



HFMA/NEHIA

2024 Compliance & Internal Audit Conference Code Red: Responding to Cyber and Ransomware Attacks in Healthcare


Wednesday, December 4 - Friday, December 6, 2024
Mystic Marriott Hotel, Groton, CT



PAUL
HASTINGS

Code Red: Responding to Cyber and Ransomware Attacks in Healthcare

December 2024



PAUL HASTINGS

Agenda

- Overview
- Building a strong incident response team
- Special considerations with ransomware
- Third-party and supply chain risk
- Prepare for future cyber attacks





Overview



Why is the Health Care Industry Vulnerable to Cyber Threats?

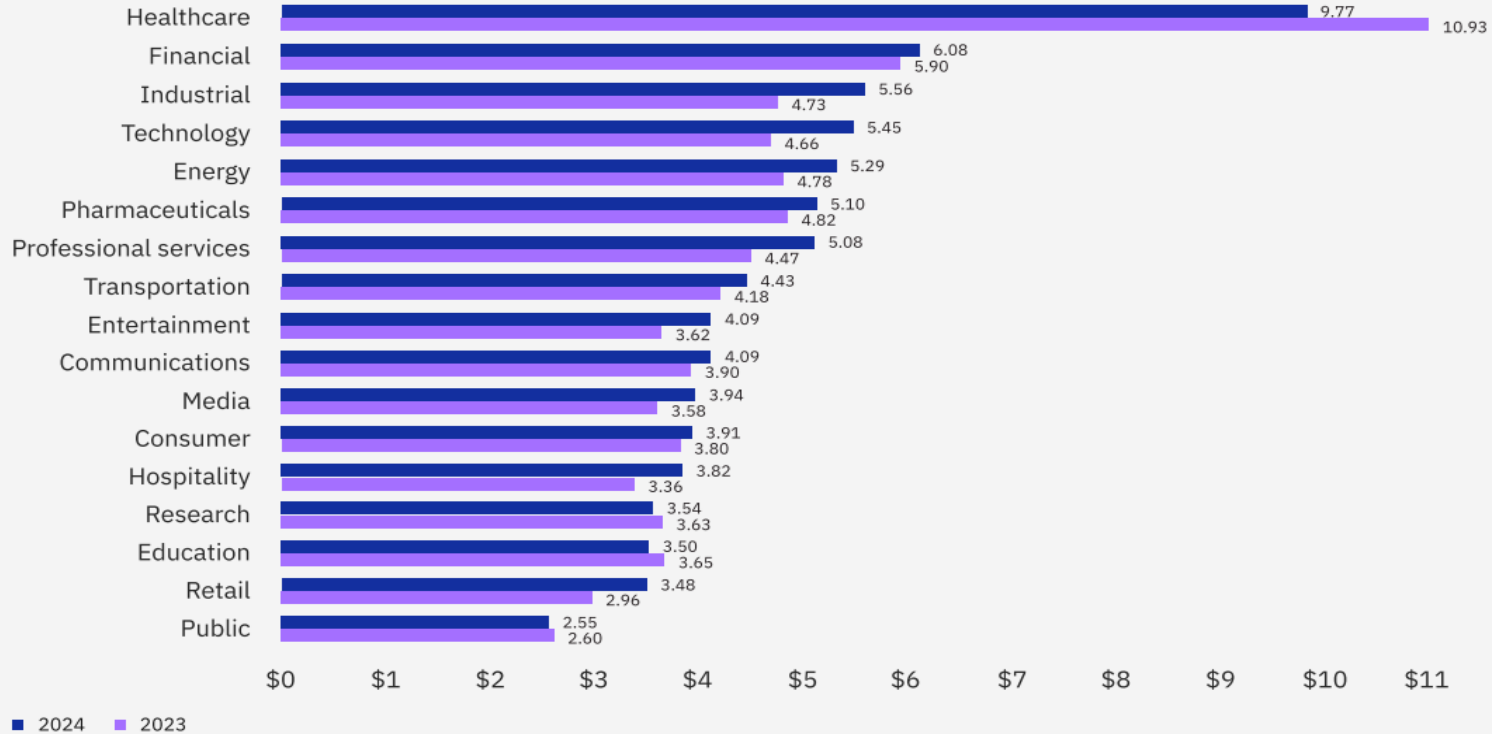
Health information is highly valuable on the black market.

