Monthly Cyber Briefing

August 1, 2024

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A chat box.

Materials

Briefing materials will be provided after event.

Survey

Provide feedback via survey prompt at end of session.

Agenda & Speakers

- Cyber Update
- Preparing for New Cybersecurity Mandates: Insights for Healthcare Organizations

Jon Moore

Chief Risk Officer & SVP Consulting and Client Success
Clearwater

Steve Cagle

Chief Executive Officer

Clearwater

Clearwater

Cyber Update

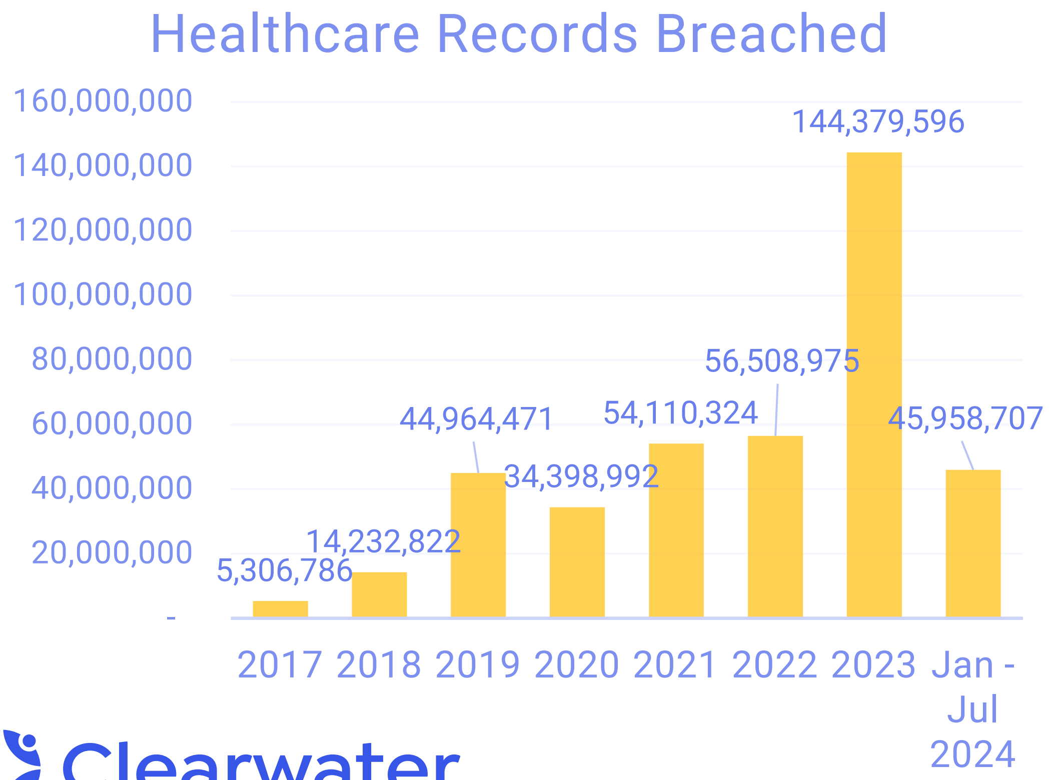
Steve Cagle

Clearwater

Breach Reports via OCR Breach Portal and Other Reports

OCR Breach Portal Data[1]

- 144.4M records reported breached in 2023, an increase of 156% vs 56.5 million in 2022
- 2024 – 46m records from 416 breaches reported vs 414 breaches reported in 2023 same period



Notable in OCR Breach Portal

- Includes "placeholder" reports from Change Healthcare (7/19) and Ascension (7/3) – each only listing 500 records – the minimum number that can be reported

Other Reported Breaches (not yet on OCR Portal)

