Monthly Cyber Briefing

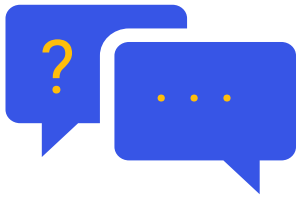
September 4, 2025

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.

Clearwater

Healthcare's Monthly Cyber Briefing

Agenda + Speakers:

- Cyber & Regulatory Update
- OCR Enforcement Findings in Cloud Environments
- Q+A

Dave Bailey, Clearwater VP Security Services

Steve Cagle, Clearwater CEO

Cyber & Regulatory Update

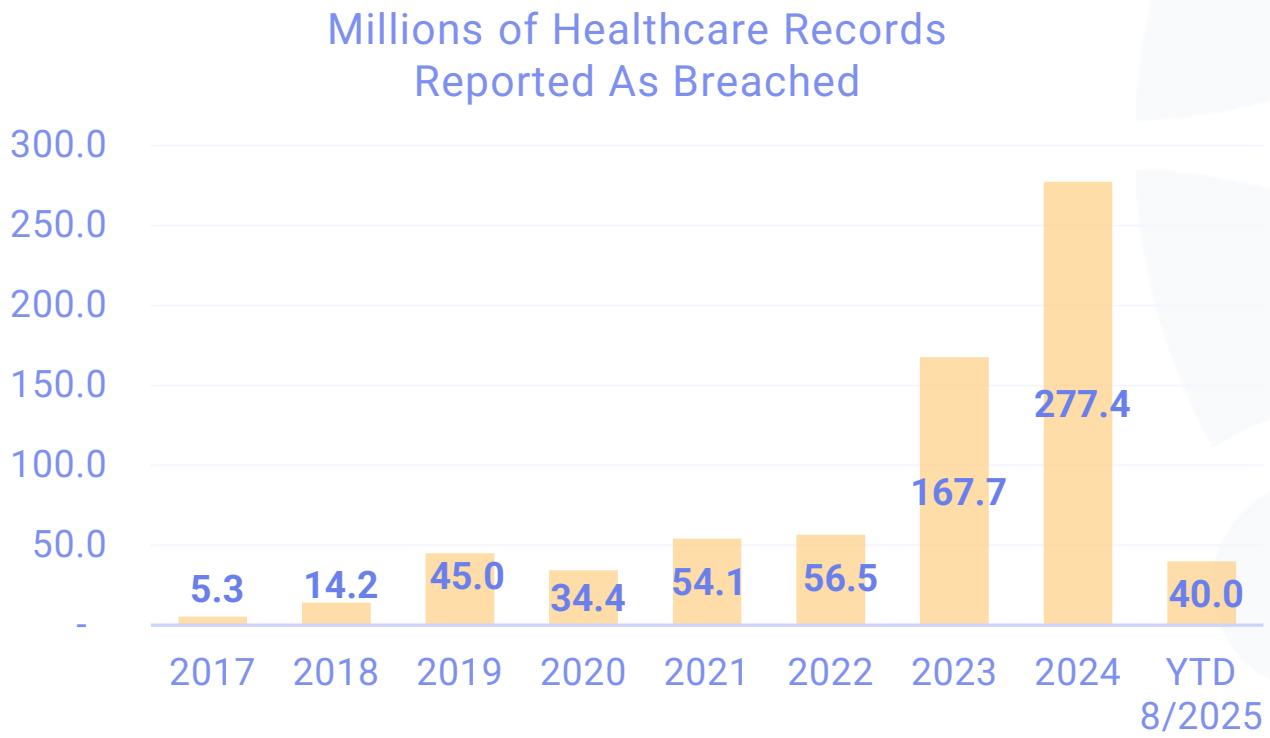
Steve Cagle, MBA, HCISPP, CHISL, CDH-E

CEO, Clearwater

Clearwater

Breach Reports via OCR Breach Portal[1]

- 2024 breach data: 277.4M individuals from 734 breaches
- YTD 2025 breach data: 40.0M individuals from 480 breaches
- ~4M records reported in past month and 62 new breaches