Health operations can be life or death, making the functioning of a health care entity or institution's systems critical.

Health information technology provides critical and life-saving functions and consists of connected, networked systems that leverage wireless technologies and, in turn, leave those systems more vulnerable to cyber attacks.

Health Care Data Breaches Come with High Costs

Cost of a data breach by industry

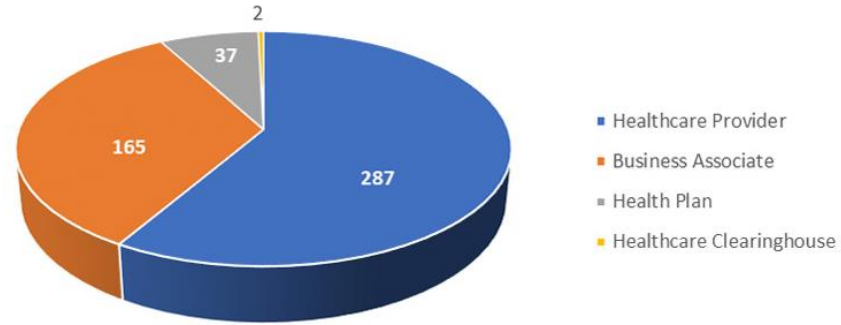


Source: IBM, Cost of a Data Breach 2024. Measured in Millions.

What Do Cyber Threats in Health Care Look Like?

- Last year had the most reported data breaches and the most breached records. In 2023, **725 data breaches** were reported to OCR and across those breaches, more than **133 million records** were exposed or impermissibly disclosed.
- Worldwide **ransomware attacks** against the health care sector have **nearly doubled since 2022**, reaching **389 claimed victims** in 2023 compared with 214 in 2022.
- Due to ransomware attacks, U.S. hospitals have delayed medical procedures, disrupted patient care because of multiweek outages, diverted patients to other facilities, rescheduled medical appointments, and strained acute care provisioning and capacity.

Data Breaches at HIPAA-Regulated Entities in 2024





Change Healthcare 2024 Ransomware Attack



Change Healthcare discovered it was the victim of a ransomware attack on February 21, 2024.



ALPHV/Blackcat ransomware group used compromised credentials to remotely access a Citrix portal that did not have multi-factor authentication (MFA).



One in three Americans' information is touched by Change Healthcare's systems, which means the attack could be the largest ever health care data breach, potentially involving PHI of 100+ million Americans.



Types of information exposed/stolen vary by individual and may include information such as insurance information, diagnoses, images, treatment, and claims.



Building a Strong Incident Response Team




Building a Strong Incident Response Team

Incident Response teams may vary slightly in their makeup depending on the organization, but there are some common roles that may be included in an incident response team at any organization including:

- **Incident commander:** Conducts overall incident coordination and decision-making.
- **Triage analyst:** Assess incident severity, prioritizes response efforts, and identifies critical areas for immediate attention.
- **Forensic investigator:** Conducts detailed investigations to determine the root cause of the incident and gathers evidence for further analysis.
- **Communications specialist:** Manages internal and external communications to ensure stakeholders are informed about the incident and its progress.
- **Remediation expert:** Develops and implements strategies to mitigate the impact of the incident, including containment and recovery of affected systems.
- **Legal advisor:** Provides guidance on legal and compliance aspects to ensure the incident response efforts align with relevant regulations and requirements.
- **Public relations representative:** Manages public image and perception of the organization during and after a cyber incident to maintain trust and credibility.

Key Incident Response Considerations

- 
- 1 If you are a public company, establish written disclosure controls related to cyber incidents with key points of escalation.
 - 2 Regulators may require day-to-day and minute-by-minute accounts of a cyber event.
 - 3 Clear points of escalation to board or C-level executives; designated individuals responsible for escalation and reporting.
 - 4 Privilege and communications considerations with auditors during investigations.
 - 5 Records of events, including non-privileged summaries are important for showing regulators you did your due diligence and providing a basis for certain actions taken, including if events are not reported.
 - 6 Attorney-client privilege and sufficient records can be complicated in the event of litigation or regulatory investigations.

