Healthcare's Cyber Briefing

January 8, 2026

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.

Clearwater

Healthcare's Cyber Briefing

CRITICAL THREAT BRIEF FOLLOWED BY

2026 HEALTHCARE CYBER AND REGULATORY OUTLOOK WITH SPECIAL GUEST GREG GARCIA

FEATURING:

David Bailey VP, Consulting Solutions & Strategy

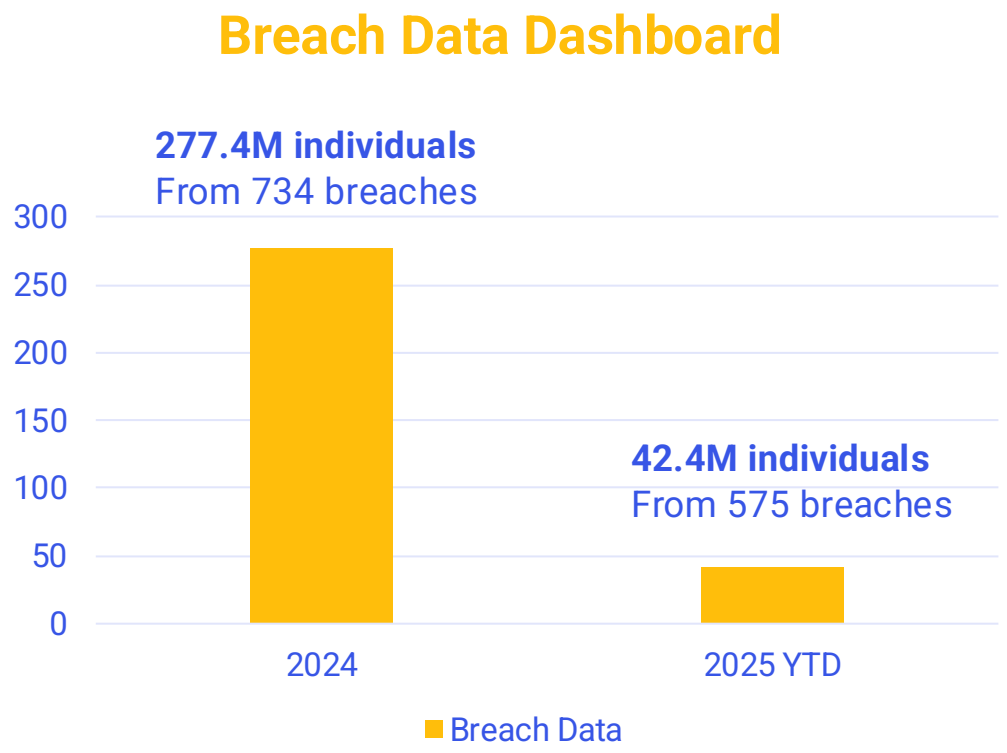
Greg Garcia Executive Director
Health Sector Coordinating Council

Breach Portal Updates

Dave Bailey, VP Consulting Solutions & Strategy

Clearwater

15 Breaches Added in Dec



1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 12/31/25, pulled 1/5/26)

Clearwater

Largest Breaches of 2025

- **Aflac** – Health Plan – **26.5M***
- **Conduent Business Services** - BA – **10.5M**
- **Yale New Haven HS** – Provider – **5.6M**
- **Episource, LLC** – BA – **5.4M**
- **Blue Shield of California** – BA – **4.7M**
- **DaVita Inc.** – Provider – **2.7M**
- **Anne Arundel Dermatology** – Provider – **1.9M**
- **Radiology Associates of Richmond** – Provider – **1.4M**
- **Lockton** – BA – **1.1M**
- **Community Health Center** – Provider – **1M**
- **Frederick Health** – Provider – **934K**
- **McLaren Health** – Provider – **743K**
- **Medusind Inc** – BA – **701K**
- **Kelly & Associates Insurance Group** – BA – **553K**
- **Numotion** – Provider - **529K**
- **Oracle Health** – BA – **Unknown**

Healthcare Industry Threat Information

Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

CISA publishes multiple Industrial Control System Medical Advisories impacting the healthcare sector