Notable (large) Breaches

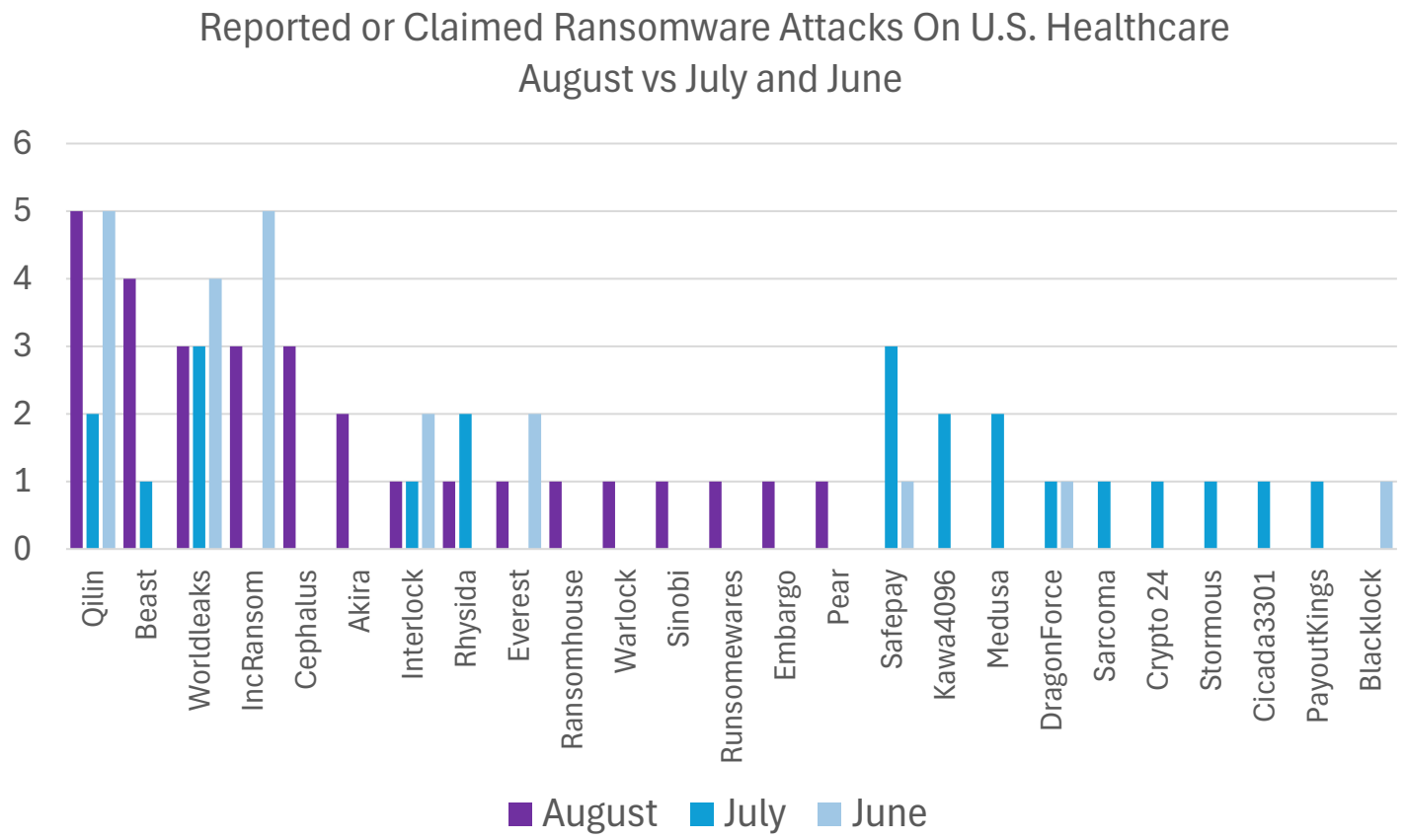
- DaVita (dialysis services) – Highly disruptive ransomware attack by Interlock that resulted in breach of 2.7M individuals
- Highlands Oncology Group – Medusa remained undetected for 4.5 months until deploying ransomware – 112K individuals affected in breach
- Vital Imaging Medical Diagnostic Centers – Another example of an attack on an imaging center resulting in breach of 270K individuals
- Aspire Rural Health, a Michigan-based healthcare provider – ransomware attack by BianLian going back to 2024 – 138K individuals affected

Clearwater

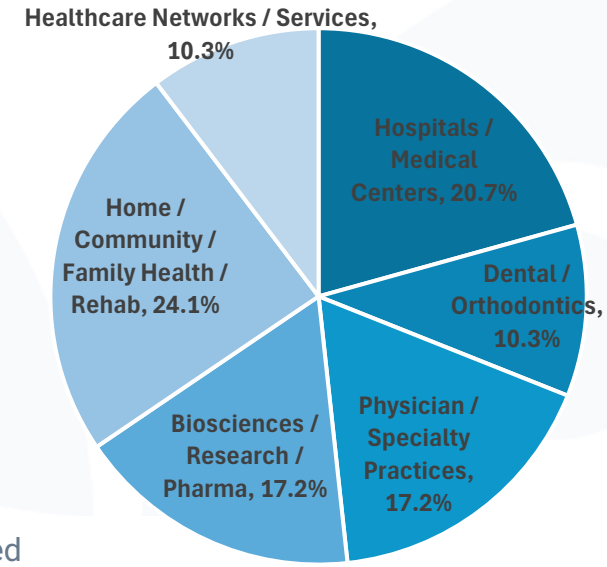
1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 8/31/25, pulled 8/31/25)

Healthcare Ransomware Attacks/Leaks Since Last Briefing

29 newly identified ransomware attacks on U.S. Healthcare organizations in August – 32% increase over average of previous three months



