Monthly Cyber Briefing

October 3, 2024

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A chat box.

Materials

Briefing materials and recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Agenda & Speakers

- Cyber Update
- View from Washington: How Federal Cybersecurity Policy May Impact Healthcare Organizations

Steve Cagle
Chief Executive Officer
Clearwater

Mari Savickis
Vice President, Public Policy
CHiME

Cyber Update

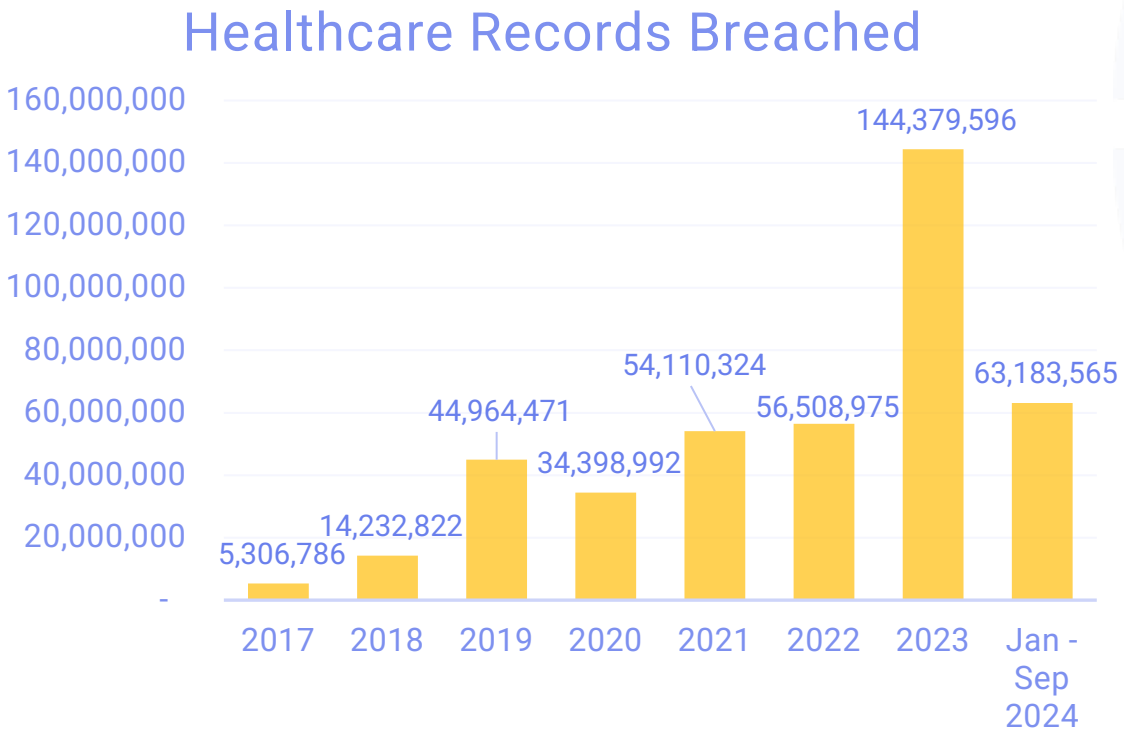
Steve Cagle

Clearwater

Breach Reports via OCR Breach Portal

OCR Breach Portal Data[1]

- 144.4M records reported breached in 2023, an increase of 156% vs 56.5 million in 2022
- YTD = 63m records from 519 breaches in 2024, an increase of ~9M records and 48 breaches since last month



Change Healthcare still reporting 500 records

Notable in OCR Breach Portal

- Centers for Medicare & Medicaid Services (CMS) and Wisconsin Physicians Service Insurance Corporation (WPS) (1M) records – May 2023 MOVEit breach, just reported in September of this year
- Acadian Ambulance (2.9M records)– Ransomware attack by Daixin group on June 21st – initially claimed 10M unique patient records[3]

