

# Monthly Cyber Briefing

January 9, 2025

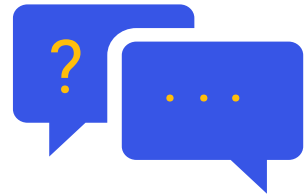


# Meeting Logistics



## 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.

# Agenda & Speakers

- Cyber Update
- Fireside Chat
  - Looking Back & Moving Forward: A Candid Conversation with Health Sector Coordinating Council Leaders
- Q+A



**Erik Decker**  
Panelist

Vice President and Chief  
Information Security Officer  
**Intermountain Health**



**Chris Tyberg**  
Panelist

Chief Information Security Officer  
**Abbott Laboratories**

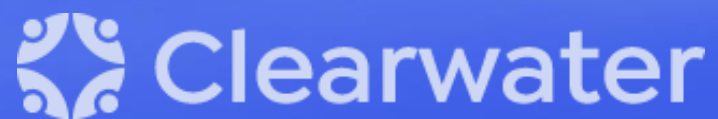


**Steve Cagle**  
Moderator

Chief Executive Officer  
**Clearwater**

# Cyber Update

Steve Cagle



# Breach Reports via OCR Breach Portal

## OCR Breach Portal Data<sup>1</sup>

- 706 breach reports totaling 184.5M individual records, an increase of 10% over 2023
- Top 10 Breaches of 2024 represented 84% of reported records breached

## Healthcare Records Breached<sup>2</sup>



## Top 10 Breaches of 2024

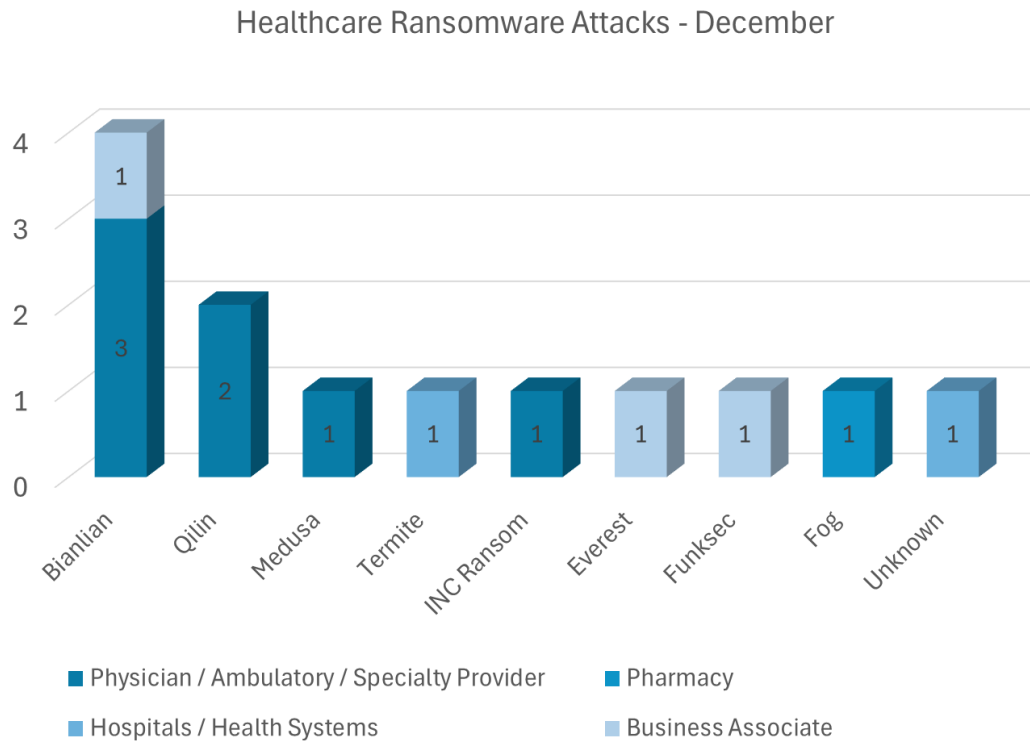
| Regulated Entity                    | Records            |
|-------------------------------------|--------------------|
| Change Healthcare, Inc.             | 100,000,000        |
| Kaiser Foundation Health Plan, Inc. | 13,400,000         |
| Ascension Health                    | 5,599,699          |
| HealthEquity, Inc.                  | 4,300,000          |
| Concentra Health Services, Inc.     | 3,998,163          |
| CMS                                 | 3,112,815          |
| Acadian Ambulance Service, Inc.     | 2,896,985          |
| A&A Services d/b/a Sav-Rx           | 2,812,336          |
| WebTPA Employer Services, LLC       | 2,518,533          |
| INTEGRIS Health                     | 2,385,646          |
| <b>Total</b>                        | <b>141,024,177</b> |