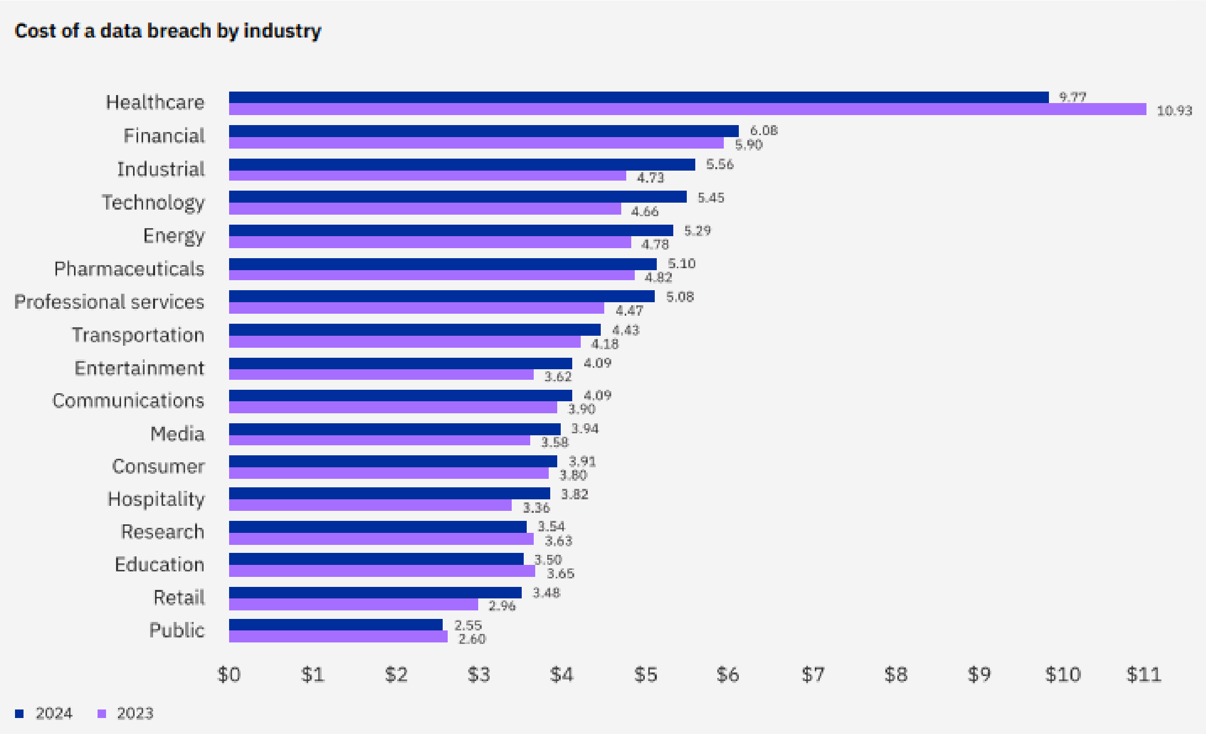
- HealthEquity reported breach of 4.3M records due compromised vendor account with access to a data repository[2]
- Rite Aid reported 2.2M records, claiming PII bit not ePHI. Attack claimed by RansomHub[3]

Clearwater

[1] HHS Breach Portal (2024 data through 7/29/24, pulled on 7/30/24)
[2] HealthEquity data breach could affect 4.3M | Healthcare Dive
[3] Rite Aid says June data breach impacts 2.2 million people (bleepingcomputer.com)

Annual Cost of Data Breach Report (Ponemon)

Cost of data breach across all industries rose 10% to $4.9M and in healthcare fell 10% to $9.8M, however this is still the highest among any industry at $9.8M and 2X the average cost.



Study period: March 2023 – February 2024

Data Source (IBM/Ponemon): Cost of a Data Breach Report 2024 (ibm.com)