- INC Ransom, who was inactive last month, returns with 3 ransomware attacks
- Qilin continues lead in attacks since May. Evolving techniques, capabilities and network
- Two new threat actors in top 5 – Cephalus and Beast (see next slides) among 8 new threat actors not previously seen this year in healthcare

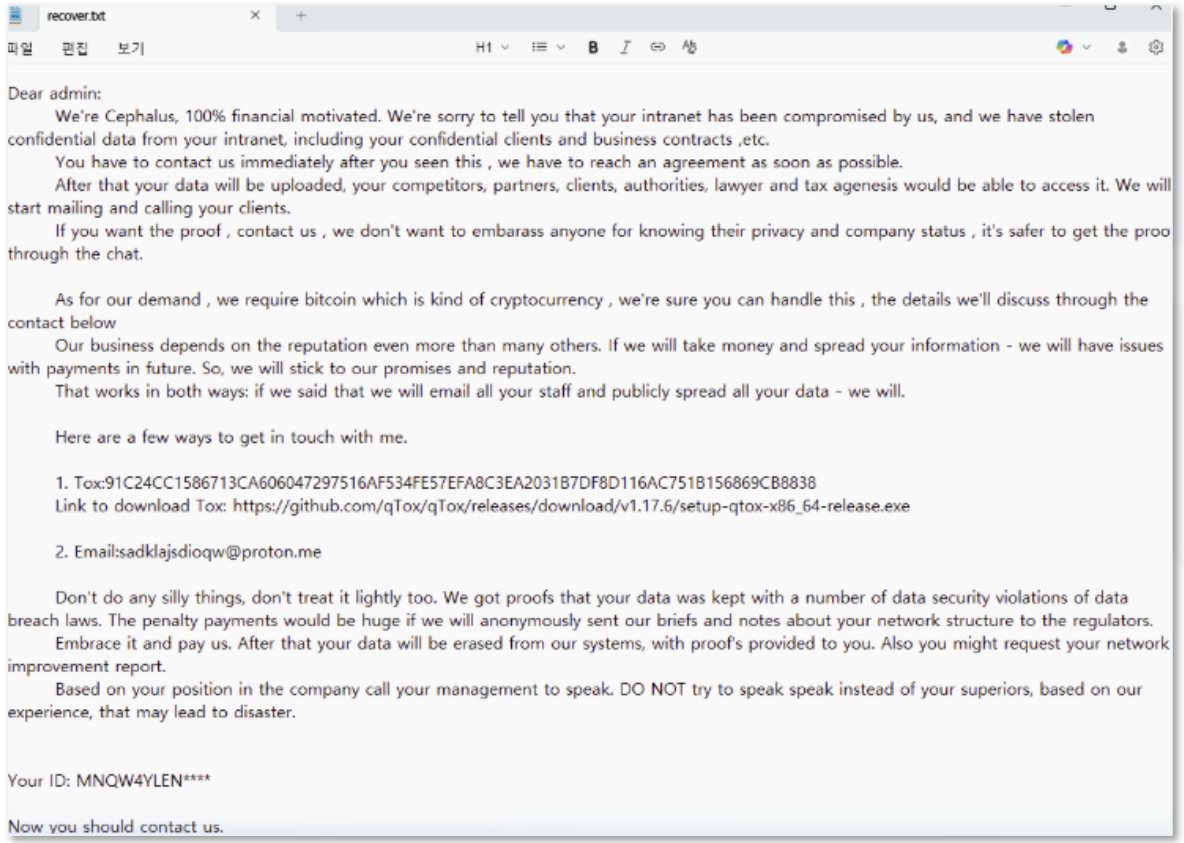


Clearwater

Source: Ransomware.live Healthcare or publicly reported but not yet leaked

New Threat Actor Targeting Healthcare - Cephalus

3 Attacks on U.S. Healthcare organizations including Colorado Health Network, Texas Pregnancy Care Network and what appears to be a second extortion of CareSTL Health



recover.txt

파일 편집 보기

Dear admin:

We're Cephalus, 100% financial motivated. We're sorry to tell you that your intranet has been compromised by us, and we have stolen confidential data from your intranet, including your confidential clients and business contracts ,etc.

You have to contact us immediately after you seen this , we have to reach an agreement as soon as possible.

After that your data will be uploaded, your competitors, partners, clients, authorities, lawyer and tax agenesis would be able to access it. We will start mailing and calling your clients.

If you want the proof , contact us , we don't want to embarass anyone for knowing their privacy and company status , it's safer to get the proo through the chat.

As for our demand , we require bitcoin which is kind of cryptocurrency , we're sure you can handle this , the details we'll discuss through the contact below

Our business depends on the reputation even more than many others. If we will take money and spread your information - we will have issues with payments in future. So, we will stick to our promises and reputation.

That works in both ways: if we said that we will email all your staff and publicly spread all your data - we will.

Here are a few ways to get in touch with me.