<sup>1</sup> The [HHS Breach Portal](#) (2024 data through 12/31/24, pulled on 1/6/25; 2023 data pulled 11/3/24)

<sup>2</sup> [Rocky Mountain Gastroenterology Reportedly Experiences Triple Cyberattack, Resulting in Data Breach Affecting Up to 169k | Console and Associates, P.C. - JDSupra](#)

# Ransomware Attacks

December was a particularly difficult month for Healthcare sector as existing and emerging threat actors continued to target hospitals, physician groups and healthcare services organizations.



- At least 18 known attacks in the healthcare sector in December
- As reported last month, we continue to see specialty care / physician management groups highly targeted
- Multiple attacks on California Hospitals over last 45 days
- In 2024 118 confirmed and 147 unconfirmed ransomware attacks took place in the US healthcare sector costing the industry \$21.9B.<sup>3</sup>

Source: [Halcyon Attacks Lookout](#) (December ransomware attacks as reported on 12/27/24)

<sup>1</sup> [California hospital recovers from cyber attack after nearly 2 weeks](#)


<sup>2</sup> [Cyber criminals claim they hacked 17 million patient records at PIH Health hospitals – Daily News](#)

<sup>3</sup> Source: [Comparitech](#)


# HC3 Alert – Credential Harvesting

The Health Sector Cybersecurity Community Center (HC3) issued an alert about on-going credential harvesting campaigns targeting the healthcare sector.

- Specific campaigns targeting healthcare and other industries
- Techniques employed
  - Phishing
  - Man in the Middle
  - Key logging
  - Credential Stuffing
  - Social Engineering
  - Phony Login Pages
  - Malware
- *Credential phishing attacks increased by 703% and social engineering attacks 141% in 2<sup>nd</sup> half 2024<sup>1</sup>*



Office of  
Information Security  
Securing the HHS



Health Sector Cybersecurity  
Coordination Center

## HC3: Analyst Note

December 17, 2024 TLP:CLEAR Report: 202412171700

### Defense and Mitigations

Credential harvesting is a technique leveraged by cyberattackers to collect legitimate usernames and passwords from unwitting victims for the purposes of using them in future attacks. The end result can be attacks that lead to data theft, disruption of critical systems, or other malicious impacts. There are a number of defense and mitigation steps to take when protecting against credential harvesting attacks, some of the more important are as follows:

- **Educating Your Workforce:** Ensure your workforce understands the following steps they can take to protect themselves as individuals, as well as your organization:
  - Use strong passwords (avoid personal details or anything easy to guess).
  - Do not re-use passwords across multiple accounts; this is a common practice that facilitates the success of credential harvesting.
  - Be reasonably sceptical and cautious when handling suspicious-looking e-mails; learn to recognize a phishing attack.
  - Be reasonably sceptical and cautious when handling suspicious phone calls; learn to recognize a social engineering attack.
  - Be cautious about suspicious-looking websites; always ensure you are submitting credentials to the proper site/application.
  - When in doubt of any form of communication, verify first.
- **Multi-Factor Authentication (MFA):** This requirement for multiple means of authentication can minimize the probability of a compromise, because if one factor (such as a password) is compromised, another is still required to access a system.
- **E-mail/Malspam Filtering:** Filters can be deployed and properly configured, which minimizes the amount of unwanted traffic flowing into your organization. Phishing is one of the most prolific infection vectors used by cyberattackers, and proper filtering can minimize associated risk.
- **Endpoint Security:** Utilizing endpoint security solutions can help detect and prevent malware-based credential harvesting techniques such as keylogging.
- **Monitoring/Detection:** Real time, comprehensive event and incident analysis across an enterprise infrastructure can help identify credential harvesting attacks as they occur. Leveraging appropriate tools and maintaining appropriately trained staff will improve this capability.
- **Vulnerability/Patch Management:** Keeping software and systems up-to-date with the latest security patches and updates can help address known vulnerabilities that attackers may exploit to harvest credentials. Maintaining a comprehensive and accurate inventory of all IT assets will improve the probability of success in this area.
- **Incident Handling/Response:** Developing and maintaining a full-lifecycle incident handling and response program (which should function closely with monitoring/detection above) can minimize the impact of credential harvesting on operations and patients.