Unique Challenges for Incident Response Teams

Communication
Channels

Department-
Specific Disaster
Plans

Third Party
Communications

Delayed
Escalation

Reporting &
Investigation
Roadblocks



Special Considerations with Ransomware



Legal, Regulatory, and Ethical Issues in Deciding Whether to Pay Ransom

- FBI advises against paying ransom as it encourages criminal activity and may further endanger an organization once it's known to hackers the organization will pay.
- Payments to criminals going against an organization's core values, culture, or code of ethics.
- Motivation to get decryption key to get systems back online and to prevent stolen sensitive data (PII, PHI) from being made public.
- Sanctions checks should be completed and clearly documented. The U.S. Office of Foreign Assets Control (OFAC) poses sanction risks associated with ransomware payments.
- Threat actors may not hold up their end of the deal, and data may still be published or sold.
- If an organization has cyber insurance, it should consider degree to which insurance company must be involved whether it prefers that insurance cover the ransom payment.

Is Deployed Ransomware a Breach?

Possibly.

- Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a **fact-specific determination**. A breach under the HIPAA Rules is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” See 45 C.F.R. 164.402.
- When electronic protected health information (ePHI) is **encrypted** as the result of a ransomware attack, **a breach has occurred** because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.
- Unless the covered entity or business associate can demonstrate that there is a “...**low probability** that the PHI has been compromised,” based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then **comply with the applicable breach notification provisions**, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

Recent OCR Enforcement Actions Under Security Rule

- **Providence Medical Institute Notice of Final Determination (Oct. 3, 2024)**
 - Ransomware enforcement action following 2018 breach report. Failed to have a BAA and failed to implement policies and procedures to allow only authorized persons or software access to ePHI.
- **Cascade Eye and Skin Centers, PC Resolution Agreement and Corrective Action Plan (Sept. 26, 2024)**
 - Ransomware enforcement action following complaint. Failed to conduct complaint risk analysis and to have sufficient monitoring of its system activity to protect against cyber attack.
- **Heritage Valley Health System Resolution Agreement and Corrective Action Plan (July 1, 2024)**
 - Ransomware compliance review following media reports. Failed to conduct accurate and thorough risk analysis and to establish and implement policies for responding to an occurrence that damaged systems with ePHI and to restrict access.
- **Green Ridge Behavioral Health, LLC Resolution Agreement and Corrective Action Plan (Feb. 21, 2024)**
 - Ransomware enforcement action. Failed to conduct accurate and thorough risk analysis, to implement security measures to reduce risks and vulnerabilities to a reasonable level, to implement policies to regularly review records of system activity, and to disclose information only as permitted by Privacy Rule.



Third Party & Supply Chain Risk



NIST Examples of Cyber Supply Chain Best Practices



Security requirements included in every RFP contract



Once a vendor becomes part of the supply chain, a security team works with them on-site to address vulnerabilities and security gaps



Secure software lifecycle development programs and training for all engineers in the lifecycle



Source code is obtained for all purchased software



Supply chain cybersecurity management partners with teams touching products during the development lifecycle to ensure cybersecurity is at the forefront



Legacy support for end-of-life products and platforms



Tight controls on access by service vendors are imposed

Third Party Risks: Mergers and Vendors

Mergers

- Merging systems
- Insurance risk
- Lack of IT and IS investment pre-merger
- Threat actor focus on publicly disclosed mergers

Vendors

- Communication
- Notification
- Ongoing litigation
- Contractual provisions
- Diligence



Prepare for Future Cyber Attacks

Best Practices to Protect Against Ransomware and Other Cyber Threats

Secure offline,
encrypted
backups of
critical data

Legacy system
management

Administrative
privilege review

MFA and
network
segmentation

Penetration
testing and risk
assessments

Incident
response plan

Tabletop
exercises

Employee
training

Vendor
management

Data
minimization

Law
enforcement
relationships



QUESTIONS?