1. Tox:91C24CC1586713CA606047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838
Link to download Tox: https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe

2. Email:sadklajsdioqw@proton.me

Don't do any silly things, don't treat it lightly too. We got proofs that your data was kept with a number of data security violations of data breach laws. The penalty payments would be huge if we will anonymously sent our briefs and notes about your network structure to the regulators.

Embrace it and pay us. After that your data will be erased from our systems, with proof's provided to you. Also you might request your network improvement report.

Based on your position in the company call your management to speak. DO NOT try to speak speak instead of your superiors, based on our experience, that may lead to disaster.

Your ID: MNQW4YLEN****

Now you should contact us.

Image of Cephalus ransomware note.

- Emerged August 2025 – already claims 19 victims
- Entry via RDP using accounts without MFA
- Uses MEGA as part of data exfiltration
- Abuses legitimate SentinelOne executables[1] to deploy its payload via dynamic-link library (DLL) sideloading
- Cripples recovery with shadow-copy deletion
- Systematically attempts to disable Windows Defender through PowerShell and registry manipulations.
- High pressure ransomware note

1 **SentinelBrowserNativeHost.exe**, a legitimate **SentinelOne** executable, was launched from the user's Downloads folder, which then loaded **SentinelAgentCore.dll**. From this, **data.bin (ransomware)** was then loaded.

Clearwater

For more technical information see: Cephalus Ransomware: Don't Lose Your Head | Huntress

New Threat Actor Targeting Healthcare - Beast

4 Attacks on U.S. Healthcare organizations including Van Hook Dental Studio, Huron Regional Medical, Rehabilitation Health Services and Provail

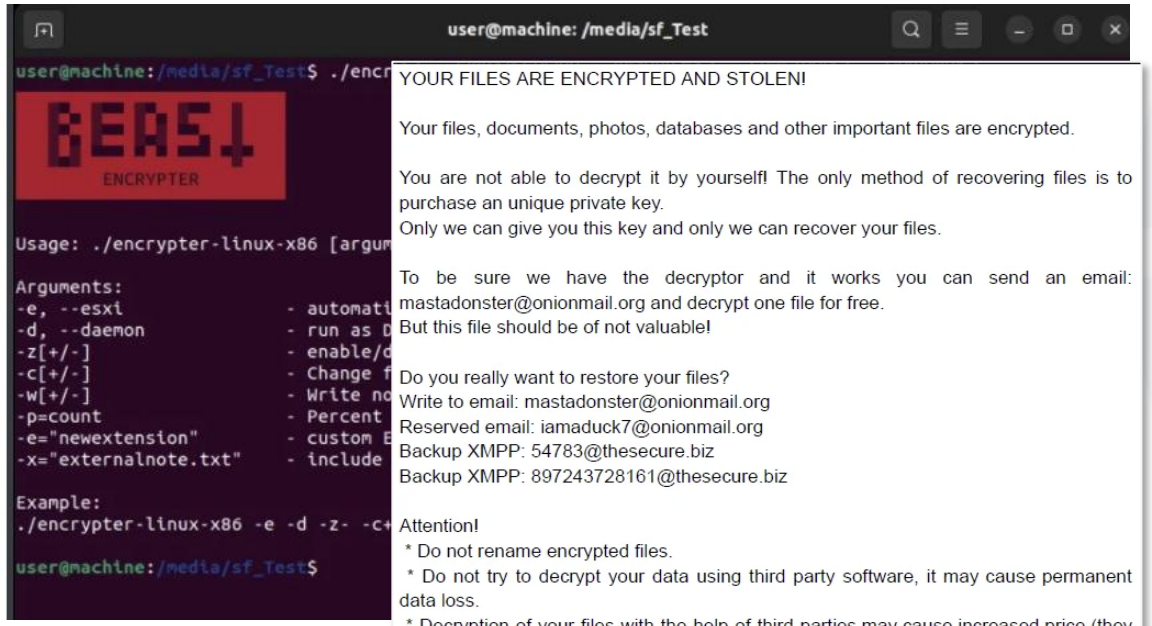


Image of Beast encryptor.

YOUR FILES ARE ENCRYPTED AND STOLEN!

Your files, documents, photos, databases and other important files are encrypted.

You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an email: mastadonster@onionmail.org and decrypt one file for free.
But this file should be of not valuable!

Do you really want to restore your files?
Write to email: mastadonster@onionmail.org
Reserved email: iamaduck7@onionmail.org
Backup XMPP: 54783@thesecure.biz
Backup XMPP: 897243728161@thesecure.biz

Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
* We have been in your network for a long time. We know everything about your company most of your information has already been downloaded to our server. We recommend you to do not waste your time if you dont wont we start 2nd part.
* You have 24 hours to contact us.
* Otherwise, your data will be sold or made public.

