

Monthly Cyber Briefing

February 6, 2025

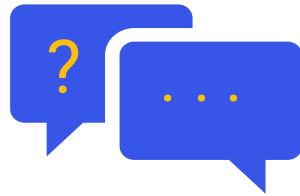


Meeting Logistics



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 & Speakers

- Cyber & Regulatory Update
- The Return of OCR Audits: What It Means and How to Prepare for Potential Action
- Q+A



Andrew Mahler
Speaker

Vice President, Consulting
Services, Privacy & Compliance
Clearwater



Iliana L. Peters
Speaker

Shareholder, **Polsinelli** & Former
Acting Deputy Director
HHS Office for Civil Rights



Steve Cagle
Speaker

Chief Executive Officer
Clearwater

Cyber & Regulatory Update

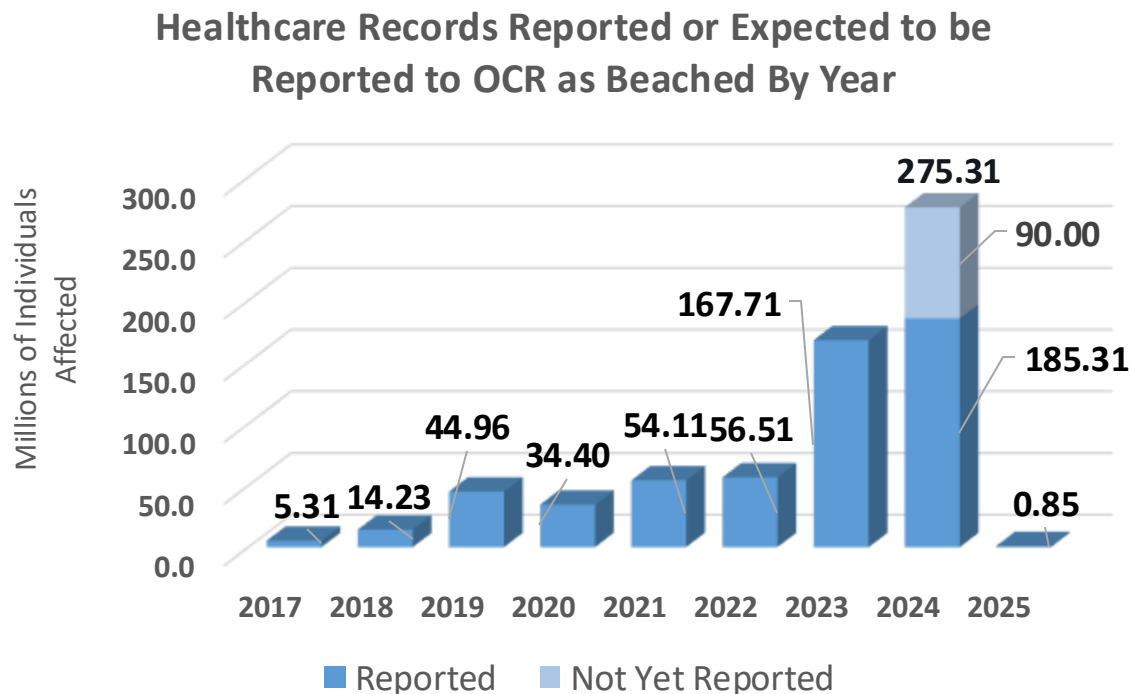
Steve Cagle



Breach Reports via OCR Breach Portal

OCR Breach Portal Data¹

- 2024 breach data updated to 185.31 individuals from 726 breaches
- 2025 – 850K individuals reported from 56 breaches, with 23 being related to each other



- Change Healthcare Breach Update
 - 2024 includes 100m records reported as breached by Change Healthcare
 - Change Healthcare announced recently they believe an additional 90m individuals were affected
 - Over \$3.1B in costs, exceeding updated estimates²
- Largest breach reported in January was Asheville Eye Associates resulting from ransomware attack claimed by DragonForce³
- Connecticut Community Health Center disclosed a data breach of 1M records to Maine SAG⁴

¹ The [HHS Breach Portal](#) (2024 data through 12/31/24, pulled on 2/1/25; 2025 data through 1/24/25 pulled 2/1/25)