HC3 has released [a credential harvesting sector alert](#) with additional analysis and recommendations.

### References

HC3 Sector Alert: Credential Harvesting and Mitigations  
<https://www.hhs.gov/sites/default/files/credential-harvesting-sector-alert-tlpclear.pdf>

Digital Identity Guidelines

[TLP:CLEAR, ID:202412171700, Page 2 of 4]

U.S. Department of Health and Human Services  
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)

# OCR Begins 2024-2025 Auditing Program

OCR continues enforcement for breach and ransomware HIPAA violations. Additionally, it has initiated the 2024 – 2025 Audit program previously announced.

## 2024-2025 HIPAA Audits Initiated

OCR has initiated its 2024-2025 HIPAA Audits. Ransomware, destructive malware, and other forms of malicious hacking present a growing and ongoing threat to the U.S. health care and public health sector and the privacy and security of electronic protected health information. In recent years, HIPAA covered entities (health plans, health care clearinghouses, and most health care providers) and business associates have experienced significant cyberattacks, which have impacted hospital operations, patient care, access to patient records and have had massive financial ramifications. Substantial increases in large breaches involving hacking and ransomware reported to OCR and the number of individuals affected by large breaches demonstrates the need for HIPAA covered entities and their business associates to ensure that they are complying with the HIPAA Security Rule.

The 2024-2025 HIPAA Audits will review 50 covered entities' and business associates' compliance with selected provisions of the HIPAA Security Rule most relevant to hacking and ransomware attacks.

**December 4, 2024**

**HHS Office for Civil Rights Imposes a \$1.19 Million Penalty Against Gulf Coast Pain Consultants for HIPAA Security Rule Violations**

**December 6, 2024**

**HHS Office for Civil Rights Imposes a \$548,265 Penalty Against Children's Hospital Colorado for HIPAA Privacy and Security Rules Violations**



# Proposed HIPAA Security Rule Update

HHS OCR Published NPRM on December 27<sup>th</sup> to modify the HIPAA Security Rule

## Key Takeaways

- OCR states intended to provide clarity and adjust to current technology and threat environment
- Clarifies scope: all systems that create, receive, transmit or maintain ePHI, connected systems, or systems that contain information that could provide access or threaten above systems
- Removes current concept of “addressable” and makes all security measures required
- Requires security controls as standards: *References* NIST, 405(d) HICP, HHS CPGs and other standards
- Requires regulated entities to maintain technology asset inventory and network map
- Provides specificity on Risk Analysis (largely reflects 2010 Final Guidance, but adds business associates)
- Strengthens requirements for planning for contingencies and responding to security incidents
- Requires compliance audits every 12 months
- Requires implementation, deployment and testing of technical controls every 12 months
- Require business associates to notify covered entities upon activation of contingency plan

[Link to Clearwater NPRM HIPAA Security Rule Client Fact Sheet.pdf](#)

OCR has published [a fact sheet located here.](#)

The [Notice of Proposed Rule Making \(NPRM\)](#) as published in the federal register is located here.

# Fireside Chat: Looking Back & Moving Forward

Moderator: Steve Cagle

Panelists: Erik Decker and Chris Tyberg





Q&A



# Upcoming Events & Webinars



## 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
- We are teaming up with Holland & Knight, Guidehouse & 25m Health for a networking night on Sunday to kickoff the week.
- [Click here](#) for more information and to register



## Guiding the Future: A Board Member's Framework for Managing AI Risks | February 4 @ 1:00 CST

- Join Jon Moore, Chief Risk Officer at Clearwater, for this essential webinar designed specifically for healthcare board members of The Governance Institute.
- This session will equip board members with the tools to navigate the complexities of AI, enhance organizational resilience, and oversee AI deployment that benefits both employees and patients while adhering to regulatory and ethical standards.
- [Click here](#) for more information and to register



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

- Clearwater Chief Risk Officer and Head of Consulting Services & Client Success Jon Moore is teaming with Michal Gross, Manager of Cybersecurity Intelligence for the Cleveland Clinic, to deliver the presentation "Mastering Cyber Threat Intelligence to Protect Patient Safety". Be sure to catch Jon and Michael's session on Tuesday, March 4, at 10:15am PT.
- [Click here](#) for more information and to book a meeting with us



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](http://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.