BEAST ransomware

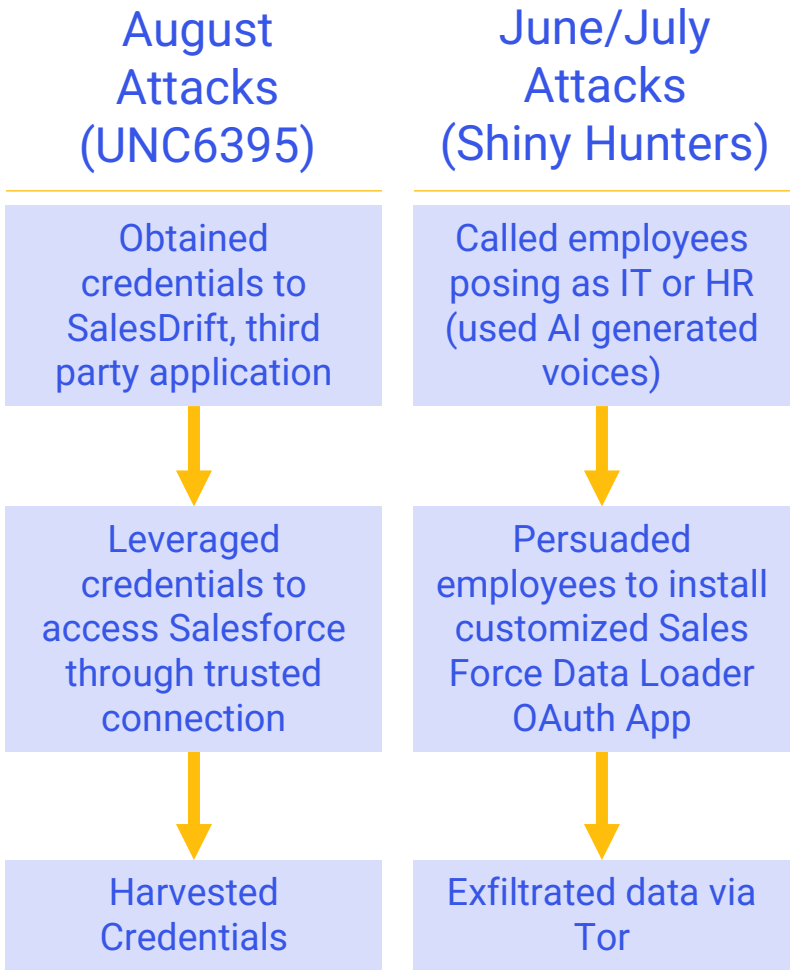
Image of Beast ransomware note.

- Active since 2022 (formerly Monster), however, new capabilities and affiliate program promoted starting June of this year
- Use brute forced, password spraying or purchased leaked credentials, as well as target misconfigured internet-exposed servers, often finding credentials that don't have MFA
- Avoids detection by disguising executables and binaries to look like they are legitimate
- Uses Tor leak site and onion network making it harder for law enforcement to trace them
- Typical double extortion with short turnaround time to leak data if ransom is not paid

Clearwater

Reference THREAT ANALYSIS: Beast Ransomware by Cyberreason

Cyber Attacks on Salesforce Customers



Threat Actors targeting Salesforce in multiple attack campaigns, enabling them to compromise sensitive data from large companies

Recent Attack – August - **UNC6395**

- Used compromised OAuth credentials associated with Salesloft Drift to exfiltrate data from Salesforce customer instances
- Stole credentials, focusing on sensitive information like AWS access keys, passwords, and Snowflake-related access tokens
- 700 victims, including Cloudflare, Palo Alto, and Zscaler, and a limited number of Google Workspaces

June/July Attacks – **Shiny Hunters (+ Scattered Spider & LAPSUS$)**

- Impersonated IT staff in phone calls, convincing targets to install a customized version of Salesforce Data Loader OAuth application
- Leveraged stolen credentials/tokens stolen through phishing pages
- Victims include Google, Qantas, Allianz Life, Workday, Pandora, Cisco, Chanel, and Adidas
- Members of 3 gangs teamed to become "Scattered LAPSUS$ Hunters"

Clearwater

OCR Enforcement For Ransomware & Risk Analysis

OCR finds that failure to conduct risk analysis related to ransomware attack that resulted in a breach of 24,891 individuals. *15th Ransomware Enforcement Action.*

BST & Co. CPAs, a New York accounting, advisory, and management consulting firm entered into a 2-year CAP and paid $175,000 settlement

- BST is a HIPAA business associate and receives financial information that also contains protected health information (PHI)
- December 7, 2019, BST discovered that part of its network was infected with ransomware
- OCR's investigation determined that BST had failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by BST

Key quotes from new OCR Director Paula Stannard:

"A HIPAA risk analysis is essential for identifying where ePHI is stored and what security measures are needed to protect it."

"Completing an accurate and thorough risk analysis that informs a risk management plan is a foundational step to mitigate or prevent cyberattacks and breaches."

OCR Given Additional Enforcement Responsibility

HHS Secretary Robert F. Kennedy, Jr. announced it is empowering Office for Civil Rights to administer and enforce confidentiality of Substance Use Disorder patient records.

