Cyber Risk Benchmark Report on Healthcare Private Equity-Backed Portfolio Companies

June 4, 2025

Clearwater

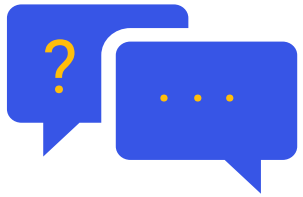
Welcome

- Meeting logistics and introductions
- Cybersecurity trends impacting healthcare organizations and investors
- Key findings from Clearwater's benchmark report on PE-backed healthcare companies
- Recommendations for strengthening cybersecurity by market segment
- Q&A

Meeting Logistics

Microphones

All attendees are on mute.



Questions

Type your questions in the Q&A box.

Resources

Upcoming events & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

Our Presenters

Baxter Lee, MBA

CFO
Clearwater

- 20 years in Finance, primarily in the healthcare sector
- 10 years of experience in banking, private equity and M&A
- Advise startups in strategic planning, operational development and capital raising

John Santana, CCSFP, CHQP, CISSP

Principal Consultant, Private Equity and Digital Health Team
Clearwater

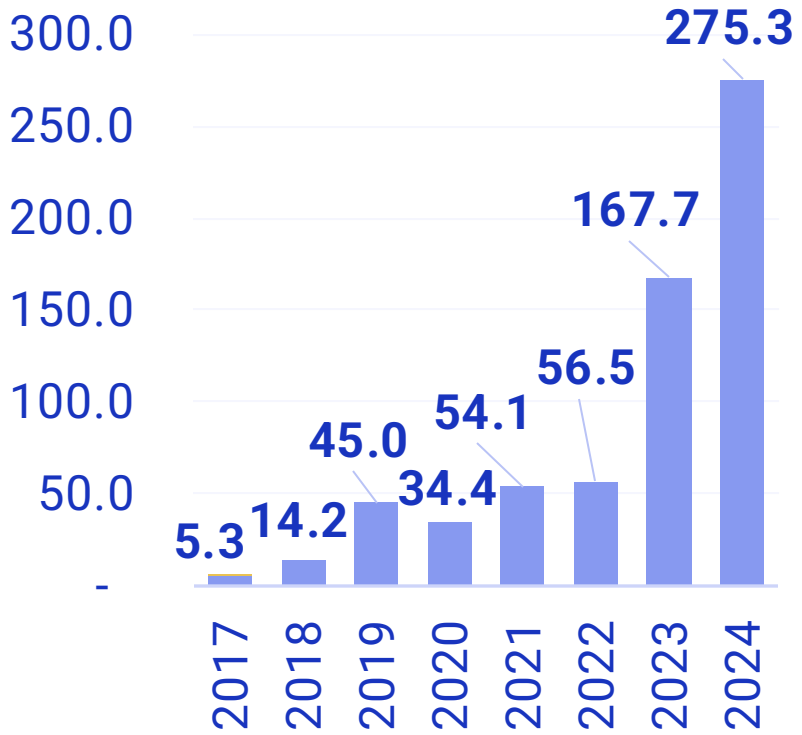
- Extensive experience supporting healthcare IT risk management initiatives, including portfolio-level Cyber Risk Management services
- Expertise in risk analysis and risk response engagements, as well as providing overall vCISO-level governance support regarding HIPAA, NIST, HITRUST, and 405(d) HICP
- Lead author of Clearwater's Cyber Risk Benchmark Report on PE-Backed Healthcare Companies

Healthcare’s Cybersecurity Imperative

Threats to Healthcare Continue to Grow

Breaches in healthcare continue to break records, and ransomware attacks are increasing, are more damaging and are taking longer to recover from.

Millions of Healthcare Records Breached[1]



Healthcare organizations report a ransomware attack last 12 months

2023	2024
60%	67%

> than 1 week to recover

2023	2024
50%	79%

Why are breaches increasing in healthcare and becoming harder to recover from?

