Monthly Cyber Briefing

May 1, 2025

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Agenda

- Cyber & Regulatory Update
- Alliance Agenda: A Discussion on HSCC's Vision for Advancing Healthcare Cybersecurity
- Q+A

Greg Garcia

Executive Director
Healthcare & Public Health Sector Coordinating Council Cybersecurity Working Group

Lisa Munro

Director, Healthcare Marketing
Clearwater

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

Chief Executive Officer
Clearwater

Clearwater

Cyber & Regulatory Update

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

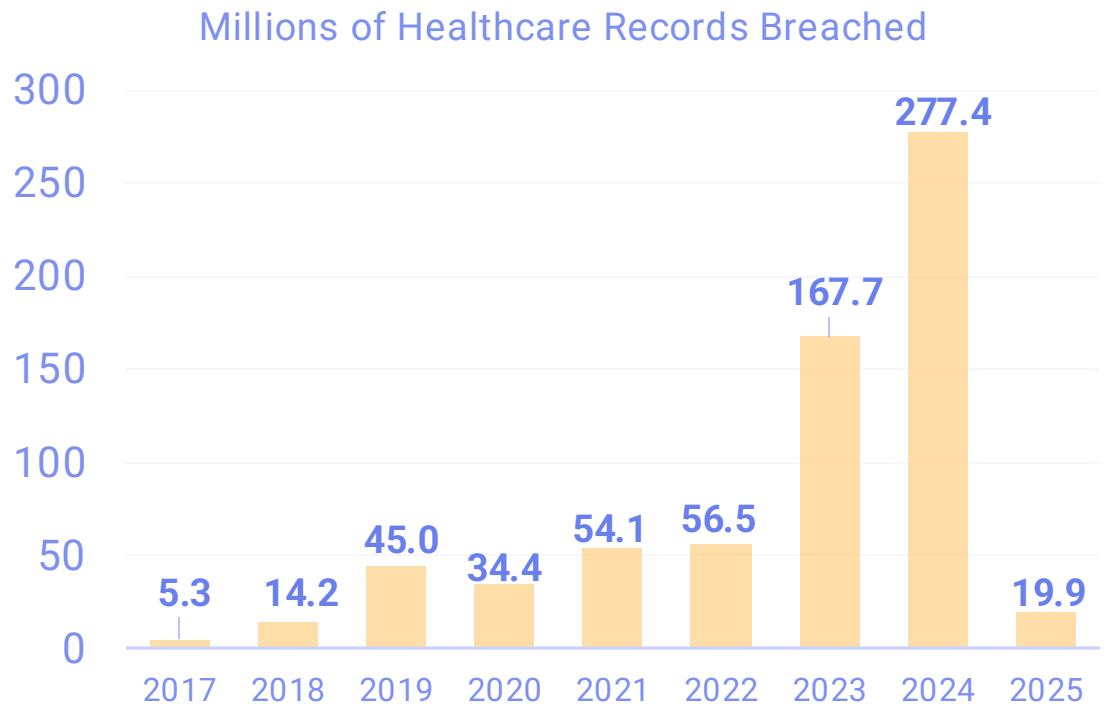
CEO, Clearwater

Clearwater

Breach Reports via OCR Breach Portal

OCR Breach Portal Data[1]

- 2024 breach data: 277.4M records from 734 breaches
- YTD 2025 breach data: 19.9M individuals from 218 breaches - 14.2M records reported in past month



Three major breaches reported since last briefing in April

- Frederick Health: 934K records stemming from January 2025 ransomware attack
- Blue Shield of California: 4.7M records from Google Analytics ad platform – exposed April 2021 – April 2024
- Yale New Haven Health System reported a massive data breach affecting 5.5 million patients

Clearwater

1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 4/28/25, pulled 4/28/25)

UPDATED FROM MARCH BRIEFING

Alleged Oracle Cloud Infrastructure (OCI) Breach

Threat actor claimed hack of ~6 million lines of data from Oracle Cloud's SSO and LDAP.