Authorities delegated include:

1. Impose civil money penalties under section 1176 of the Social Security Act, as amended, for failures to comply with requirements under 42 CFR Part 2;
2. Enter into resolution agreements, monetary settlements, and corrective action plans, as appropriate, to resolve indications of noncompliance with requirements of that section;
3. Issue subpoenas requiring the attendance and testimony of witnesses and the production of any evidence that relates to any matter under investigation or compliance review for failure to comply with requirements of that section.

Link to Federal Register Fact Sheet 42 CFR Part 2 Final Rule | HHS.gov

Recommendations

Relevant actions based on current healthcare threat actor TTPs & regulatory enforcement trends discussed in this briefing.

- Don’t expose RDP directly to the internet; instead, use a VPN or Zero Trust Network Access (ZTNA)
  - Restrict RDP access to only those users who absolutely need it
  - Monitor RDP Sessions: Keep a close eye on RDP activity and logs to detect suspicious actions
- Enforce strong passwords and enable phishing resistant Multi-Factor Authentication (MFA) and Network Level Authentication (NLA)
- Train workforce on AI powered vishing TTPs; conduct vishing and smishing testing using realistic attack scenarios
- Monitor for latest IOCs, particularly of threat actors targeting healthcare
- Apply strict controls and perform regular audits of OAuth-connected applications; generate alerts for unusual activity
- Protect tokens or credentials associated with integrations. Periodically revoke and rotate credentials in APIs and monitor for updates from vendors. Use concept of least privilege for integration accounts and limit data accessible to minimum necessary
- Continuously scan for vulnerabilities and patch critical and high-risk vulnerabilities right away
- Update your risk analysis ensuring it includes all information systems, it’s up to date, and have a Risk Management Plan

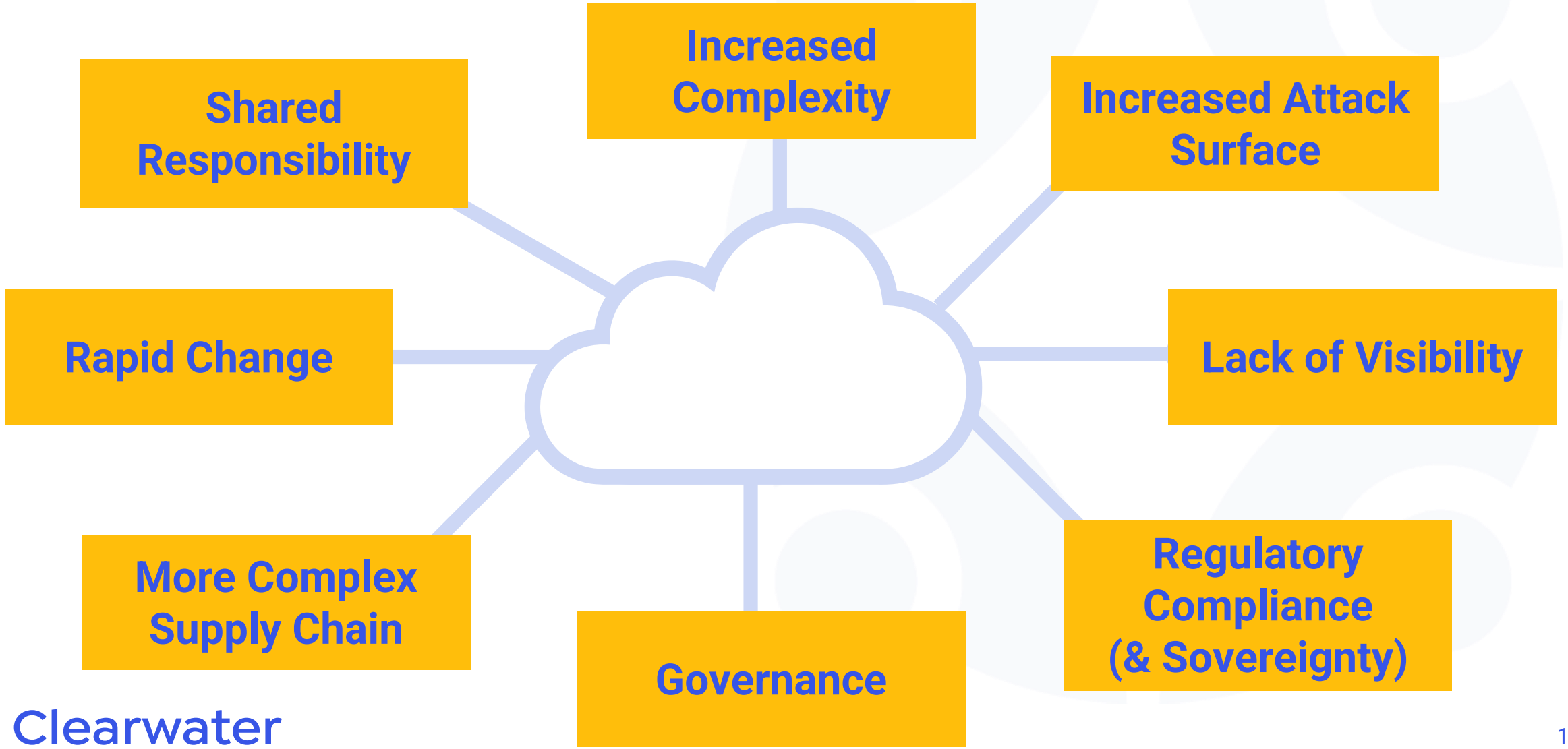
OCR Enforcement Findings in Cloud Environments