Mirion Medical EC2 Software NMIS Bios – 12/2

- **Vulnerabilities**: Incorrect Permission Assignment for Critical Resource, Use of Client-Side Authentication, Use of Hard-coded Credentials
- Successful exploitation of these vulnerabilities could allow an attacker to modify program executables, gain access to sensitive information, gain unauthorized access to the application, and execute arbitrary code

Grassroots DICOM (GDCM) –12/11

- **Vulnerabilities**: Out-of-bounds Write
- Successful exploitation of this vulnerability could allow an attacker to craft a malicious DICOM file and, if opened, could crash the application resulting in a denial-of-service condition

Varex Imaging Panoramic Dental Imaging Software –12/11

- **Vulnerabilities**: Uncontrolled Search Path Element
- Successful exploitation of this vulnerability could allow a standard user to obtain NT Authority/SYSTEM privileges

AI made scams more convincing in 2025

Google Threat Intelligence

Voice cloning	• One of the main areas where AI improved was around voice-cloning, which was immediately picked up by scammers. In the past, they would mostly stick to impersonating friends and relatives. In 2025, they went as far as impersonating senior US officials . The targets were predominantly current or former US federal or state government officials and their contacts.
AI Agents	• Agentic AI is the term used for individualized AI agents designed to carry out tasks autonomously. One such task could be to search for publicly available or stolen information about an individual and use that information to compose a very convincing phishing lure.
Social media	• Combining data posted on social media with data stolen during breaches is a common tactic. Such freely provided data is also a rich harvesting ground for romance scams , sextortion , and holiday scams
Prompt Injection	• Researchers and criminals alike are still exploring ways to bypass the safeguards intended to limit misuse. • Prompt injection is the general term for when someone inserts carefully crafted input, in the form of an ordinary conversation or data, to nudge or force an AI into doing something it wasn't meant to do.
Malware Campaigns	• Attackers have used AI platforms to write and spread malware . Researchers have documented campaign where attackers leveraged Claude AI to automate the entire attack lifecycle, from initial system compromise through to ransom note generation, targeting sectors such as government, healthcare, and emergency services.

Looking toward 2026, the biggest shift may not be technical but psychological. As AI-generated content becomes harder to distinguish from the real thing, verifying voices, messages, and identities will matter more than ever.

Ransomware Update

Impacts from Ransomware in December

Google Threat Intelligence

Clearwater

December ransomware activity lead by Qilin with 6 reported victims on their data leak site

December ransomware activity shows **high operational intensity**, **actor diversification**, and a **continued focus on outpatient medical organizations**