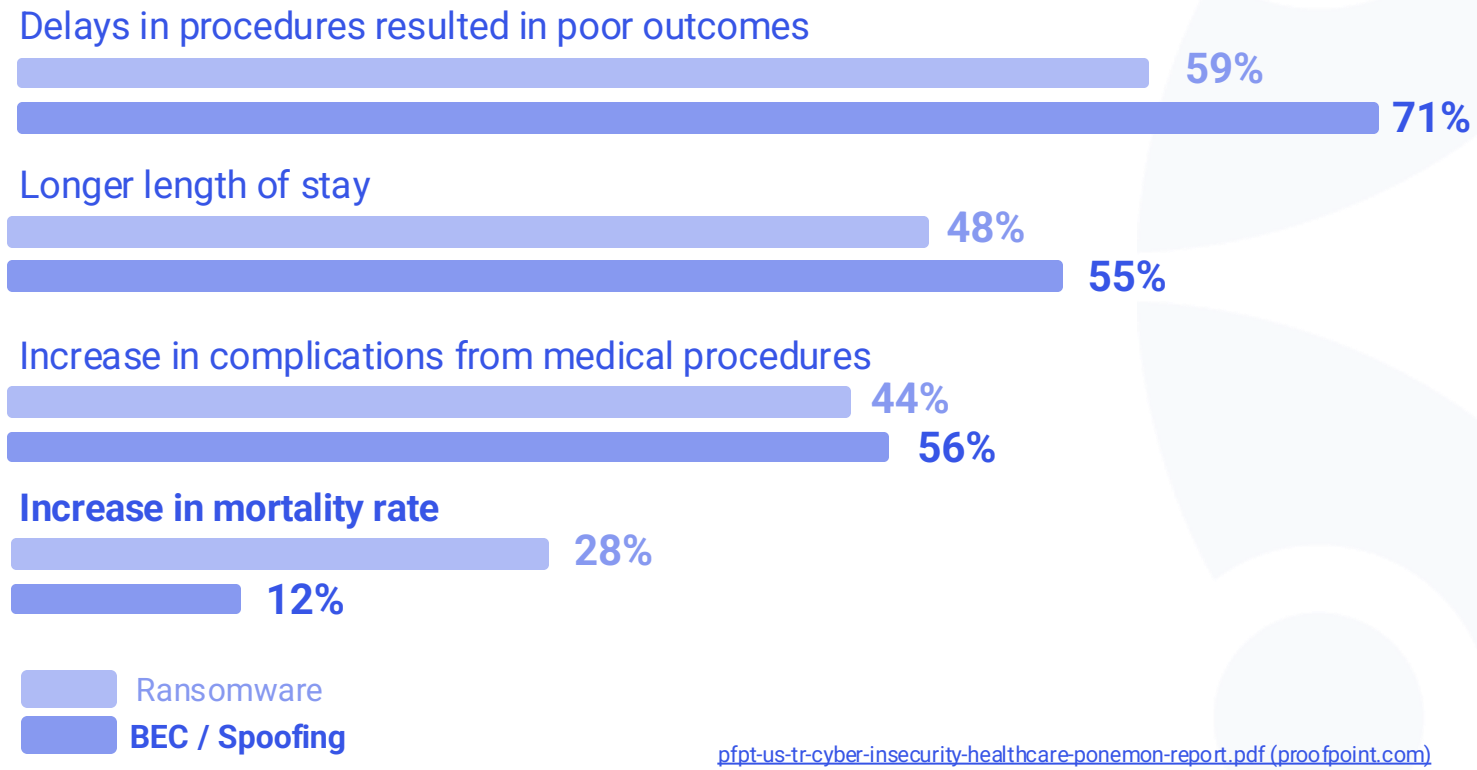
- Growing attack surface with more vulnerabilities
- ePHI is most valuable data
- Most likely to pay ransom
- Number of attackers increasing
- TTPs are evolving quickly
- Weak security programs
- Limited resources

1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 1/31/25; 2023 data pulled 11/3/24) + 90 million additional records Change Healthcare announced earlier this year
2 The State of Ransomware in Healthcare 2024 – Sophos News

Clearwater

Cybersecurity is Patient Safety

Numerous studies and surveys support that breaches and ransomware attacks directly impact patient outcomes and safety, in addition to costing an average of $9.5m just for small breaches.



pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf (proofpoint.com)

2021: CISA reported ransomware causes **excess deaths** due to disruption.[1]

2023: Of providers with a **ransomware** attack, **28% reported increased in mortality rates** following the attack.[2]