Dave Bailey, VP of Security Services, Clearwater

Clearwater

Cloud risks are different because they **shift control boundaries**, increase **third-party dependencies**, and create **compliance challenges** around data location, auditability, and vendor accountability

Cloud adoption must be paired with rigorous governance, contracts, monitoring, and regulatory mapping



Clearwater

Shared responsibility requires clear understanding of the boundaries

Cloud Service Provider

The cloud service provider ensures **the cloud** is secure

Customer

The customer ensures **their usage of the cloud** is secure

Cloud Infrastructure

Application(s)

Data

Clearwater

The customer's role centers on securing what they put in and how they use the cloud

Infrastructure: IaaS	Platform: PaaS	Software: SaaS
Compliance & Governance	Compliance & Governance	Compliance & Governance
Logging & Monitoring	Logging & Monitoring	Logging & Monitoring
Identity & Access Mgmt	Identity & Access Mgmt	Identity & Access Mgmt
Data Security and Privacy	Data Security and Privacy	Data Security and Privacy
Application	Application	Application
Operating System	Operating System	Operating System
Network & Virtualization	Network & Virtualization	Network & Virtualization
Physical Facilities	Physical Facilities	Physical Facilities

Provider Shared Customer

Clearwater

Cloud Service Providers are Business Associates

A covered entity (or business associate) that engages a CSP should understand the cloud computing environment or solution offered by a particular CSP so that the covered entity (or business associate) can appropriately **conduct its own risk analysis** and **establish risk management policies**, as well as enter into appropriate BAAs

Question	OCR Guidance
A CSP is a Business Associate if:	The CSP stores only encrypted ePHI and does not have a decryption key
Do the HIPAA Rules require a CSP to maintain ePHI for some period beyond when it has finished providing services to a CE or BA?	No, the HIPAA Rules generally do not require a business associate to maintain electronic protected health information (ePHI) beyond the time it provides services to a covered entity or business associate. The Privacy Rule provides that a business associate agreement (BAA) must require a business associate to return or destroy all PHI at the termination of the BAA where feasible. See 45 CFR § 164.504(e)(2)(ii)(J).
Do the HIPAA Rules require CSPs that are Bas to provide documentation, or allow auditing, of their security practices by their customers who are CEs or BAs?	No. The HIPAA Rules require covered entity and business associate customers to obtain satisfactory assurances in the form of a business associate agreement (BAA) with the CSP that the CSP will, among other things, appropriately safeguard the protected health information (PHI) that it creates, receives, maintains or transmits for the covered entity or business associate in accordance with the HIPAA Rules.

Source: https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

Multiple OCR enforcement actions in 2025 point to growing concern for inadequate risk analysis among cloud service providers

Cloud Service	Finding
Elgon Information Systems	▪ Cloud-based EHR/billing provider failed to conduct accurate and thorough risk analysis contributing to ransomware incident
Virtual Private Network Solutions	▪ Deficient risk analysis cited in cloud service provider's OCR settlement announcement
Comstar LLC	▪ Provider of billing and collection services delivered via cloud cited for insufficient risk analysis related to ransomware incident

Encryption, permissions, and lack of effective authentication among top weaknesses in AWS

Cloud adoption enables speed, scale, and innovation. However, without proper assessment and secure configuration, AWS environments can expose sensitive data, disrupt operations, and create regulatory risk

Top Risks	Description
S3 Misconfigurations	Public access, lack of encryption, no versioning
IAM Weaknesses	Overly permissive roles, no MFA, hardcoded keys
Logging	Missing or misconfigured CloudTrail, no monitoring of privilege escalations
Unencrypted Data/Backups	EBS snapshots, RDS backups left unencrypted.

Misconfigurations, elevated privileges, and identity practices among top weaknesses in Azure

Assessing and securely configuring Azure is essential to protecting data, ensuring compliance, and enabling resilient business operations. It is not just an IT concern—it is a core business obligation that safeguards trust and reduces risk.