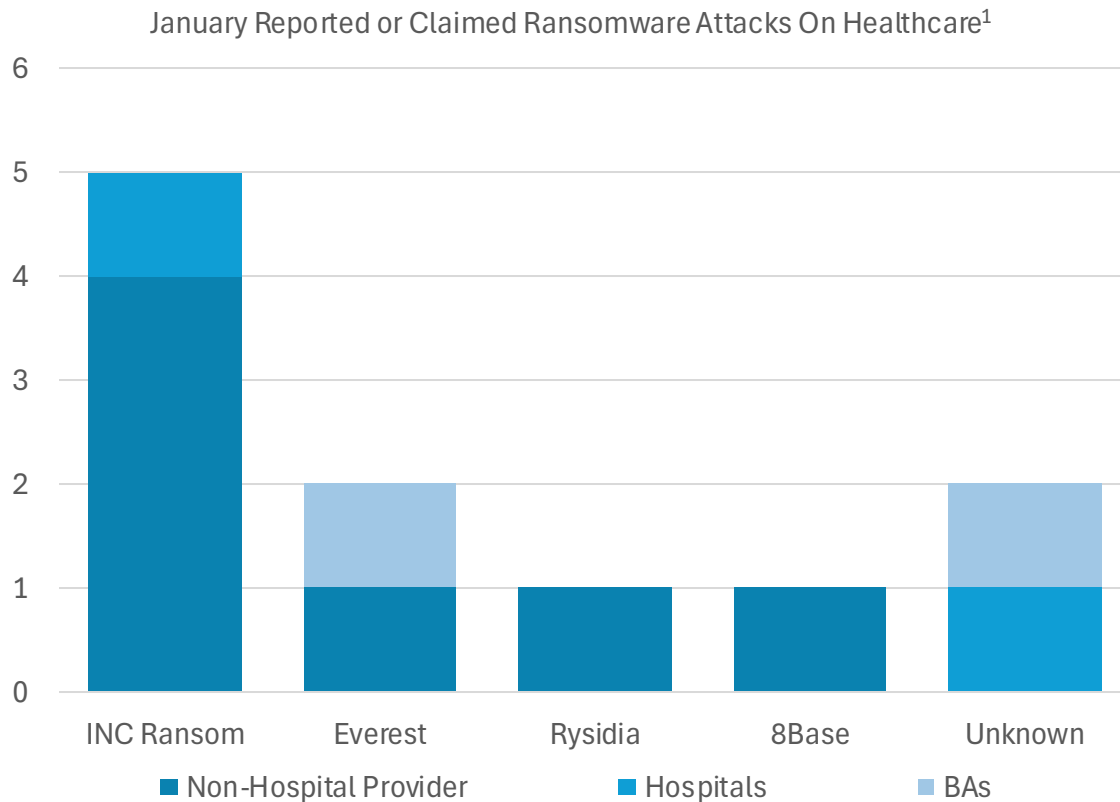
² [UnitedHealth reaches record revenue in 2024, though profit falls | Healthcare Dive](#)

³ [Asheville Eye Associates Data Breach Lawsuit - Sign Up Today](#)

⁴ [Medical Records Stolen As 1 Million Patients Hit By Healthcare Hack](#)

Ransomware Attacks – January 2025

In January ransomware gangs successfully executed many attacks in U.S. Healthcare with strong targeting of ambulatory/specialty providers. INC Ransom continuing to be very active.



- At least 11 ransomware attacks on the healthcare space identified¹
- Frederick Health Hospital of Maryland attacked 1/27; treating patients but diverting emergency cases² – Spillover causing strains on other hospitals³
- NY Blood Center attack week of 1/27 compounding impact from existing blood shortage emergency⁴
- New data: Of 402 surveyed healthcare organizations, 67% said they had experienced a ransomware attack in the past 12 months, up from 60% the previous year and 37% took more than a month to recover⁴

¹ Data compiled from multiple sources, including Halycon Ransomware Research and Published Media Reports

² [Notice | Frederick Health](#)