- If cracked, stolen encrypted SSO and LDAP passwords could enable further Oracle Cloud breaches
- Hack supposedly includes JKS files, encrypted SSO passwords, key files, and enterprise manager JPS keys
- The threat actor claimed to have compromised the subdomain login.us2.oraclecloud
- Research firms validated Oracle fusion middleware had a critical vulnerability CVE-2021-35587
- Oracle denied the breach even though clients confirmed it

UPDATE

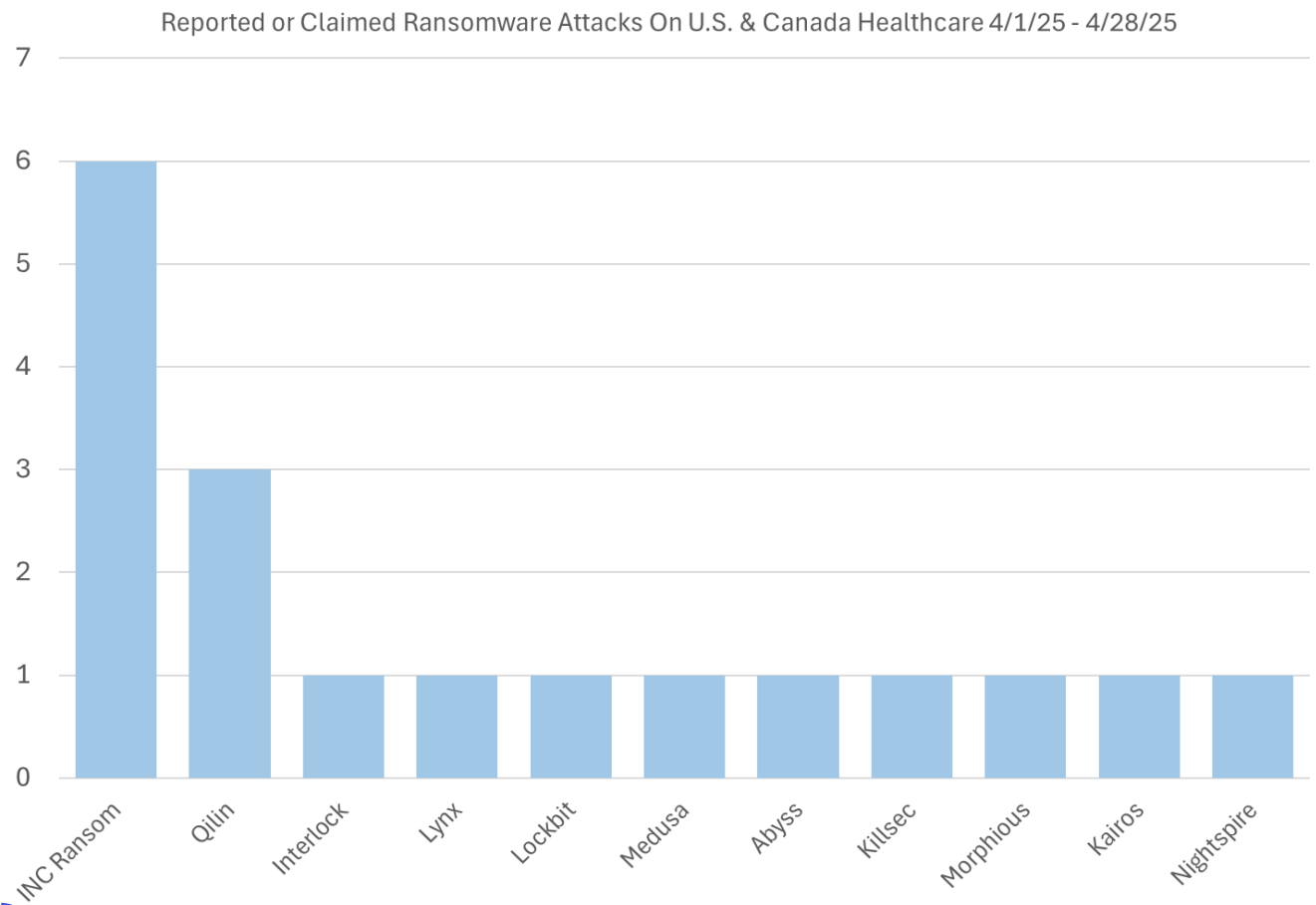
- Oracle's lack of transparency was criticized, especially following another breach of Cerner data
- Oracle eventually admitted there was a breach of "legacy" servers (in the cloud)
- CISA issued advisory with mitigation recommendations

Clearwater

Link to CISA Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise | CISA

Ransomware Attacks on Healthcare in April

18 identified data leaks from ransomware attacks on U.S. & Canada Healthcare organizations 4/1/25 – 4/28/25