2023: JAMA study found hospitals adjacent to those affected by ransomware attacks *also* have disruptions in patient care and **risks to increased mortality**.[3]

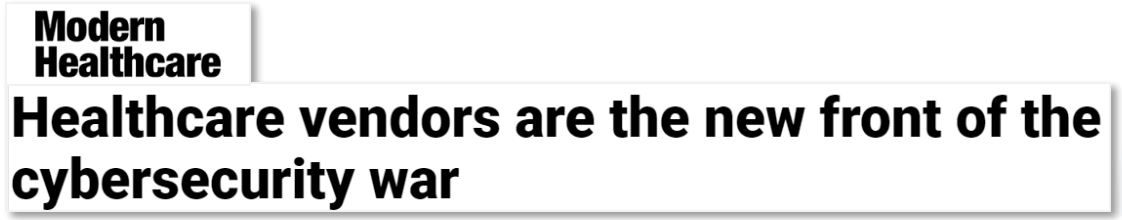
2023: FBI and DOJ treat patient cyber-attacks as **"threat to life"** crimes.[4]

1 CISA Insights Report: Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm
2 Cybersecurity Insecurity in Healthcare. The Cost and Impact on Patient Safety in Healthcare. Ponemon Institute. 2023.
3 Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US | Emergency Medicine | JAMA Network Open | JAMA Network
4 *"Hospital Resiliency Landscape Analysis." Healthcare and Public Health Sector Coordinating Council, Office for Civil Rights, Centers for Medicare and Medicaid Services, and HHS 405(d) Working Group. Joint Publication. March 2023."*

Clearwater

Vendor Cyber Risk is a Growing Concern

Cyberattacks on healthcare vendors have surged since the Change Healthcare attack in February 2024, with each attack impacting multiple providers or payors.



Clearwater

Third-Party Breach Statistics & Impact

Healthcare experiences more third-party data breaches than any other industry

41%

of all third-party breaches affected healthcare organizations[1]

77%

of all reported breached records originated from a business associate data breach[2]

$9.8M

Average cost of healthcare data breach, which is 2X the average of all industries[3]

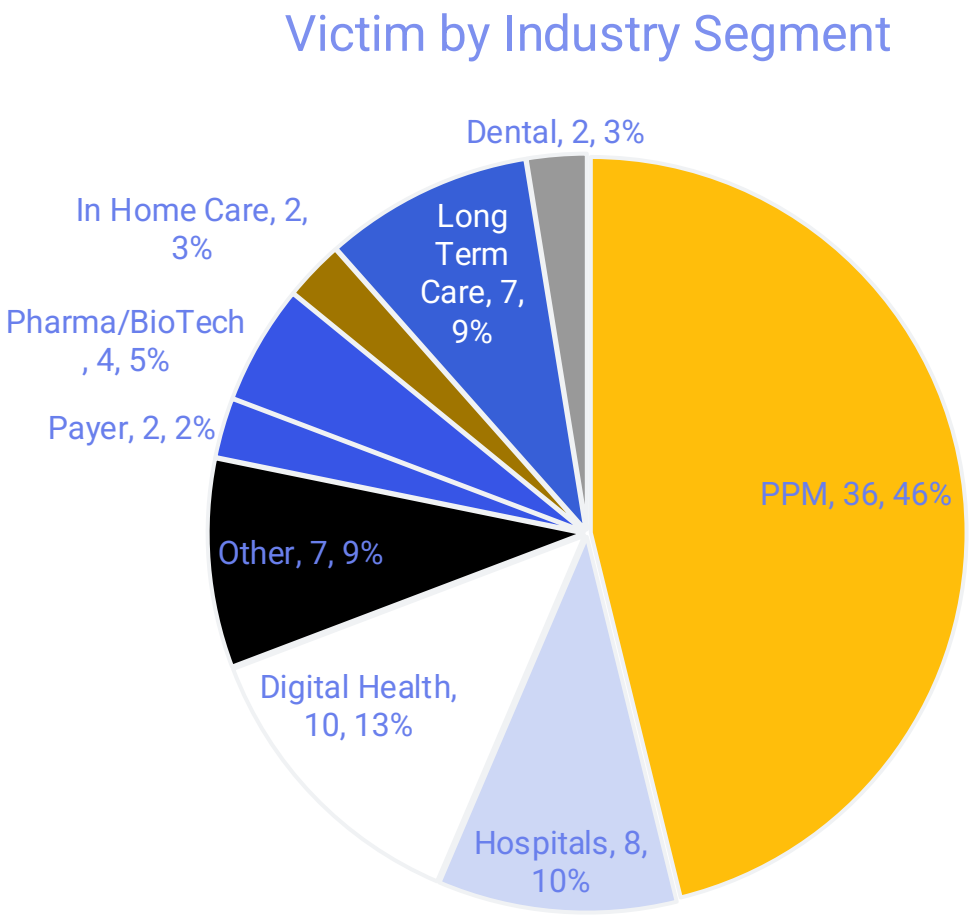
"Software vendors were among the most often targeted entities, accounting for one-quarter of breaches as hackers turned their attention to software supply chains."