Other Findings

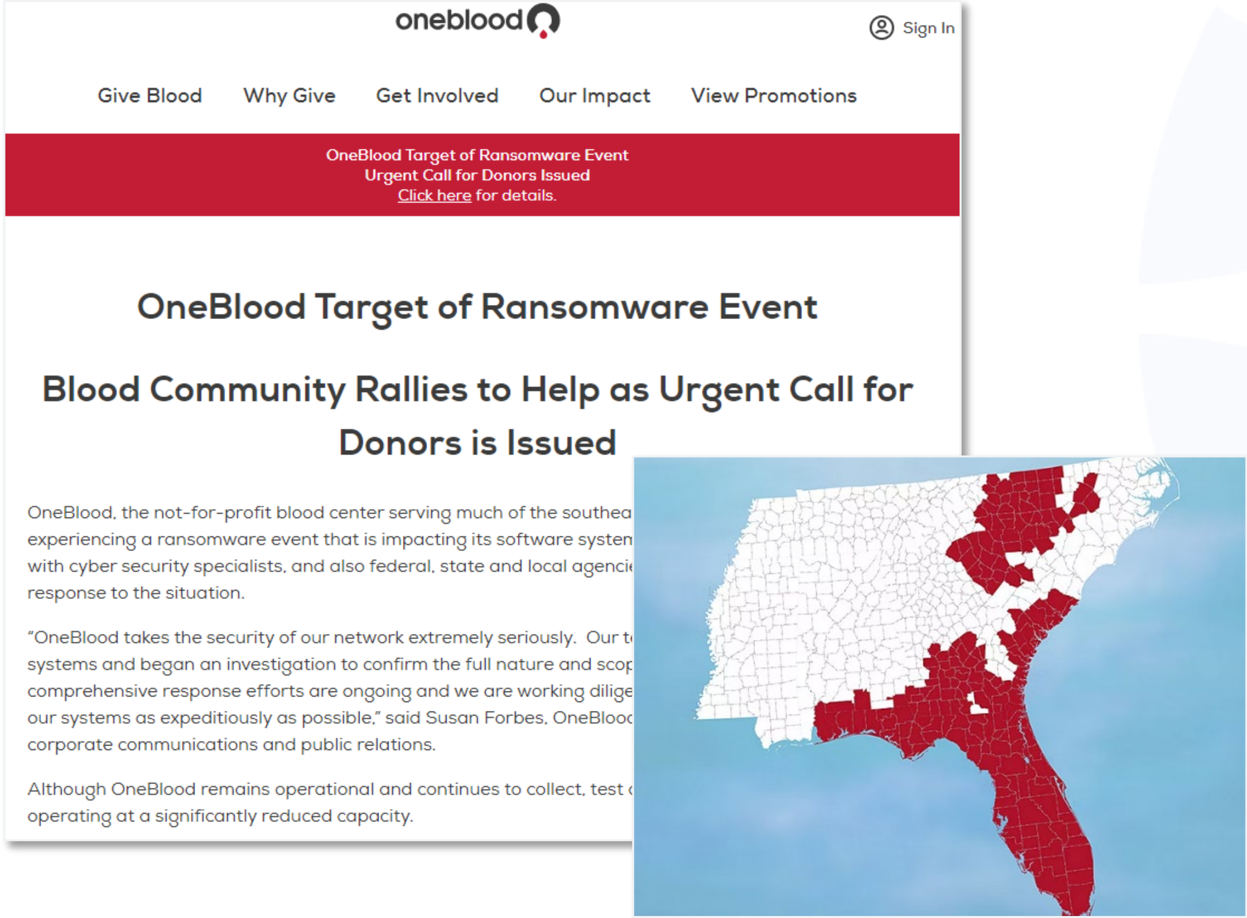
- For the 2nd year in a row, stolen or compromised credentials and phishing were the 2 most prevalent attack vectors (combined 31% of attacks)
- Half the breached organizations faced staffing and skills shortage
- 70% of organizations said the breach caused significant or very significant business disruption

Of Note

- Study did not include any breaches greater than 113,000 records. Mega data breaches of 1 million+ records treated separately **and saw costs of 9 times the global average.**

Potential Blood Shortage in Southeast due to Cyber Attack

Cyber attackers continue to attack high impact healthcare supply chain targets.



OneBlood Target of Ransomware Event
Urgent Call for Donors Issued
Click here for details.

OneBlood Target of Ransomware Event

Blood Community Rallies to Help as Urgent Call for Donors is Issued

OneBlood, the not-for-profit blood center serving much of the southea
experiencing a ransomware event that is impacting its software system
with cyber security specialists, and also federal, state and local agenci
response to the situation.

"OneBlood takes the security of our network extremely seriously. Our t
systems and began an investigation to confirm the full nature and scop
comprehensive response efforts are ongoing and we are working dilige
our systems as expeditiously as possible," said Susan Forbes, OneBlood
corporate communications and public relations.

Although OneBlood remains operational and continues to collect, test
operating at a significantly reduced capacity.