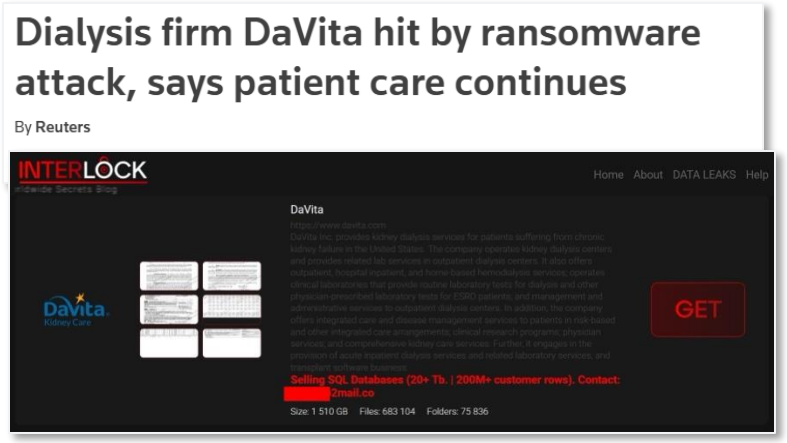
- Inc. Ransom has become one of the top Ransomware gangs targeting Healthcare. Notable recent attacks include the Loretto Hospital, Glengarry Memorial Hospital, and various specialty care practice groups.
- It's been reported that RansomHub has gone dark. Potentially rebranded as Lynx.
- Qilin might be gaining RansomHub's affiliate network. Qilin's recent healthcare attacks include The Galveston County Health District and Coastal Carolina Health Care Primary Care.
- DaVita attack claimed by Interlock – see next slide.

Clearwater

Source: Ransomware.live - Last ransom claims

DaVita Attacked by Interlock Ransomware

Also refer to February 2025 Cyber Briefing where we warned of Interlock targeting treatment and community centers and discussed TTPs



- Ransomware attack discovered 4/12/25
- 2,600 dialysis centers and serves around 200,000 patients through about 760 hospitals
- Encrypted systems, forcing DaVita to operate on back-up procedures
- Interlock listed 1.5TB of data for sale

- Lures victims to a fake website, which executes download scripts
- Typically made to look like Google Chrome, MS Edge, or MS Teams updaters that installs remote access tools
- Moves laterally using native tools
- Employs double extortion

Clearwater

Elenor-corp & Mimc 7.5 – New Threat Actor Targeting HC

Security Firm Morphisec a new ransomware strain known as ELENOR-corp, identified as version 7.5 of the Mimic ransomware

Link to Technical analysis of ELENOR-corp Ransomware: Mimic Ransomware Variant

Advanced capabilities, including data exfiltration, persistent access and anti-forensic strategies designed to cripple recovery efforts and maximize damage.

- Deploys Clipper credential harvesting software pre-ransomware payload deployment
- Employs aggressive evidence tampering to limit forensic recovery
- Enables parallel sessions of RDP overriding restrictions on multiple logins
- Modifies power settings to speed up encryption
- Deletes windows back-up and recycle bin

Epic Data Breach

An increase in social engineering campaigns at hospitals in recent weeks resulted in numerous compromised MyChart accounts

CHIME
DIGITAL HEALTH LEADERS

Dear Members,

We want to make you aware of a recent surge in impersonation attacks targeting hospital and health system help desks. Bad actors are calling in and fraudulently requesting account access changes, such as password resets — posing a significant risk to system security and patient privacy.

Several organizations have reported a high volume of these incidents. While these types of social engineering attempts are unfortunately common, the current pattern represents a coordinated uptick in activity.

We encourage all CHIME members — regardless of platform — to remain on alert. Reinforce your internal protocols, educate frontline IT staff, and connect with your platform contacts if you suspect any unusual behavior.

CHIME will continue to share relevant updates and serve as a trusted resource in times of elevated threat. Together, we can strengthen awareness and resilience across the digital health ecosystem.