Clearwater

1 The HHS Breach Portal (2024 data through 9/30/24, pulled on 10/1/24)
2 CMS Notifies Individuals Potentially Impacted by Data Breach | CMS3 Acadian Ambulance hit by ransomware attack; Daixin claims info on 10 million patients stolen –3 DataBreaches.Net

Ransomware – Additional Facts and Figures

2,018 Average weekly attacks on healthcare, a 32% increase over last year

$65M Lawsuit settlement for breach of ePHI, including nude photos of cancer patients

$1.3B Estimated cost to Ascension from recent ransomware attack

$2.5B Estimated cost to Change Healthcare from its ransomware attack

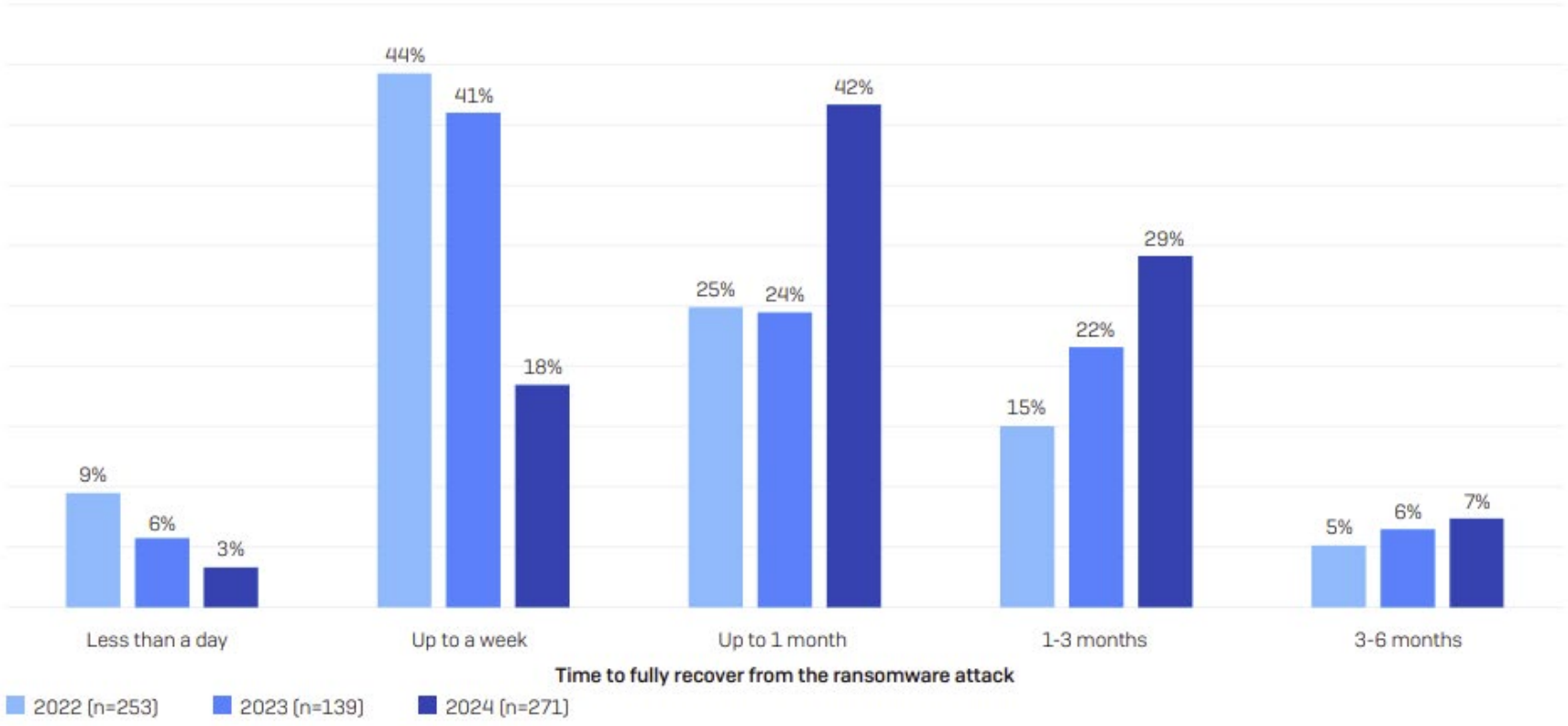
70% Percentage of providers impacted by Change Healthcare ransomware