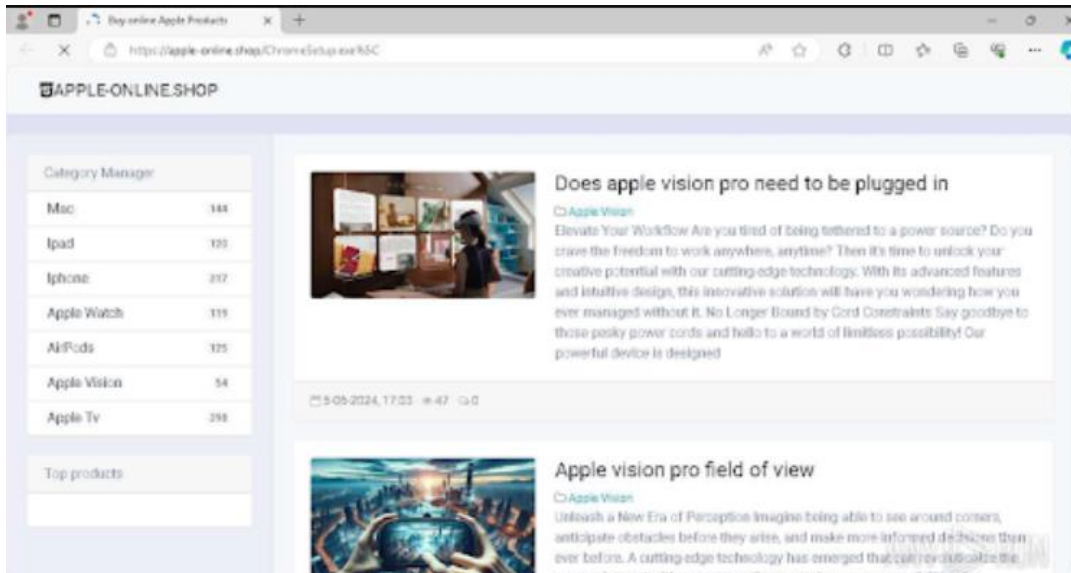
³ [Meritus Medical Center dealing with increased patient load](#)

⁴ [New York Blood Center Enterprises Cybersecurity Incident Update- New York Blood Center Enterprises](#)

⁵ [Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Sophos Survey Finds | Sophos](#)

Rising Threat Actor: Interlock Ransomware

Interlock Ransomware is a relatively new threat actor targeting healthcare, using double extortion techniques, potentially linked to the Rhysida gang. TTPs noted to be evolving since November.



The malicious website used by Interlock

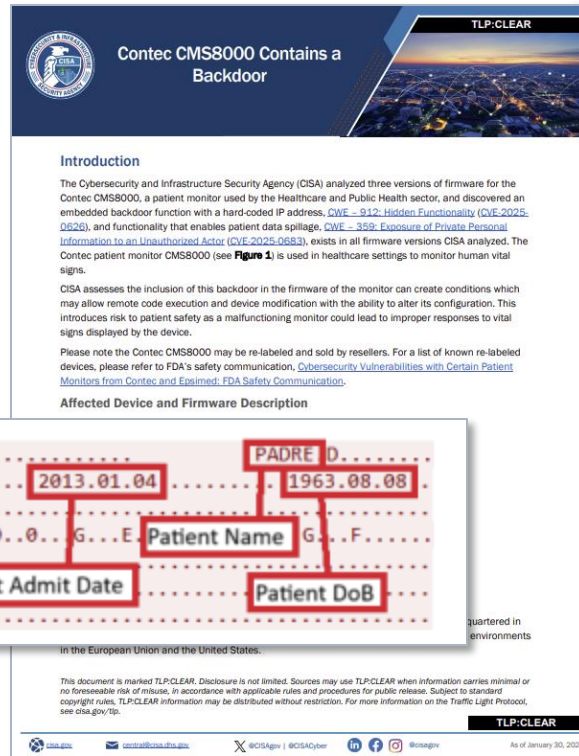
- Tricks victims by luring them to a fake website, which executes download scripts
- Fake updater installs a remote access tool disguised as a legitimate update
- This RAT establishes a secure C2 connection and installs a credential-stealing component
- Evades detection by disabling Endpoint Detection and Response and clearing event logs
- Moves laterally using legitimate tools, e.g., Anydesk, RDP
- Exfiltrates data using cloud storage services