Top Risks	Description
Blob Storage Misconfigurations	Anonymous access, unencrypted storage
Overly Permissive RBAC	Global admin assigned broadly, no MFA
Audit Logging Failures	No Defender for Cloud, no Sentinel alerts
Unsupported Services	Using Power BI, Logic Apps, OpenAI without HIPAA coverage
Identity Risks	Illicit consent grant attacks via Entra ID, insecure group permissions
Weak Password Policies	leads to password spraying and PHI compromise

Continuous risk analysis & assessment is essential

One-time hardening is insufficient. Continuous risk analysis, security assessments and configuration reviews keep risk aligned to business tolerance

Cloud Changes Rapidly	• New cloud services and features launch frequently
Dynamic Business Needs	• Mergers, integrations, and new applications shift workloads
Evolving Threat Landscape	• Attackers actively target cloud misconfigurations

Clearwater

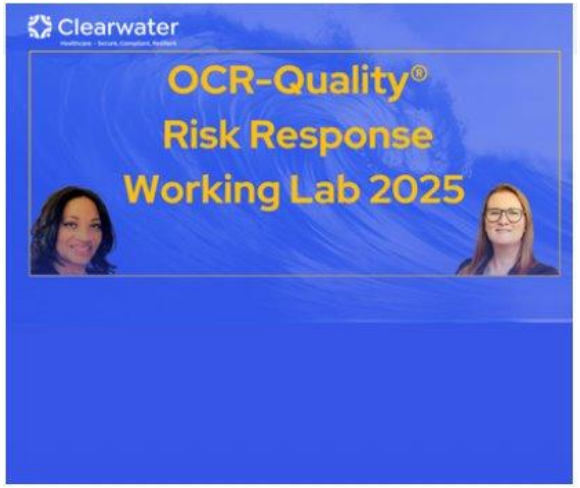
While CSPs secure the underlying infrastructure, customers are responsible for securing their data, access, and configurations

- Build and maintain a comprehensive cloud asset inventory
- Apply least privilege across IAM and AAD roles; enforce MFA
- Enable comprehensive logging & monitoring (CloudTrail, Azure Defender, Sentinel)
- Encrypt all ePHI (data at rest, in transit, and in backups)
- Validate BAA coverage for every cloud service used
- Conduct regular DR tests; ensure multi-region redundancy
- Adopt continuous cloud security posture management with healthcare-aware tools

Most cloud breaches don’t come from the cloud failing – it is customer misconfigurations or lack of implemented controls that can directly expose sensitive data

Q&A

Upcoming Webinars



OCR-Quality® Risk Response Working Lab 2025: Beginning September 10 @ 11:00 am CT

- Hands-On, Interactive E-Learning Series to Help You Minimize Cyber Risk Exposures and Meet Compliance Requirements
- 2-Part Series
- Register here

AHLA Webinar: Health Care's Due Diligence Dilemma | September 16, 2025 | 2:00 – 3:00 pm ET

- Andrew Mahler, VP Privacy and Compliance Services presenting on how organizations can address cybersecurity and data privacy challenges during health care mergers and acquisitions.
- Register here

Clearwater's Rural Critical Access Connect | September 18, 2025 | 12pm – 1pm CT

- Clearwater's Rural Critical Access Connect is your quarterly chance to connect and learn with peers facing the same cybersecurity challenges.
- Register here

Secure and Compliant: OCR-Quality® Risk Management in Action | October 1, 2025 | 12pm – 1pm CT

- Steve Cagle, CEO, Clearwater
- Lori Dutcher, CCO at Beth Israel Lahey Health
- Jon Moore, CRO and Head of Consulting Services, Clearwater
- Will Explore how healthcare organizations can build and sustain OCR-quality risk management programs that go beyond checkbox compliance
- Register here

Clearwater

Upcoming Events

McGuireWoods Healthcare GO Conference | September 16-17, 2025 | Charlotte, NC

- Attending the **McGuireWoods Healthcare GO Conference**, a premier two-day event convening leaders across healthcare operations, life sciences, private equity, and finance.
- Learn More & Register here

Nashville Healthcare Sessions | September 29-30, 2025 | Nashville, TN

- Several Clearwater Colleagues attending **Nashville Healthcare Sessions**, the nation's premier healthcare innovation and finance event.
- Learn More & Register here

Hospital Horizons Symposium 2025 | October 6–7, 2025 | Washington, DC

- Clearwater is proud to sponsor the second annual **Hospital Horizons Symposium**, hosted by Holland & Knight.
- Expert panels & networking
- Register & learn more here

SCALE Healthcare Leadership Conference | October 14, 2025 | New York, NY

- Clearwater is a proud sponsor
- Clearwater leading a panel discussion "Understanding Cyber Security Risks in a world of AI"
- Learn more & Register here

Clearwater

See you next month! October 9th

- **Speaking the Same Language: Building Trust Between Security and the Enterprise**
  Fireside chat with Steve Cagle, CEO Clearwater & Tracy Touma, Cybersecurity Business Liaison on the Cleveland Clinic Advisory Team
- Meeting moved to the 2nd Thursday of the month, October 9th
- You are already registered and will automatically be enrolled in next month's briefing.

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.