$1.5M Median ransomware payment of “severe strain” up 650% from 2023

1 Check Point Blog
2 Pa. health system agrees to $65 million settlement after hackers leaked nude photos of cancer patients | CNN Business
3 Ascension financials show $1.3 billion cost from cyberattack | STAT (statnews.com)
4 Change Healthcare's Breach Costs Could Reach $2.5 Billion (bankinfosecurity.com)
5 Healthcare IT Spending: Innovation, Integration, and AI | Bain & Company
6 Ransomware review: September 2024 - ThreatDown by Malwarebytes

Ransomware Recovery Time Increasing

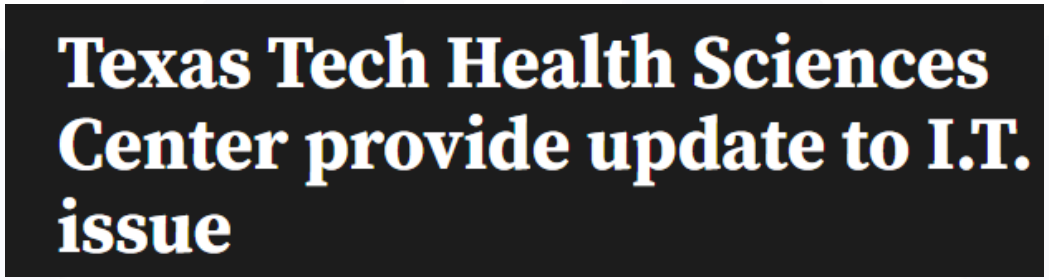
According to a new report by Sophos, the time taken to recover from a ransomware attack has steadily increased in healthcare.



Clearwater

sophos-state-of-ransomware-healthcare-2024.pdf

Two On-Going Incidents In West Texas



University Medical Center, Lubbock, TX

- Only Level 1 Trauma Center in West Texas
- IT outage reported last week, later confirmed to be ransomware attack 9/26
- Initially diverted all emergency and non-emergency care. Now accepting some ambulances with emergency care. Patients in clinics.
- Attack is on-going

Texas Tech University Health Sciences Center

- Limited clinical operations and all academic operations canceled
- Have not announced the cause of the attack
- Adding to diversion of patients to Covenant Health System, the other major provider in the Lubbock area
- No timeline for restoration of operations according to website

Clearwater

Ransomware Attack Forces UMC to Divert Emergency Patients - Infosecurity Magazine (infosecurity-magazine.com)
Texas Tech Health Sciences Center experiencing I.T. issues (msn.com)

Vanilla Tempest Targeting Healthcare With INC Ransomware

Microsoft Threat Intelligence team recently warned that the Russian speaking Vanilla Tempest ransomware group (previously known as Vice Society) has been actively attacking the healthcare sector.

