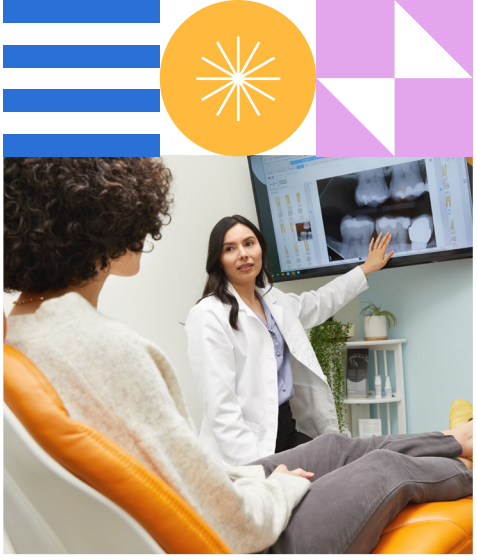
Coalition



THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Healthcare Industry

Patient confidentiality is paramount in the healthcare industry. Healthcare providers and other related businesses are entrusted to collect, transmit, and store not only health-related information but also personal, financial, and other identifying details. This sensitive data is often required to be available digitally, making it a frequent target of cybercriminals.

Healthcare providers use many technologies that present cyber risks, such as internet-accessible medical devices, remote monitoring tools, and telemedicine applications. Organizations must not only protect sensitive patient information but also maintain security and availability of data, as well as lifesaving technology. Even a minor breach or failure can have major cyber implications, potentially hindering the delivery of service and impacting the health and safety of patients.

Merger and Acquisition (M&A) activity also increases risks in the healthcare industry. Acquirers must evaluate cyber risks thoroughly during the M&A process and prior to integration to avoid inheriting new cyber threats and exposures.

Claims Insights

It's just a little security incident. How bad could it be?

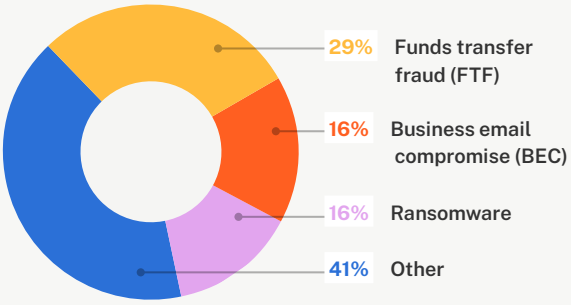
$134,000

Average cost of a cyber insurance claim for healthcare organizations

Claim Examples

ORGANIZATION	EVENT TYPE	LOSS
Patient-Centered Medical Home	Funds Transfer Fraud	$500,000
Behavioral Health Services	Business Email Compromise	$125,000
Medical Equipment	Ransomware	$275,000

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT — Although it's not the leading event type, the average ransomware loss for organizations in the healthcare industry is nearly $355,000.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Unique Exposures

Most healthcare organizations use data and technology. Why is that risky?

Essential Technologies Can Create Cyber Risk

Customer relationship management (CRM) systems
CRM systems are used to support business development activities. Containing client data and confidential corporate information, CRM systems could be compromised and leveraged for malicious purposes, resulting in a data breach.

Electronic medical record (EMR) systems
Often cloud-or web-based, these essential systems are used to store, manage, and share patient records. A data breach or incident involving an EMR system could cause data privacy issues, regulatory violations, or even a disruption in services to patients in need of care.

Email
Business email compromise (BEC) is a frequent cause of cyber insurance claims for healthcare organizations, which can trigger data breaches, business interruption and even reputational damage.

End-of-life software & hardware
Organizations may use outdated technologies with the belief that upgrading would be expensive, time-consuming, and disruptive. However, technologies no longer supported by the manufacturer often have known security vulnerabilities and may lack important security features to protect against modern threats.

Medical devices
Outdated software, insufficient security features, and a lack of hardened baseline configurations can lead to vulnerabilities in medical devices. Exploitation of insulin pumps, defibrillators, and numerous other devices can compromise operations, patient safety, and data privacy.

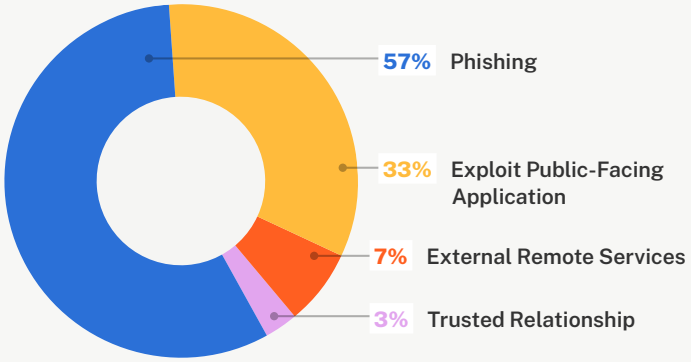
Patient portals
These websites enable patients to access electronic health records and make it easier to fill prescriptions or schedule appointments. However, a breach could expose large amounts of data and cause serious disruption due to the volume and sensitive nature of the information.