CISA & FDA Alert Backdoor on Contec CMS8000 (also rebranded to Epsimed MN-120) Monitors

Functionality that enables patient data spillage for Contec CMS8000, which can create conditions which may allow remote code execution and device modification with the ability to alter its configuration



Figure 1: Contec CMS8000



Contec CMS8000 Contains a Backdoor

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) analyzed three versions of firmware for the Contec CMS8000, a patient monitor used by the Healthcare and Public Health sector, and discovered an embedded backdoor function with a hard-coded IP address, CVE-912:Hidden Functionality (CVE-2025-0526), and functionality that enables patient data spillage, CVE-359:Exposure of Private Personal Information to an Unauthorized Actor (CVE-2025-0683), exists in all firmware versions CISA analyzed. The Contec patient monitor CMS8000 (see Figure 1) is used in healthcare settings to monitor human vital signs.

CISA assesses the inclusion of this backdoor in the firmware of the monitor can create conditions which may allow remote code execution and device modification with the ability to alter its configuration. This introduces risk to patient safety as a malfunctioning monitor could lead to improper responses to vital signs displayed by the device.

Please note the Contec CMS8000 may be re-labeled and sold by resellers. For a list of known re-labeled devices, please refer to FDA's safety communication, [Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed](#); [FDA Safety Communication](#).

Affected Device and Firmware Description

DR B 88
QED1337
Hospital Department
Patient Number
Patient Admit Date
Patient Name
Patient DoB
PADRE D...
2013.01.04
1963.08.08

In the European Union and the United States.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/tp](#).

TLP:CLEAR

As of January 30, 2025

- The reverse backdoor provides automated connectivity to a hard-coded IP address from the Contec CMS8000 devices, allowing the device to download and execute unverified remote files
- The IP Address is owned by a University in China
- Once started up, the device will automatically beacon to this IP address and once a connection is established, patient information is then transmitted via port 515 to the IP address
- Researchers were able to perform a simulation, which demonstrated patient information was sent to the IP address immediately upon connection

HIPAA Regulatory Update

HIPAA Security Rule NPRM Resources

HIPAA Security Rule NPRM

[Federal Register : HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information](#)

Clearwater Blog:

[Proposed HIPAA Security Rule Changes](#)

Polsinelli Blog:

[OCR Proposes Regulatory Facelift to the HIPAA Security Rule](#)

Clearwater Webinar

[HIPAA Security Rule NPRM: What to Know and What to Do - Clearwater](#)

HIPAA Security Rule Enforcement Actions

5 Resolution Agreements with OCR in January

Each of these settlements found that the regulated entity failed to conduct a compliant risk analysis as required by the Rule

- Elgon Information Systems – 1/7/25 \$80,000
- Virtual Private Networks – 1/7/25 \$90,000
- UCR Holdings – 1/8/25 \$337,750
- Solara Medical Supplies – 1/15/25 \$3,000,000
- Northeast Surgical – 1/15/25 \$10,000

Recommendations

Recommendations related to topics discussed in this briefing:

Related to Contec CMS8000

- Identify devices on your network using medical device inventory tool (e.g., Ordr, Asimily, Medigate/Xdome)
- If your patient monitor relies on remote monitoring features, unplug the device and stop using it
- If your device does not rely on remote monitoring features, unplug the device's ethernet cable and disable wireless (that is, WiFi or cellular) capabilities

Other recommendations

- Segment networks and ensure that remotely accessible devices are behind firewalls
- Ensure active monitoring is in place that is current with the latest threat intelligence and IoCs
- Continue to educate your users on the latest tactics and techniques as they evolve
- Maintain an accurate inventory of your information systems and your medical devices
- Perform a risk analysis at the information system and component level to identify risks to specific technologies. Risk analysis should be well documented and updated as changes to your environment occur
- Assess your critical vendors for risk, and create contingency plans (e.g., blood supply, lab services, SaaS)

The Return of OCR Audits? What It Means and How to Prepare for Potential Action

Andrew Mahler, Clearwater
Iliana L. Peters, Polsinelli



OCR Audits: Background

- Section 13411 of HITECH requires HHS to audit covered entity and business associate compliance with the HIPAA Rules: *“The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements.”*
- Audits initiated in 2012, 2016, 2024
- November 2024 OIG Report: OCR’s audit implementation too narrowly scoped to effectively assess ePHI protections and demonstrate a reduction of risks within the health care sector and oversight was not effective at improving cybersecurity protections at covered entities and business associates

2016-2017 OCR Phase 2 Audits: Findings



Notice of Privacy Practices: 2% of covered entities fully met the content requirements



Right of Access 89% failed to show they were correctly implementing the individual right of access



Breach Notification: 67% submitted notification letters to individuals that were missing one or more pieces of required content.