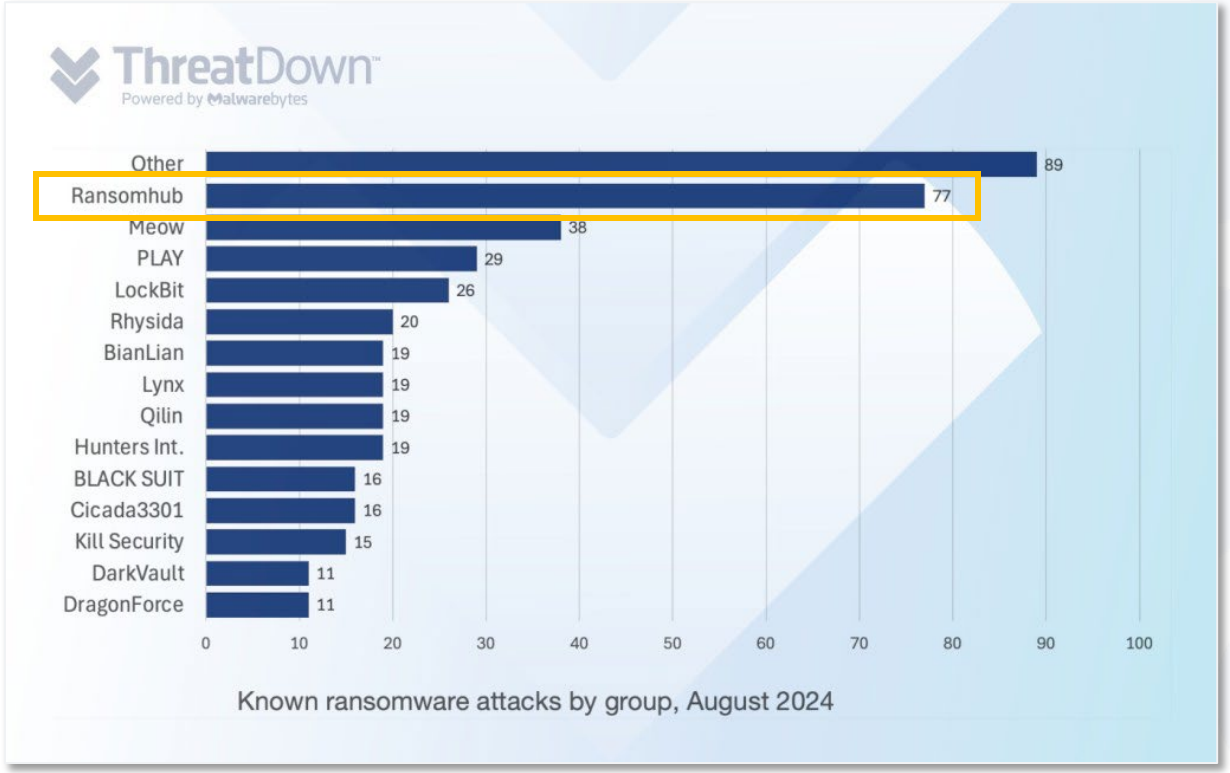
Link to Microsoft Threat Intelligence

- Also known as Vice Society, previously focused on education and other industries
- Works with Storm-0494 threat actor, who deploys GootLoader Malware, for initial access,
- Once inside, use Supper malware and deploy legitimate AnyDesk remote monitoring and MEGA data synchronization tools
- Then performs lateral movement through Remote Desktop Protocol (RDP) and uses the Windows Management Instrumentation Provider Host to deploy the INC ransomware payload.
- Microsoft states “Defender for Endpoint detects multiple stages of Vanilla Tempest activity and known INC ransomware and other malware identified in this campaign”

Clearwater

RansomHub Continues Its Rise to Top Ransomware Gang

As previously reported in August and September, RansomHub has become one of the most active and successful threat actors, building the largest affiliate network.



- The FBI and CISA and HHS released a joint advisory to disseminate known RansomHub ransomware IOCs and TTPs on August 29th
- Number of attacks increased from 53 in July to 77 in August
- Defense evasion techniques include “EDR Killers” such as using TDSSKiller, a legitimate tool from Kaspersky, to attempt disabling endpoint detection and response (EDR) services on target systems, and EDRKillShifter to install drivers with exploitable vulnerabilities
- Recent attacks
  - One point Patient Care (9/15/24)
  - Southeastern Retina Associates (9/13/24)
  - Cardiology of Virginia (9/7/24)

Clearwater

Resurgence of MEOW Ransomware

MEOW quickly reached second place for ransomware attacks in August.

readme.txt - Notepad

File Edit Format View Help

```
MEOW! MEOW! MEOW!

Your files has been encrypted!

Need decrypt?  Write to e-mail:

meowcorp2022@aol.com

meowcorp2022@proton.me

meowcorp@msgsafe.io

meowcorp@onionmail.org

or Telegram:

@meowcorp2022

@meowcorp123

Uniq ID: 4d2942e6-49a6-410b-9a09-a02423f53e1c
```

> "Don't miss this unique chance to access confidential data from Hewlett Packard Enterprise at an affordable price. Simply click the 'Buy' button and provide your contact information for registration. Our team will ensure a smooth and confidential transaction."