- Affects blood supply for 250 hospitals in Florida, Georgia, and the Carolinas
- OneBlood notified customers on 7/28 of potential shortages and delays
- This may be related to recent Microsoft-reported VMWare ESXi hypervisor CVE-2024-37085 (not confirmed)[1]
- H-ISAC Sector alert issued on Tuesday 7/30 of "IT Outage". Reported 7/31 due to cyberattack
- Reverting to manual procedures
- Hospitals advised to activate their critical blood shortage protocols

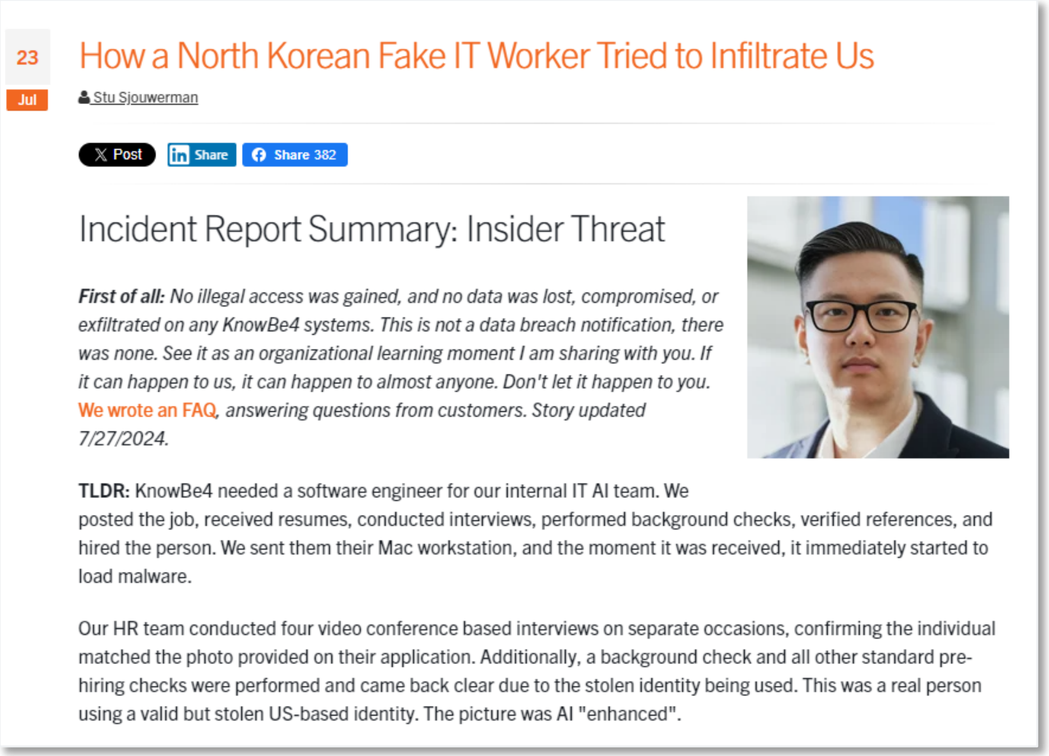
Clearwater

Ransomware Details | OneBlood

Microsoft Threat Intelligence: Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption | Microsoft Security Blog

North Korean Hacker Hired By Cyber Firm KnowBe4

Stolen credentials and an AI Enhanced photo enabled North Korean threat actor to trick HR.



How a North Korean Fake IT Worker Tried to Infiltrate Us

Stu Sjouwerman

Incident Report Summary: Insider Threat

First of all: *No illegal access was gained, and no data was lost, compromised, or exfiltrated on any KnowBe4 systems. This is not a data breach notification, there was none. See it as an organizational learning moment I am sharing with you. If it can happen to us, it can happen to almost anyone. Don't let it happen to you.* We wrote an FAQ, *answering questions from customers. Story updated 7/27/2024.*

TLDR: KnowBe4 needed a software engineer for our internal IT AI team. We posted the job, received resumes, conducted interviews, performed background checks, verified references, and hired the person. We sent them their Mac workstation, and the moment it was received, it immediately started to load malware.

Our HR team conducted four video conference based interviews on separate occasions, confirming the individual matched the photo provided on their application. Additionally, a background check and all other standard pre-hiring checks were performed and came back clear due to the stolen identity being used. This was a real person using a valid but stolen US-based identity. The picture was AI "enhanced".

