging from data breaches to system failures, that can disrupt care and compromise patient trust.

CYBER THREATS IN HEALTHCARE

- Protected health information (PHI) and personally identifiable information (PII)
- Violation of regulations (HIPAA and GDPR)
- Extortion and ransomware
- Intellectual property (IP) infringement and trade secrets
- Supply chain and third-party vendors
- Threat to Internet of Things (IoT) medical devices

Illustrative Claim Scenarios*

Privacy Breach

Employee of ABC Physicians has their employee email account hacked from a phishing attack. The IT department discovers the unauthorized access of the employee's email account a month later. ABC Physicians' IT department launches an investigation with help from a third-party forensic firm. The investigation finds that the email accounts included patients' personal information, such as insurance information, medical data and dates of birth. ABC Physicians begins notifying patients and recommends that patients review any statements they receive from their insurance carrier to make sure they're not billed for services that they didn't receive.

Privacy Breach

HospitalX's third-party transcription vendor is hacked because of an error made during a software upgrade. This breach results in the exposure of 20,000 HospitalX's patient records over a period of two months. HospitalX hires forensic investigators and post-breach lawyers to draft breach notifications.

Ransomware

HospitalX uses an HMIS system to host its patients' medical data, including medicine dosages and diet information. A ransomware attack on the HMIS blocks access to the patients' data and asks for a payment of $1 million USD in Bitcoin to allow access to the patients' data. During the cyberattack, nurses and doctors are unable to prescribe the correct dosage of medicine. HospitalX has not backed up its data on a different server. They are forced to immediately hire cyber investigators and IT experts to see if the ransom is worth paying.

Ryan Financial Lines' (RFL) cyber insurance solution is built to help shield against enterprise risks associated with operating modern health information systems. We don't just insure data — we help empower resilience.

*These examples are hypothetical scenarios used solely to illustrate potential outcomes and not reflective of policy terms and conditions or the facts of a specific claim.

RFL's Cyber Solution

At RFL, we treat cyber as a core operational peril, not just a technical issue. Our policy is built to address the full spectrum of risks that data and system failures can create across the healthcare enterprise. From business interruption and data restoration to computer crime, social engineering, extortion, and privacy breaches, RFL's cyber insurance solution is designed to help respond when it matters most. Our best-in-class coverage combines first-party cost reimbursement with third-party defence and regulatory protection, underpinned by a broad, forward-thinking definition of data and computer systems.

1ST PARTY

Crisis Response: Intended to help mitigate the costs and expenses to respond to a system event or privacy breach event

Cyber Extortion: Intended to help mitigate the costs and expenses to respond and resolve an extortion demand that threatens to release or destroy data and/or disrupt or damage the computer system

Computer System Interruption: Intended to help mitigate the net income losses and additional operating costs that occur during a business interruption event due to systems and / or data being taken offline in a malicious attack or other operational failure. Coverage may include:

- Renting, leasing or hiring external equipment to reduce the duration of a material interruption
- Additional operating costs including services, premises, employing contract staff, and overtime cost
- Costs to switch service from a named IT vendor to a new provider if the service cannot be restored within the indemnity period (when event is caused by vendor systems)
- Procuring product or services from alternative sources to meet contractual obligations in supplying the insured's customers
- Paying any service credits or contractual penalties that the insured is contractually required to pay as a result of a material interruption

Reputational Damage: Intended to help mitigate the direct loss of net income due to a reduction in business or the loss of a service contract with a client in the wake of the public being notified of a system event, privacy breach event, or network security event

Fraud and Social Engineering: Intended to help mitigate the direct financial loss from the wrongful transfer of money by fraudulently accessing the computer system or intentionally misleading an authorized person to transfer funds to a third party purporting to be a vendor, client, or employee. This cover also extends to the financial loss arising from the unauthorized access of a client's telecommunication system by a malicious third party

Data and Software Restoration: Intended to help mitigate the costs and expenses to recover corrupt data or software, and potentially even upgrading / replacing affected software applications or equipment

3RD PARTY

Privacy Breach and Other Third-Party Liability: Intended to help mitigate the defence costs and damages arising from:

- Any unauthorized disclosure or access to personal or confidential corporate data
- Any liability that arises from other cyber events such as the transmission of a malicious code, contract breaches due to a business interruption (BI) event, and unauthorized access to data by a third party

Vendors

In a time of crisis, RFL wants insureds to have access to best-in-class vendors and for the claims process to be as easy to execute as possible. RFL's cyber solution not only provides insureds with thorough cyber breach response options but also aligns them with a panel of expert resources to help limit their exposure to cyber events and to help minimize the fallout if they experience a cyberattack.

Privacy Counsel: UK & ROW

Hotline:
Kennedys Law LLP

Incident reporting:
RyanFinLinesIR@kennedyslaw.com
UK / EMEA: +44 203 137 8749
AUS / APAC: +613 9498 6688

Alternate counsel options:
Weightmans LLP
Pinsent Masons LLP

Privacy Counsel: US

Hotline:
Pierson Ferdinand LLP

Incident reporting:
RFLCyber@pierfed.com
833-737-7444

Alternate counsel options:
McDonald Hopkins LLC
Cipriani & Werner, PC
Mullen Coughlin
Wood Smith Henning & Berman LLP

Forensics: US

CyXcel
S-RM
Kroll
IronGate
CrowdStrike
PNG Cyber
Palo Alto Networks - Unit 42

Forensics: UK & ROW

CyXcel
S-RM

Data Mining

Asceris
Consilio
CyXcel
Epiq

Notifications

Epiq
IDX
Kroll

Please note that the use of these vendors is subject to the terms, conditions, and reporting requirements outlined in your policy. We reserve the right to amend our vendor panel at any time.

RYAN SPECIALTY | FINANCIAL LINES CYBER

Who We Are

Ryan Financial Lines (RFL) was formed in March 2024 to offer clients a wide-ranging, single platform of financial lines insurance products. Ryan Financial Lines brings together the Management and Professional Liability talent at Ryan Specialty Underwriting Managers to provide greater synergies and efficiencies that further enhance risk management solutions and services for our clients and carriers. This unified approach brings together our expansive network of expertise with more than 70 teammates located across key territories, including North America, United Kingdom, Europe and Latin America.

ryanfinlines.com

UK & ROW: RFL-UK-Cyber@ryanfinlines.com | US: RFL-US-Cyber@ryanfinlines.com

[i] "Hack at UnitedHealth's Tech Unit Impacted 192.7 Million People, US Health Dept Website Shows." Reuters, August 14, 2025. https://www.reuters.com/business/hack-unitedhealths-tech-unit-impacted-1927-million-people-us-health-dept-website-2025-08-14/.

[ii] 2024 Data Breach Investigations Report: Healthcare Snapshot. 2024. Verizon. https://www.verizon.com/business/resources/Ta55/infographics/2024-dbir-healthcare-snapshot.pdf.

[iii] Alder, Steve. 2023. "IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million." The HIPAA Journal. July 24, 2023. https://www.hipaajournal.com/2023-cost-healthcare-data-breach/.

[iiii] Alder, Steve. 2025. "Healthcare Data Breach Statistics." The HIPAA Journal. May 26, 2025. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[iv] Arif, Mohammad. 2024. "UNPACK: The UnitedHealth Group Hack - a Billion Dollar Cyber Loss Event through the Lens of FAIR." Fairinstitute.org. May 6, 2024. https://www.fairinstitute.org/blog/unitedhealth-hack-data-fair-analysis.