33

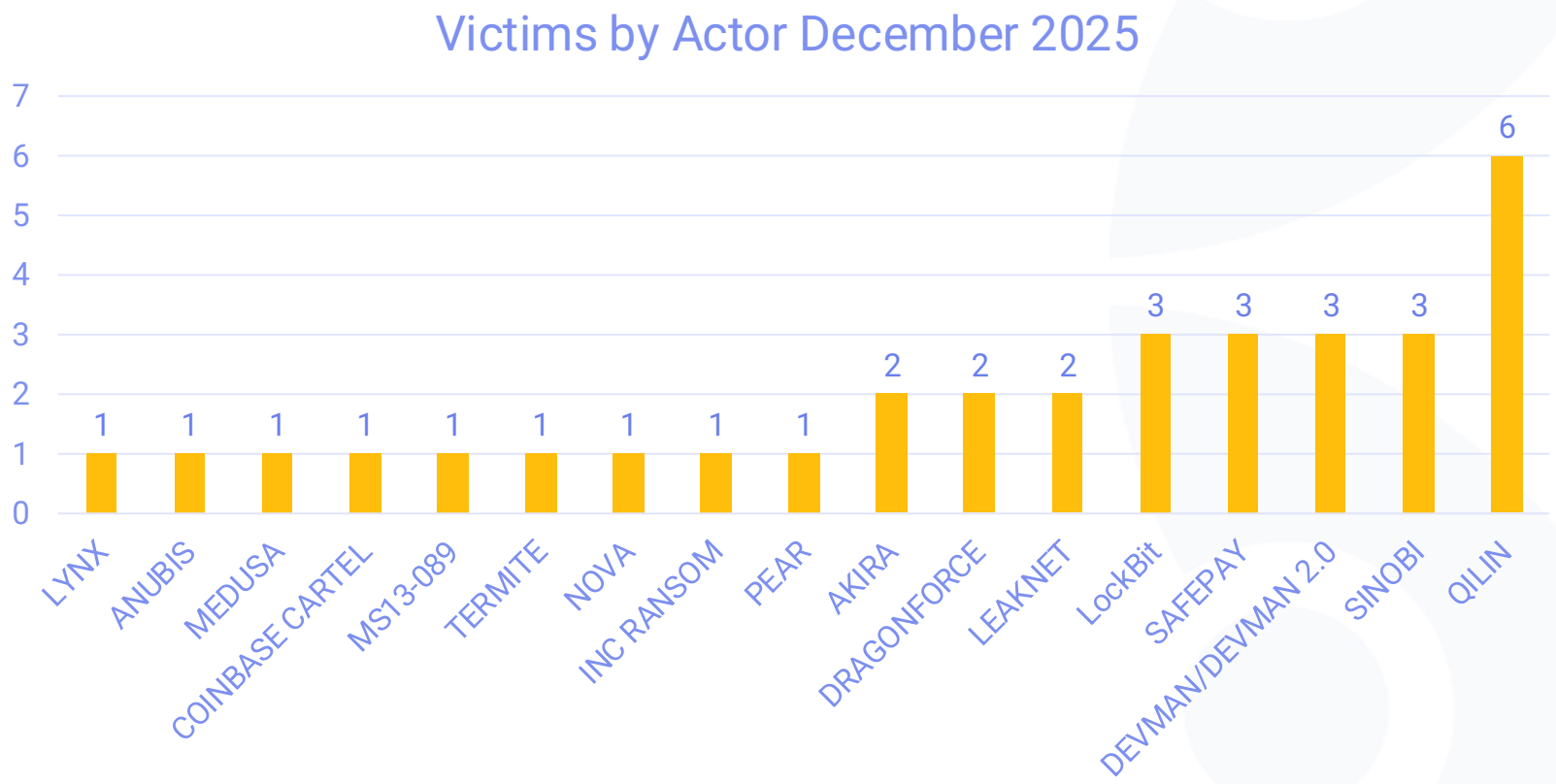
December concluded with **33** reported ransomware incidents against the U.S. healthcare sector across **hospitals, medical practices, pharmacies, and dental offices.**

55%

Key ransomware operators—**Qilin, SafePay, Sinobi**, **Devman**, and **LockBit** —accounted for **55%** of total activity, underscoring sustained, coordinated targeting of healthcare networks and patient information systems.

Qilin continues clustered timeline of victims

December shows fragmentation across many threat actors but a clear leader in Qilin



Industry Focus:

- **Medical Practice Focus**: Increase in attacks on mid-size organizations and other healthcare business
- **Dominance in Data Exfiltration**: Data theft is a critical component with many groups abandoning encryption
- **Geographic Concentration**: The U.S. remains the country with the highest number of ransomware attacks on healthcare orgs

Qilin and Inc Ransomware are #1 and #2 in reported victims in U.S. Healthcare

Qilin

- The Qilin ransomware group, active since at least August 2022, operates a ransomware-as-a-service (RaaS) model, employing **double extortion tactics**: The ransomware used is known as “Agenda”
- Recently enhanced its offerings to affiliates, introducing a "Call Lawyer" feature in early May 2025
- Introduced a distributed denial-of-service (DDoS) capability in April 2025. Other planned features include a DDoS panel, an email spamming tool, a call/SMS spamming tool/service, and the involvement of journalists.
- Initial access is typically gained through leaked credentials via a virtual private network (VPN), followed by the deployment of tools like Cobalt Strike and Mimikatz for persistence and further credential theft