-Black Kite 2025 Third-Party Breach Report

1 Black Kite's 2025 Third-Party Breach Report
2 Bluesight's 2025 Breach Barometer report
3 IBM's Cost of Data Breach Report 2024

Clearwater

Physician Practice Management Groups Have Been a Major Focus of Attacks



Source: Recorded Future Threat Intelligence

Between August and October of 2024, 46% of ransomware attacks on healthcare were conducted on PPMGs

Clearwater

Cyber Risk & Healthcare Investors

WSJ PRO

Deep-Pocketed Investors Make Startups a Target for Hackers

Despite risks, cybersecurity isn't always a primary focus of due diligence in funding deals, investors say

By *Angus Loten*

April 28, 2025 1:34 pm ET | WSJ PRO

"Investors have recognized that proactive engagement is among the best defenses against data breaches."

Derek Hernandez, senior emerging tech analyst at venture-capital research firm PitchBook

Clearwater's Benchmark Report on PE-Backed Healthcare Companies

About the Report

- Based on our work with private equity firms and their portfolio companies to identify vulnerabilities, assess cyber maturity, and drive measurable improvements before identified risks impact the bottom line
- Reflects assessed organizations across a diverse set of private equity-backed portfolio companies spanning all corners of the healthcare ecosystem
- Most of the companies evaluated fall within the middle-market category within their respective market segments

405(d) HICP: A Standard Framework for Assessing Healthcare Cybersecurity Practices