- Emerged in 2022, derived as a strain from Conti Ransomware
- Free encryptor available in 2023
- Targeting mainly U.S. companies, with healthcare a primary target
- No specific CISA or HC3 advisories at this time
- Recent attacks on U.S. healthcare:
  - Advanced Physician Management Services (9/11/24)
  - Zydus Pharmaceuticals (8/15/24)
  - American Contract Systems (8/13/24)
  - The Physical Medicine Rehabilitation Center (7/26/24)

Addressing Current Threat Environment

Specific recommendations related to content in this briefing

- Ensure you have a complete information asset inventory (you can't protect what you are not aware of)
- Conduct risk analysis at the information system and component level to address specific risks
- Require phishing-resistant non- SMS-based multi-factor authentication.
- Educate users to both recognize and report more sophisticated phishing attempts
- Separate user and admin privileges
- Assess third-party access. Limit as much as possible. Verify third-party controls are sufficiently followed.
- Install updates for operating systems, software and firmware immediately
- Ensure current password controls are in place – Review NIST SP 800-63B Digital Identity Guidelines
- Evaluate your monitoring, detection and response capabilities – are they sufficient?
- Validate security controls mapped to the MITRE ATT&CK framework (Secure Controls Validation Assessment)

Federal Cyber Policy Update

October 3, 2024

Big Picture

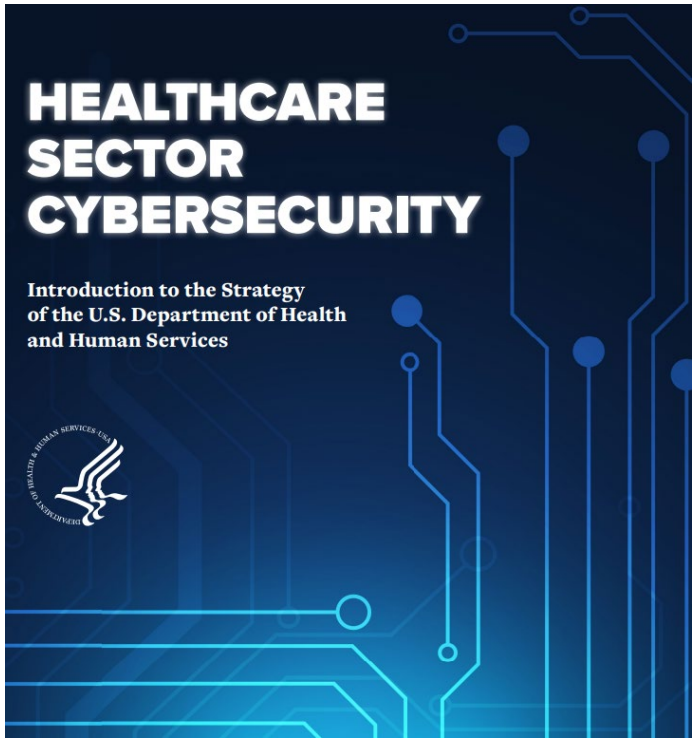
Congress	Administration	Other Issues
• Cyber is bipartisan issue – scrutiny continues • For now, all eyes on election • Congress out of session until after election • Little moving until end of the year • 2 possible cyber bills in play • Cyber funding for providers unlikely this year	• Rules coming but delayed • New Administration will slow things down • New cyber executive order expected • WH-led legislation announced at DEFCON on AI with security focus	• Impact from Chevron decision • Particle Health vs Epic • Privacy overlays everything • AI complicating picture