Michelle A. Reed

Partner,
Litigation Department

2001 Ross Avenue, Suite #700-168
Dallas, TX 75201
P: +1(972) 936-7475
F: +1(972) 936-7375

michellereed@paulhastings.com

Michelle Reed is a partner in the Data Privacy and Cybersecurity Group of Paul Hastings and is based in the firm's Dallas office. She has two decades of experience advising companies, boards, and executives on navigating the evolving risks in privacy and cybersecurity regulation, enforcement, and class action litigation.

Michelle is a leading lawyer in crisis management, guiding corporations in data breach investigations and notifications, Securities and Exchange Commission (SEC) cybersecurity compliance, regulatory investigations, privacy and data protection compliance, and emerging developments in artificial intelligence, biometrics, children's privacy, geolocation, and national security.

A Certified Information Privacy Professional (CIPP/US, International Association of Privacy Professionals), Michelle assists clients in conducting comprehensive privacy and security risk assessments and develops policies and procedures to mitigate and remediate privacy and cybersecurity threats, frequently working across teams to find practical solutions. *Chambers* describes Michelle as "incredibly responsive and super knowledgeable."

Michelle also represents clients in a variety of complex civil litigation matters, including securities class actions, derivative suits, and consumer class actions.

Representative Experience

Class Actions

- Representing numerous companies in defending against claims asserted under federal and state anti-wiretapping laws, including the California Invasion of Privacy and the Wiretapping and Electronic Surveillance Control Act.
- Defended client in consolidated putative class actions arising from data breach involving the alleged exposure of personally identifiable information and asserting common law tort claims, as well as New York and California statutory claims, including claims under the California Consumer Privacy Act (CCPA), and obtained a full dismissal at the district court level of all claims.

Data Privacy

- Advising a multinational Fortune 500 company on the development, communication, and operationalization of privacy program and governance structure in the U.S., Canada, and international data protection across 18 jurisdictions, including creation of privacy principles, policies, notice, cross-border data strategy, data lifecycle management, individual rights management, Privacy by Design, third-party risk management, and training.
- Built an extensive privacy risk assessment framework for one of the largest broadband communications and video services providers in the U.S., evaluating privacy risk for delivery of content to approximately 4.9 million customers across 21 states.
- Advising private equity and other investment funds in the U.S., Europe, and Asia on implementing and operationalizing the CCPA, NY Department of Financial Services Cybersecurity Regulation, GDPR, GLBA, SEC rules, and evolving state and federal privacy regulations.

Cybersecurity

- Represented an online retailer in a data breach affecting 50 states and 16 countries; assisting with the identification of the nature and scope of the intrusion; working with the information technology team and experts to restore normal system operation; providing customer notification and call center management, states' regulatory negotiations, discussions with PCI-DSS council and payment card issuers, and public relations communications.

- Led investigation of a ransomware attack by an advanced persistent threat actor, retaining forensic investigators, recovery and restoration service, and public relations consultants, ensuring OFAC compliance, advising on SEC cyber disclosures, facilitating communications with auditors, communicating with law enforcement, and providing notification to approximately 16 million individuals and 52 different regulators.

Awards & Accolades

- *Chambers Global*, Privacy & Data Security (2024)
- *Chambers USA*, Privacy & Data Security: Cybersecurity USA–Nationwide (2021-2024)
- *Chambers USA*, Litigation: Securities–Texas (2022-2024)
- *D Magazine*, Best Lawyers in Dallas, Business/Commercial Litigation (2017, 2022-2024)
- *The Legal 500 U.S.*, Cyber Law (2017-2024)
- *The Legal 500 U.S.*, Securities Litigation: Defense (2023-2024)
- *Lawdragon*, 500 Leading Litigators in America (2024)
- *Corporate Counsel*, Women, Influence and Power in Law Awards, Best Mentor (2023)
- *Pro Bono Champion*, ABA Commission on Immigration (2023)
- *The Best Lawyers in America*, Litigation - Securities (2022-2023)
- *Cybersecurity Docket*, Incident Response (2021-2023)
- *JD Supra*, Readers' Choice Awards (2020-2024)
- *The American Lawyer*, Best Mentor finalist (2021)
- *Super Lawyers*, Securities Litigation (2015-2020)
- *Super Lawyers*, Class Action/Mass Torts (2015-2020)
- *Super Lawyers*, Civil Litigation: Defense (2015-2020)
- *Texas Lawyer*, Attorney of the Year finalist (2020)
- *Who's Who Legal*, Investigations (2020)
- *Texas Lawyer*, Texas Trailblazer (2019)
- National Diversity Counsel, Top 50 Women Lawyers in Dallas (2017)
- *Dallas Business Journal*, Women in Business Award (2017)
- *Texas Lawyer*, Lawyers on the Rise (2016)
- Recipient of the Frank Scurlock Award for Outstanding Pro Bono Service, State Bar of Texas (2013)