Risk Analysis: both covered entities and business associates failed to implement effective risk analysis and risk management activities to safeguard ePHI

2016-2017 OCR Phase 2 Audits: Ratings



Audit Compliance Effort Ratings—Legend	
Rating	Description
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	The audit results indicate the entity's efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - <i>e.g.</i> , policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of a serious attempt to comply with the Rules.

2024-2025 OCR Audits: The Process

- Notification via email introducing the process
- Will include:
 - Request to schedule 45-minute virtual meeting
 - Request for information about the organization
 - Request for information/documentation related to audited provisions
- Response within 30 calendar days
- Voluntary?

2024-2025 OCR Audits: Provisions subject to the Audit

Risk Analysis

Information System Activity Review

Security Awareness and Training

Security Incident Response Procedures

Response and Reporting

Data Backup Plan

Disaster Recovery Plan

Testing and Revision Procedures

Audit Controls

Person or Entity Authentication



OCR Audits: How to Prepare



OCR Audits: How to Prepare

- Conduct a comprehensive (and documented) Risk Analysis
- Develop and maintain detailed policies and procedures that cover all aspects of HIPAA compliance
- Regularly train staff on HIPAA privacy and security policies; training should be specific to your organization's practices and roles
- Ensure BAAs are in place wherever appropriate/required
- Review/Revise Incident and Recovery Response Plans
- Stay updated with regulatory changes
- Mock Audits and tabletop exercises
- Keep accurate records of all compliance efforts, including training records, risk assessments, and incident handling



Q&A



Upcoming Events



ViVE | February 16-19, 2025 Nashville, TN

- Clearwater is excited to again serve as title sponsor of the Cybersecurity Pavilion as the ViVE conference returns to Nashville in early 2025.
- [Click here](#) for more information and to register



HIMSS Global Conference | March 3-6, 2025 | Las Vegas, NV

- **Session Time:** Tuesday, March 4 at 10:15am PT **Session Title:** "Mastering Cyber Threat Intelligence to Protect Patient Safety".
- **Speakers:** Jon Moore, Clearwater Chief Risk Officer and Head of Consulting Services & Client Success & Michal Gross, Manager of Cybersecurity Intelligence for the Cleveland Clinic
- [Click here](#) for more information and to book a meeting with us



HPE Miami 2025 | March 5-6, 2025 | Miami, FL

- Stop by Clearwater's dedicated meeting table in the networking lounge to connect with our team of experts—Baxter Lee, CFO, David Kolb, Sales VP, and Richmond Donnelly, Sr. Account Executive.
- [Click here](#) for more information and to book a meeting with us



ADSO Summit 2025 | March 16-19, 2025 | San Diego, CA

- Be sure to stop by the Clearwater Kiosk to meet our team, including John Howlett, CMO & SVP and David Anderson, Sr. Account Executive.
- [Click here](#) for more information and to book a meeting with us

Upcoming Webinars and Virtual Events



Early 2025 Vulnerability Trends and the Future of Data Encryption Risk Hackers are Betting On Now | March 6, 2025 @ 12:00 CST

- Clearwater's March Cyber Briefing
- Steve Cagle, CEO, Clearwater
- Dave Bailey, VP, Consulting Services, Security, Clearwater
- Steve Akers, CTO & CISO, Clearwater



Forty-Second National HIPAA Summit | March 25-28, 2025 – Virtual

- Clearwater is thrilled to participate in the Virtual HIPAA Summit happening March 25-28, 2025! This event brings together top professionals and thought leaders in healthcare compliance, cybersecurity, and privacy to tackle the most pressing issues in healthcare today.
- [Click here](#) for our speaking sessions and 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/](https://www.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

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*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.