HHS Cyber Rules in Play

HIPAA Security Rule	Healthcare System Resiliency and Modernization	HTI-2
OCR - Proposed	**CMS - Proposed**	**ONC - Proposed**
• Forthcoming – Dec. • Being re-opened • Economically significant • Cyber mandates expected	• Forthcoming – late • Revise / update national emergency preparedness requirements for Medicare / Medicaid-participating providers / suppliers to plan adequately for both natural and man-made disasters • Economically significant	• Published 8/5 • Calls for all certified health IT to protect ALL PHI and new requirements for server-side encryption and include the PII encryption requirements for servers in a way that maintains existing end-user device encryption requirements and applies the existing encryption standard and the default settings requirements broadly in one criterion • Economically significant

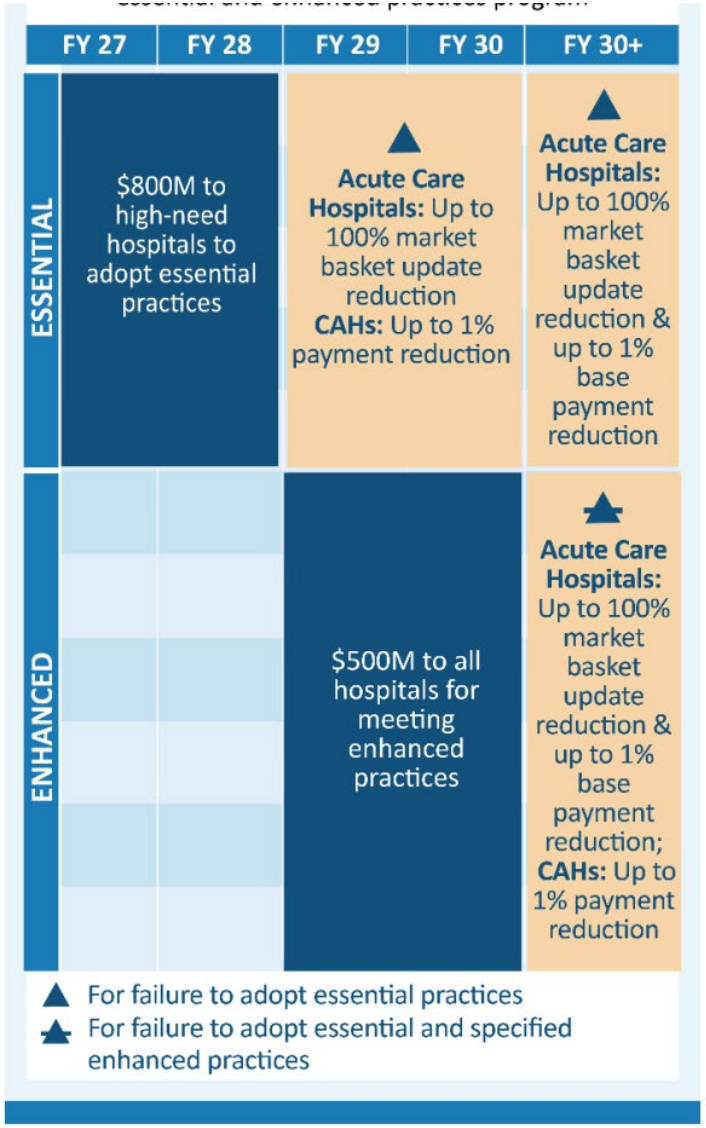
HHS Cyber Strategy

- Strategy released January 24th
- Impacted by *Chevron* decision
- Current HHS Strategy calls for:
  - Congressional funding (unlikely)
  - Multi-pronged approach
  - Mandates predicated on adoption of Cybersecurity Performance Goals (CPGs)
  - Congress to increase civil monetary penalties for HIPAA violations and funding to conduct more audits



HHS Budget Request

- The President's FY25 Budget Request for HHS requested money from Congress to fund a Cybersecurity Incentive / Disincentive Program
- Paid for out of the Medicare Trust Fund
- Asks for $1.3 billion over ten years
- Contains limited incentives and significant penalties
  - "Hospitals that fail to adopt **essential cybersecurity practices** face penalties of up to 100 percent of the annual market basket increase and beginning in FY 2031 potential additional penalties of up to 1 percent off the base payment."