Inc Ransomware

- INC Ransomware, also identified as GOLD IONIC , is a highly active and prominent ransomware and data extortion group.
- Operating under a ransomware-as-a-service (RaaS) model, INC Ransomware has been active since July 2023 .
- The group employs a "double extortion" strategy, involving both data encryption and exfiltration, with threats to leak stolen data to pressure victims into paying the ransom
- The malware family associated with this threat actor is known as "INC" . Functionally identical variants operate under different branding, including LYNX and SINOBI . There are theories that INC Ransom may have rebranded as Lynx, sold its source code, or experienced an internal split, as both groups remain active

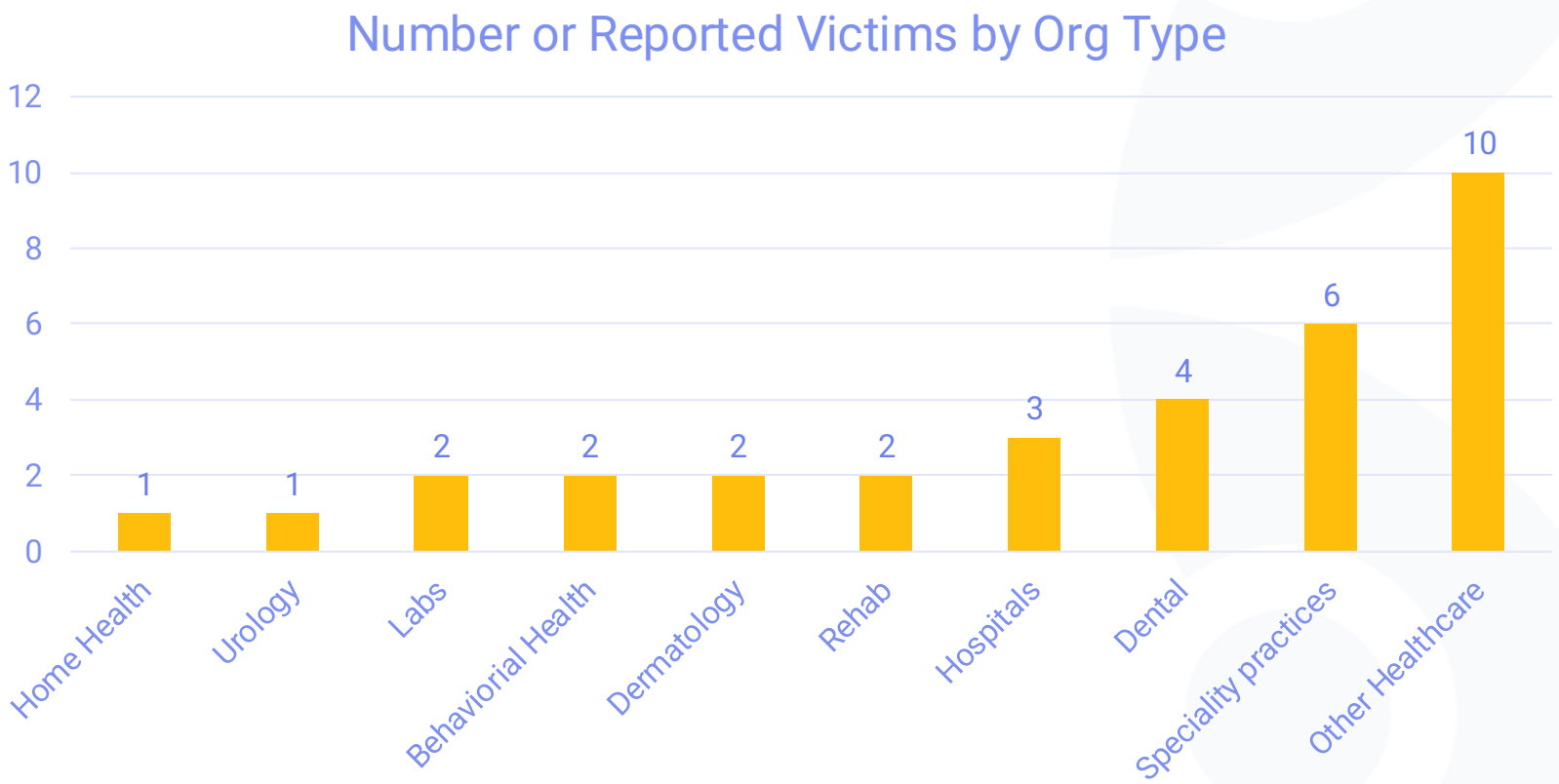
Ransomware Targeting Patterns

Impacts from Ransomware in December

Google Threat Intelligence

Clearwater

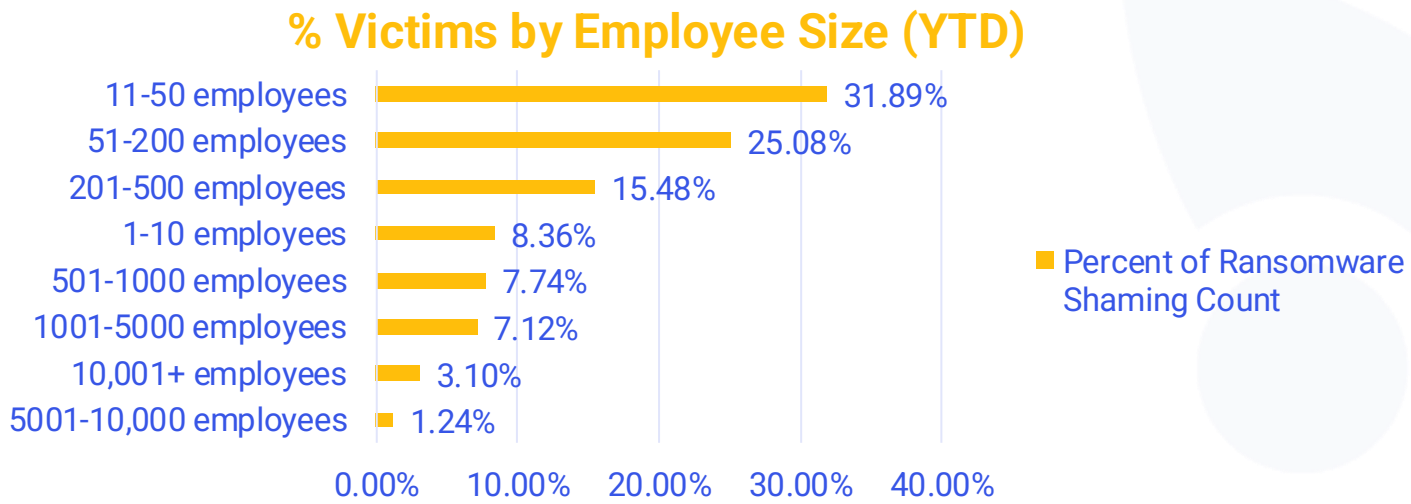
December victims skew toward **mid-market provider organizations** (specialty + outpatient + clinics)



Industry Focus:

- Several victims are narrow-specialty medical (urology, ENT/allergy, dermatology, ortho): high operational urgency, sensitive data, and varied IT maturity
- December had an expected mid month and end-of-month spike, which aligns with holiday staffing gaps and slower response cycles

Healthcare was plagued by ransomware in 2025



2025
354 Victims
62 Threat Actors

Clearwater

Google Threat Intelligence

Sector Updates

HHS Focus on Cybersecurity

Google Threat Intelligence

Clearwater

Healthcare Cybersecurity and Resiliency Act of 2025 seeks to **improve cybersecurity readiness, resilience, and incident response**