Blessings,

- A few weeks ago, multiple hospitals said they had been contacted by Epic regarding user compromised credentials
- Hackers were calling help desks and changing the MyChart password for patients and taking over accounts
- Once the malicious actor is in one hospital patient's MyChart then request all info in MyChart across all organizations
- Epic has said it has limited ability to track access across multiple organizations
- CHiME issued an alert on 4/11/25

Clearwater

HHS OCR Regulatory Enforcement Update

Despite office closures and layoffs at HHS, regulatory HIPAA enforcement action continues with focus on Risk Analysis Initiative

3 HIPAA Security Rule (Settlement) Enforcement Actions in April

- Public Hospital: Guam Memorial Hospital Authority on 4/17/25 - $25,000
- Large Health System: PIH Health, on 4/23/25 - $600,000
- Small provider: Comprehensive Neurology, PC on 4/25/25 - $25,000

"OCR urges health care entities to prioritize compliance with the HIPAA Security Rule risk analysis requirement."

-OCR Acting Director Anthony Archeval

Key Reasons Regulated Entities Fail Risk Analysis Requirement

- Not done at information system component level
- Does not include all information systems with ePHI
- Does not follow OCR's Final Guidance on Risk Analysis (Must meet all 9 elements)
- Not current and/or not updated when changes occur

Link to OCR's Final Guidance on Risk Analysis

Link to Differences Between HIPAA Security Evaluations and Risk Analysis - Clearwater

Recommendations

Addressing specific TTPs in current threat environment

- Maintain continuous vulnerability scanning, and patch critical and high vulnerabilities with extreme priority
- Update Security Awareness training to be in line with current techniques
- For Oracle Cloud: Reset passwords for any known affected users across enterprise services
- Enforce phishing-resistant multi-factor authentication (MFA) consistently including internal applications
- Prioritize review of access privileges and restrict access to minimum necessary to perform job function
- Ensure monitoring and detection for latest TTPs including evidence tampering
- Update your risk analysis or employ a more rigorous methodology if it currently does not meet OCR and/or NIST Guidelines
- Review incident response procedures and exercise them on a regular basis – adjust based on learnings

Alliance Agenda

A Discussion on HSCC’s Vision for Advancing Healthcare Cybersecurity

Fireside Chat

- A Discussion on HSCC's Vision for Advancing Healthcare Cybersecurity

Greg Garcia

Executive Director

Healthcare & Public Health Sector Coordinating Council Cybersecurity Working Group

Lisa Munro

Director, Healthcare Marketing

Clearwater

Resources

- HSCC Greg Garcia Testimony
- HSCC Statement on Healthcare Cybersecurity Policy
- HSCC 2025 Policy Statement
- HSCC Recommendations for Government Policy & Programs

Clearwater

Q&A

Upcoming Webinars

Rural Critical Access Connect: AI Overload | May 22 | 12pm – 1pm CT

- Rural and critical access hospitals face a unique set of cybersecurity challenges—limited staff, aging infrastructure, constrained budgets, and no shortage of risk.
- **Clearwater's Rural Critical Access Connect** is your quarterly opportunity to connect, learn, and lead alongside professionals who understand exactly what you're up against.
- Register for the quarterly sessions here

Cyber Risk Benchmark Report on Healthcare PE-Backed Portfolio Companies | June 4 | 12pm – 1pm CT

- Clearwater's recently published Cyber Risk Benchmark Trend Report for Healthcare Private Equity reveal systemic gaps in cybersecurity preparedness. These findings highlight critical risks that could impact financial stability, regulatory compliance, and operational resilience for private equity-backed companies.
- Join us on June 4 as we review key take-aways from our report and share insight on the path to improvement.
- Register here

Monthly Cyber Briefing June 5 | 12pm – 1pm CT

- You are already registered and will automatically be enrolled in next month's briefing.

Clearwater

Upcoming Events

McDermott HealthEx | May 6-9, 2025 | Nashville, TN

- Clearwater is proud to be a Patron-Level Sponsor. We will have a meeting table – come meet with our team!
- Jon Moore speaking on May 5th during the Hospitals & Health Systems Pre-Conference

- Click here to register & see our session details

McGuireWoods Healthcare Private Equity & Finance Conference | May 14–15 | Chicago, IL

- Meet our **Private Equity and PPMG team members**, **Richmond Donnelly** and **David Kolb**, to learn how Clearwater helps organizations reduce cyber risk, meet regulatory demands, and protect business value before, during, and after a deal.

- Click here to register & book a meeting with us

Polsinelli Healthcare Dealmakers Conference | May 21–22 | Dallas, TX

- Be sure to connect with our attending team members:
  - Baxter Lee, Chief Financial Officer
  - David Kolb, Vice President, Sales – PPMG
  - Richmond Donnelly, Senior Account Executive, Private Equity

- Click here to register & book a meeting with us

Clearwater

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.