CISA Rulemaking

- March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
- CISA issues proposed rule 3/27
- CISA - Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements
- CHIME comments here
- Cheat sheets
  - Condensed version here Technical version here
- Final rule by law fall 2025

Chevron Deference Decision

- Chevron deference principle and impact of Supreme Court decision in and *Loper Bright Enterprises v. Raimondo* on cyber regulations and guidance
- Chevron doctrine allowed courts to defer to federal agency interpretation of the law even when a reviewing court reads the statute differently.
- Impacting cyber regs

OCR Updates

- HIPAA Proposed Rule (forthcoming)
- HIPAA settlement concerning security violations and ransomware attack – 3rd one issued by OCR
- OCR / NIST HIPAA Security Conference – Oct. 24-25 – details here

Congressional Attention

- Ongoing and strong, bipartisan interest
- Unlikely to see cyber healthcare funding for providers this year
- Senate healthcare cybersecurity working group
  - Warner, Cassidy, Cornyn, and Hassan
- Multiple hearings on Change Healthcare attack
  - CHIME E&C testimony
  - CHIME timeline of federal action
- Crowdstrike House Homeland Committee hearing 9/24 contained many cyber questions
  - My LinkedIn post recapping hearing here

Bills in Play

- Both Senate HELP and Senate Finance committees are working on bills
  - Finance just released the Health Infrastructure Security and Accountability Act
  - Expect HELP to release draft bill text this fall
  - Senator Warner (D-VA) released bill on Medicare advanced payments in March - Health Care Cybersecurity Improvement Act of 2024
- Senate Homeland Security & Government Affairs Committee (HSGAC) has a bill
  - Healthcare Cybersecurity Act of 2024 (S. 4697) directs the CISA and HHS to collaborate on cybersecurity to improve the resiliency of healthcare and public health sector entities.
  - Press release
  - **Status:** the bill was reported favorably out of the Senate HSGAC on July 31st and is front of the full Senate for consideration.

How Bills Compare

Health Infrastructure Security and Accountability Act	Health Care Cybersecurity Improvement Act of 2024 (S. 4054)	**Healthcare Cybersecurity Act of 2024 (S. 4697)**	**Forthcoming**	**Forthcoming – maybe?**
Bi-partisan? NO	Bi-partisan? NO	Bi-partisan? YES	Bi-partisan??	Bi-partisan??
Finance Committee	Senator Warner (D-VA)	Senate Homeland Security	Senate HELP Bill	Multiple
- Repeals PL 116-321 - Incentives & penalties for hospitals - New HIPAA security requirements - Audits, reporting, fines & user fees	Makes receipt of Medicare advance payments for providers during a cyber attack contingent on use of cyber best practice	Directs the CISA and HHS to collaborate on cybersecurity to improve the resiliency of healthcare and public health sector entities.	Agency coordination and oversight, standards and support	Could be amalgamation of several bills

Health Infrastructure Security and Accountability Act

- Co-sponsored by Finance Chair Senator Wyden (D-OR) and Intelligence Chair / Finance member Senator Warner (D-VA)
- Changes HIPAA security requirements for all CEs / Bas
  - Rulemaking 18 months after bill's enactment
- Civil monetary penalties for failure to comply
- Mandatory risk assessments, stress tests and hiring auditors to gauge compliance
- User fees to support federal oversight
- Compliance attestations by CEO/CISO
- Hospitals incentives and penalties
  - $800 million (2027-28) for CAHs/ high-need hospitals to adopt essentials
  - $500 million (2029-30) for hospitals to adopt enhanced
  - Penalties start 2029