Federal Agency Coordination	• Requires the Secretary of Health and Human Services **(HHS)** and the Director of the Cybersecurity and Infrastructure Security Agency **(CISA) to coordinate on cybersecurity efforts** for the HPH sector
Clarifying Roles & Oversight	• Establishes that **HHS (through ASPR) will lead oversight** of internal cybersecurity activities and coordinate with CISA and other public/private entities for preparedness and response
Cybersecurity Incident Response Plan	• **Within 1 year** of enactment, HHS must develop and implement a **comprehensive cybersecurity incident response plan**
Enhanced Breach Reporting	• Adds requirement to report number of individuals affected by breaches. • **Mandates public reporting of corrective actions taken** and consideration of recognized security practices via the OCR breach portal
Recognition of Security Practices	• Encourages **adoption of robust controls** (e.g., MFA, encryption, audits) that align with modern frameworks
Rural Provider Guidance	• Directs HHS to issue **tailored cybersecurity guidance for rural healthcare providers**, addressing breach prevention, resilience, and coordination with federal agencies
Grants for Cybersecurity	• Allows HHS to award **grants** to eligible entities (e.g., hospitals, rural clinics, cancer centers) to adopt cybersecurity best practices
Workforce Development	• Calls for **training health sector personnel** on cybersecurity risks, defensive practices, and preparedness through coordination with CISA State Coordinators and private sector experts