Payment processing software
Funds transfer fraud and invoice manipulation are often major drivers of cyber claims. For healthcare providers that use electronic payments, even one fraudulent transfer can have dire financial consequences.

Telemedicine platforms
Telehealth relies on connecting with patients and exchanging information on the internet. Patients with vulnerable devices or networks can expose healthcare organizations to phishing, malware, and other cyber attacks.

Cyber Claims in the Healthcare Industry by Attack Vector

KEY INSIGHT —— Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims**.



Source: Coalition forensics survey data

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Sensitive Data Can Increase Business Liability

Biometric data
Fingerprints, retina scans, and other biometric data technologies are used by medical offices to ensure patient identification. Much like passwords, this data can be stolen and used to impersonate individuals and perpetuate cybercrime.

Financial data
Collecting and processing financial information requires adherence to industry standards. Mishandling or unauthorized disclosure of financial data can cause direct harm to patients and trigger industry and regulatory investigations.

Non-sensitive personal information
Some data may be publicly available and not considered protected, but a breach can still impact trust and public image if it appears the organization did not handle the situation appropriately.

Personally identifiable information (PII)
PII is any data that can potentially identify a specific person. PII can be used to launch cyber attacks or gain access to networks to initiate attacks. Organizations that mishandle PII or fail to respond to a data breach appropriately can be subject to fines, penalties, and other financial damages.

Protected health information (PHI)
Most healthcare organizations collect or access PHI. Bound by the Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule, they carry additional data protection and reporting requirements if an actual or suspected data breach occurs.

Sensitive employee information
Every organization collects and stores information about its employees. Unauthorized access or disclosure of this data can cause direct harm to employees.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- HIPAA
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- International data privacy and consumer protection regulations (e.g. GDPR)
- State data privacy & consumer protection laws (e.g. CCPA)
- State notification requirements
- Payment Card Industry Data Security Standard (PCI DSS)

$10.1 million

Average total cost of a **data breach** for healthcare organizations[1]

1. IBM Security, Cost of a Data Breach Report 2022

Coalition

Business Impacts

What can healthcare organizations expect after a cyber incident?

Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, also known as first-party expenses. If a healthcare organization experiences a data breach involving PHI, it will require a prompt response and the need for additional legal counsel, forensic investigation, victim remediation, and notification to comply with regulatory requirements. Simple investigations can cost tens of thousands of dollars, while more complex matters can increase costs exponentially. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 1st Party
- Breach Response
- Crisis Management
- Cyber Extortion

Liability to others

Navigating the patchwork of laws and regulations after a security incident or data breach is especially difficult for organizations that operate in a highly regulated industry across multiple legal jurisdictions. A data breach or security failure can trigger liability to third parties and cause bodily harm or injury, even if the management of healthcare records is outsourced and the organization is otherwise in compliance with applicable regulations. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 3rd Party
- Multimedia Content Liability
- Network and Information Security Liability
- PCI Fines and Assessments
- Pollution
- Regulatory Defense and Penalties

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on a healthcare provider's ability to operate and can be highly visible to patients and other stakeholders. Even short periods of disruption can lead to direct loss of revenue and inhibit an organization's ability to support its patients, negatively impacting not only patient retention but also the delivery of essential care. Relevant insuring agreements may include:

- Business Interruption & Extra Expenses
- Reputation Repair

Cybercrime

Beyond ransomware and data breaches, cyber events can result in financial theft for a healthcare provider or its patients — often without an actual breach. If an attacker dupes someone in the billing department to alter payment instructions, an organization can lose tens or hundreds of thousands of dollars almost instantly. Attackers can also gain access to email accounts and send fraudulent invoices or payment instructions to patients, customers, and other third parties. Relevant insuring agreements may include:

- Funds Transfer Fraud
- Invoice Manipulation
- Phishing (Impersonation) and Proof of Loss Preparation Expense Endorsement
- Service Fraud

Recovery and restoration

After a cyber event, resuming operation is no easy task. If an attacker damages or destroys essential technology, data, or physical equipment, an organization may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require purchasing new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