Cyber Donation Policies

- Permitted under Medicare Stark and Anti-kickback rules
- Underutilized
- Allows non-monetary donation of certain software and hardware to providers
- Donation of multi-purpose technology unless the primary function is related to cybersecurity
- No monetary contribution required of recipients
- No restrictions around who may make the contributions
- Fact sheets
  - OIG
  - CMS

Artificial Intelligence

- Strong nexus with cyber
  - Emerging threats and opportunities
- HHS AI Task Force charge includes:
  - "incorporation of safety, privacy, and security standards into the software-development lifecycle for protection of personally identifiable information, including measures to address AI-enhanced cybersecurity threats in the health and human services sector"
  - Within 1 year develop strategic plan that includes policies & frameworks – possibly including regulatory action, as appropriate – on responsible deployment and use of AI and AI-enabled technologies in sector, and identify appropriate guidance and resources to promote that deployment
- FDA paper on AI contains cyber components
  - "Artificial Intelligence and Medical Products: How CBER, CDER, CDRH, and OCP are Working Together"
- Congress still mulling options – security is among concerns

How is AI Impacting Cyberthreats?

Threat actors are using AI for both **designing** and **executing** attacks:

- Development of phishing e-mails
- Impersonation attacks
- Rapid exploitation of vulnerabilities
- Development of complex malware code
- Deeper target reconnaissance
- Automation of attacks
- Overwhelming human defenses
- Ransomware
  - Wider spread, more evasive

Image courtesy of MIT Technology Review.

Source: HHS HC3 Bulletin

CHIME AI Principles

- CHIME AI Principles
- Principle #8 focused on cyber
- Calls on HHS to develop use cases that focus on high-priority use cases including cyber
- Calls for Congress to offer cyber funding to providers

The Great Unknown

- Who will win the election?
- Will cyber mandates withstand Chevron?
- How will a Republican administration treat cyber mandates?
- Will Congress find cyber funding for healthcare providers?
- How another massive cyber attack could prompt policymakers?
- How quickly criminals can leverage and regularly use AI for gain?

Q&A

Upcoming Webinars

Sheppard Mullin webinar – The Inevitable Intrusion: A Legal Guide to Surviving Cyber Incidents | Oct 15 @ 1 pm CT

- Learn More & Register

ISMG Webinar – Building a More Resilient Healthcare Enterprise and Ecosystem | Oct 24 @ 1 pm ET

- Learn More & Register

Upcoming Industry Events

Nashville Healthcare Sessions | Oct 7-9 | Nashville, TN

- Clearwater is hosting a dynamic collaboration with cybersecurity experts from Jarrard for an exclusive live cybersecurity incident response simulation. Join us Tuesday, Oct 8 at 10:45 am.
- Learn More & Book a Meeting with Us

Virtual National Specialty Care Summit Session | Oct 10 @ 11:40 am CT

- Clearwater will lead a cybersecurity panel discussion during the First Virtual National Specialty Care Summit, which will be broadcast October 8-11. The session "Five Commonly Overlooked Cybersecurity Practices in Fast-Growth Specialty Groups" will be moderated by Steve Cagle.
- Learn More & Register

Virtual HCCA Clinical Practice Compliance Conference | Oct 15-16

- Melissa Andrews, Principal Consultant at Clearwater Privacy & Compliance is a featured speaker.
- **October 15:** "Auditing & Monitoring: It's Not Just for Privacy with Nicole Brown, Privacy Manager at City of Hope.
- **October 16:** "Congratulations You're a Compliance Officer! Things I Wish I Knew 10 Years Ago, 2 Years Ago, and Yesterday."
- Learn More & Register

HLTH | Oct 20 – 23 | Las Vegas, NV

- Clearwater is thrilled to be part of the ScaleHealth pavilion at the upcoming #HLTH conference in Las Vegas! Several of our Clearwater team members will be attending as well as Steve Cagle.
- Learn More & 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.

Got Questions?

Mari Savickis
CHIME
VP, Public Policy
mari.savickis@chimecentral.org

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

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.