Recommended Actions for Healthcare Organizations

Focus Area	Actions
Strengthen Access & Identity Controls	▪ Enforce MFA on all accounts, especially remote access, VPNs, RDP and admin ▪ Limit external remote access to minimum necessary; strong RBAC ▪ Monitor & restrict third-party/vendor access
Vulnerability Management & Patch Hygiene	▪ Maintain a robust vulnerability management program ▪ Prioritize patching ▪ Ensure secure configuration of devices and hardening
Backup, Disaster Recovery & Resilience	▪ Maintain immutable, offline, air-gapped backups ▪ Regularly test backup restorations (table-top and live tests) ▪ Maintain an incident response plan for ransomware
Detection & Monitoring	▪ Deploy advanced endpoint detection & response (EDR) ▪ Have continuous monitoring of events ▪ Use threat intelligence to monitor for TTPs
Network Architecture & Segmentation	▪ Segment critical clinical networks ▪ Harden and monitor network boundaries ▪ Logically isolate backups
Vendor & Third-Party Risk Management	▪ Assess cybersecurity posture of vendors, MSPs, medical-device suppliers ▪ Require vendor access to be tightly controlled ▪ Include in contracts obligations for incident reporting, security reqs, and audits

Healthcare's Cyber Briefing

2026 HEALTHCARE CYBER AND REGULATORY OUTLOOK WITH SPECIAL GUEST GREG GARCIA

FEATURING:

David Bailey VP of Consulting Services & Strategy

Greg Garcia Executive Director
Health Sector Coordinating Council

HSCC Resources

Model Contract-Language for MedTech

updated reference for shared cooperation and coordination between Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) regarding the security, compliance, management, operation, and services of medical technology in the clinical environment.

Health Sector Coordinating Council
Cybersecurity Working Group

AI Cybersecurity Guidance

White papers that the Cybersecurity Working Group will publish in 2026 about A.I.: 1) Education and Enablement; 2) Cyber Operations and Defense; 3) Governance; 4) Secure by Design; and 5) Third Party Risk and Supply Chain Transparency. In addition, the first of our foundational publications on Education and Enablement is included herein on page 7, “A.I. in Healthcare: 10 Terms You Need to Know.”

Q&A

Clearwater

Upcoming Webinars

2026 Healthcare Cyber & Compliance Exchange (Virtual)

A half-day virtual briefing for healthcare security and compliance leaders navigating rising threats, shifting regulations, and the coming updates to the HIPAA Security Rule.

Read More ›

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

We invite you to attend our free, virtual monthly Cyber Briefing. During each hour-long, dynamic, educational session an industry expert will draw on their previous experience to cover several key topics & trending news related to healthcare privacy, cybersecurity, IT audit, & compliance.

Register Now ›

Upcoming Events

Founders + Funders Networking Event | January 13, 2026 | San Franciso, CA

Clearwater is a proud sponsor of StartUp Health's Founders & Funders Networking Summit, co-hosted with SVB during JPM Healthcare Week on January 13th from 4–8 PM PST in San Francisco.

Read More ›

ViVE | Feburary 22-25, 2026 | Los Angeles, CA

Clearwater is honored to return to ViVE 2026 as the Premier Sponsor of the Cybersecurity Zone.

Read More ›

HIMSS 2026 | March 9–12, 2026 | Las Vegas, NV

Schedule a one-on-one meeting with the Clearwater team during HIMSS 2026 to discuss your priorities, answer questions, and explore how we can support your organization.

Read More ›

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.