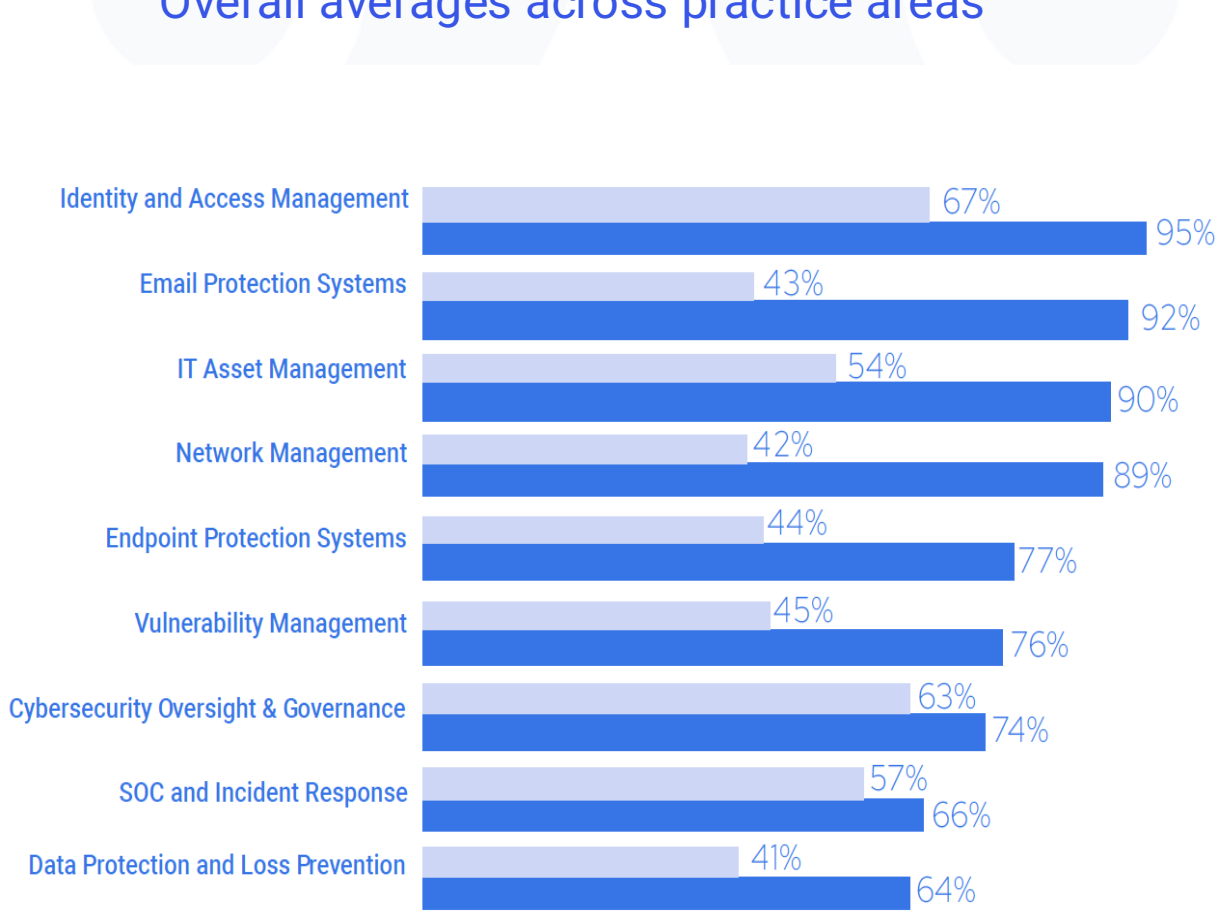
Why 405(d) works for private equity

- Practical, scalable, and designed for real-world implementation
- Federally recognized framework
- Simplified cyber risk management across segments of healthcare

HICP outlines ten key cybersecurity practices to mitigate the most pressing cyber threats in healthcare

Top Areas of Risk

- Lack a structured cybersecurity framework to guide program development
- High-level risk assessments that leave gaps
- No ongoing risk remediation effort
- Lack formalized incident response plans
- Weak data classification and handling policies



Recommendations for Strengthening Cybersecurity

Biosciences, CRO, CDMO, and R&D Companies

Research, development, manufacturing, and go-to-market consulting services for pharmaceuticals, biotech, and medical device organizations.

- Start by deploying strong data classification and handling standards
- Then align with technical tools and controls to safeguard sensitive information

Consumer Health Businesses

Businesses that focus on providing direct to consumer wellness services or products.

- Establish or strengthen policies and procedures
- Formalize and test incident response plans through tabletop exercises

Dental Service Organizations

These are organizations providing dental care or innovation in the field of oral healthcare.

- Prioritize cyber risk assessments as part of M&A due diligence
- Implement network segmentation across locations

Recommendations for Strengthening Cybersecurity

Healthcare Software, Analytics, and Business Services

Businesses services, specialized software, and analytics platforms supporting healthcare providers.

Pharmaceutical Companies

These include manufacturing and organizations that drive innovation in the supply components for pharmaceutical businesses.

Physician and Specialty Practice Clinics

Small to large practice groups that provide healthcare services or specialized healthcare.

- Invest in endpoint protection systems and managed services
- Prioritize strong data management and classification practices to minimize potential for accidental or malicious data loss

- Leverage a Managed Security Services Provider (MSSP) to deliver a secure cloud-based operating environment
- An MSSP can also help strengthen overall vulnerability management and incident response

- Consider vCISO services to expedite executive-level direction to improve cybersecurity oversight and governance
- Minimize potential for patient care disruption by strong adoption of SOC and Incident Response practices

Q&A

Upcoming Webinars & Events

Monthly Cyber Briefing Webinar | June 5 | 12:00 CT

- Our review of the latest cyber threats and regulatory development impacting healthcare organizations
- Special deep dive into the malicious use of AI by threat actors
- Click here to register

Leading With Responsible AI | June 23-25 | 11:00-1:45 CT

- Three-day virtual event featuring leading experts sharing insights and practical guidance on how to drive the responsible use of AI in healthcare
- Topics include governance, regulatory developments, compliance, risk management, and cybersecurity
- Click here to register

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.