1.87%
Coalition 2022 overall claims frequency

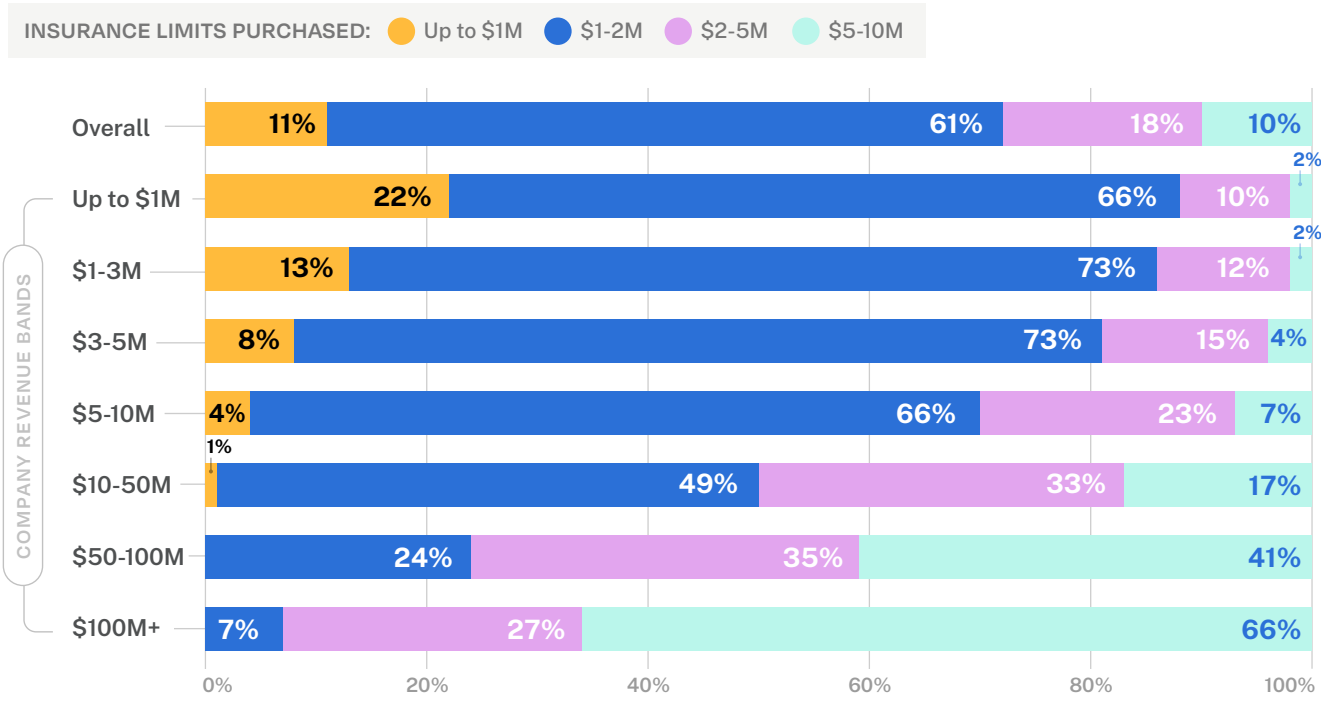
↓ 22%
Year-over-year decrease in Coalition claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the the healthcare industry

PEER PURCHASING HABITS BY REVENUE



Source: Coalition policyholder data

KEY INSIGHT —— Most small and medium-sized businesses in the healthcare industry purchase $1M-2M in limits, while many mid-market organizations purchase $5-10M in limits. For those needing more than $10M in limits, Coalition offers primary and excess terms for businesses up to $5B in revenue.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

The Power of Active Insurance

Why do healthcare organizations choose Coalition?

47%	43%	73%
Reported cyber events handled with no cost to policyholder	Reduction in critical vulnerabilities among policyholders in 2022	Average decrease in ransomware payment amount via negotiation

Active Insurance* is designed to help prevent digital risk before it strikes. Our new approach to managing digital risk provides **three layers of support**:

Active Protection

Monitoring and alerting to identify and prevent risk before it strikes

Active Response

Access to in-house resources that accelerate response and coverage if an incident occurs

Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Insurance as active as digital risk

In the digital economy, Coalition wants to ensure that all organizations can thrive by helping to protect them from the threat of emerging risks. We've built an expert team across incident response, claims, and our panel vendors. In the event of a claim, Coalition helps organizations respond and recover so they can get back to business.

Brokers

Get appointed today at signup.coalitioninc.com

Healthcare organizations

Get a free risk assessment at control.coalitioninc.com

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **coalitioninc.com**