Rachel Kurzweil

Of Counsel,
Litigation Department

2050 M Street NW, Washington,
DC 20036

P: +1.202.551.1940

F:Fax: +1.202.551.0440

rachelkurzweil@paulhastings.com

Rachel Kurzweil is an Of Counsel in the Data Privacy and Cybersecurity Group and is based in the Firm's Washington D.C. office. Rachel is a leading privacy, cyber and health regulatory attorney with broad ranging experience advising clients in areas of U.S. state, federal and international privacy regulation and compliance, data breach, cyber and privacy incidents, and regulatory compliance. Rachel has extensive experience operationalizing global privacy and cybersecurity laws and regulations including the CCPA, VPPA, CAN-SPAM, GLBA, TCPA, DPPA, COPPA, FISA, and other state privacy laws, state wiretapping laws including CIPA and WESCA, GDPR and other international privacy laws.

Rachel routinely assists a wide variety of multinational clients across industries with compliance with international, state and federal privacy, security and data breach notification laws and regulations, including conducting privacy assessments, drafting privacy policies and procedures, and data privacy impact assessments. She also has deep expertise in advising clients in highly regulated sectors, including financial services and health care. She counsels these companies and coordinates with their technology and advertising partners, to address legacy regulatory issues and the emerging privacy and cyber risks that arise from industry innovations and data sharing. She also regularly represents clients in strategic transactions involving personal data and cybersecurity risk.

Rachel regularly assists clients with complex health and life sciences matters involving the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), Section 5 of the Federal Trade Commission Act and myriad state privacy, security and breach notification laws, as well as adjacent regulatory regimes such as the ONC Information Blocking Rule. She has extensive experience in helping clients navigate the intersection between federal privacy and data protection laws and state regimes such as the California Consumer Privacy Act (CCPA), the Washington My Health My Data Act (MHMDA) and the California Confidentiality of Medical Information Act (CMIA).

Prior to joining the firm, Rachel was a Counsel with an AmLaw50 law firm, specializing in privacy and health. She also worked as a Health Litigation Fellow with AARP Foundation.

Rachel is admitted in Maryland, Pennsylvania and Washington, D.C.



Our Firm

In today's world of transformative change, our purpose is clear—to help our clients and people navigate new paths to growth.

Founded in 1951, Paul Hastings has grown strategically to anticipate and respond to our clients' needs in markets across the globe. Our innovative approach and unmatched client service has helped guide our journey to becoming one of the world's leading global law firms in such a short time.

We have a strong presence throughout Asia, Europe, Latin America, and the U.S. We offer a complete portfolio of services to support our clients' complex, often mission-critical needs—from structuring first-of-their-kind transactions to resolving complicated disputes to providing the savvy legal counsel that keeps business moving forward.

A Top-Ranked Firm
on *The American Lawyer's* A-List of the Most Successful Law Firms in the U.S. nine years in a row

A Top-Ranked Firm
in the *Financial Times* Innovative Lawyer's Report across Asia, Europe, and North America

Top 10 for "Best Place to Work" in Vault's annual survey eight years in a row

A Top-Ranked Firm
for Best Overall Diversity, according to Vault

50 Serving 50% of the Fortune 100

117 of our clients are on Fortune's Most Admired List

58 We advise clients based in 58 countries around the world

Global Presence

The Americas

Atlanta	Orange County
Century City	Palo Alto
Chicago	San Diego
Houston	San Francisco
Los Angeles	São Paulo
New York	Washington, DC

Asia

Beijing
Hong Kong
Seoul
Shanghai
Tokyo

Europe

Brussels
Frankfurt
London
Paris



1 LEGAL TEAM to integrate with the strategic goals of your business.