- Used a valid identity that was stolen from a U.S.-based individual
- Employee passed background checks and verified resources
- Employee likely had his workstation connected "to an address that is basically an 'IT mule laptop farm"
- Security Operations Center team detected "a series of suspicious activities" from the new hire when he installed info stealing malware
- No data was stolen prior to removing access

Clearwater

How a North Korean Fake IT Worker Tried to Infiltrate Us (knowbe4.com)

Addressing Current Threat Environment

Specific recommendations related to content in this briefing

- Conduct risk analysis at the information system and component level
- Review security awareness training program, and assess whether more sophisticated testing is required
  - Is the cadence of testing appropriate?
  - How are you dealing with repeat offenders?
  - Are phishing tests customized to your company? Are you including, vishing, smishing?
  - How quickly are you providing training, and testing proficiency with new colleagues?
- Assess HR vetting process for hiring of new colleagues. E.g., personal and professional data consistency checks, reference checks via phone, address validation, on camera requirements
- Limit the amount of data vendors store, as well as their level of access
- Increase monitoring, detection and response capabilities
- Be aware of the TTPs of ransomware threat actors, particularly those that are specifically targeting healthcare and implement recommended mitigation and detection (refer to previous briefings)

Unpacking HHS's Latest Cybersecurity Performance Goals (CPGs)

Jon Moore, JD MS HCISPP

Clearwater

HHS's CPGs Fulfill Goal of HHS Healthcare Sector Cybersecurity Strategy

The Healthcare Sector Cybersecurity strategy provides an overview of HHS' proposed framework to help the healthcare sector address cybersecurity threats and protect patients.

HHS will take the following concurrent steps:

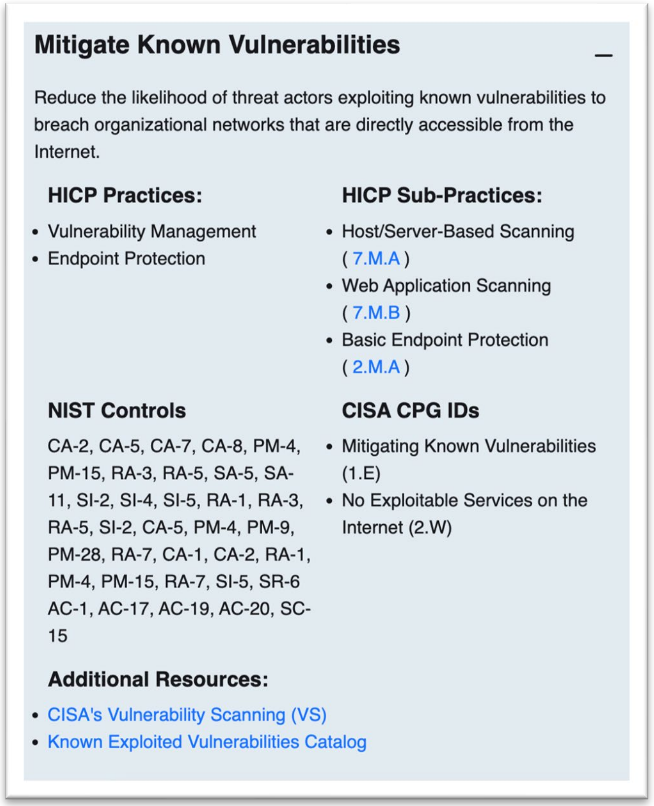
1. **Establish voluntary cybersecurity performance goals for the healthcare sector**
2. Provide resources to incentivize and implement these cybersecurity practices
3. Implement an HHS-wide strategy to support greater enforcement and accountability
4. Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity

"The Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (HPH CPGs) will help healthcare institutions prioritize implementation of high-impact cybersecurity practices. HPH CPGs will include both "essential" goals to outline minimum foundational practices for cybersecurity performance and "enhanced" goals to encourage adoption of more advanced practices."

Source: https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

HHS’s CPGs Align With Existing Frameworks

“Built off the chassis of CISA’s CPGs and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework, Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide, and the National Cybersecurity Strategy).”



Mitigate Known Vulnerabilities

Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.

HICP Practices:

- Vulnerability Management
- Endpoint Protection

HICP Sub-Practices:

- Host/Server-Based Scanning (7.M.A)
- Web Application Scanning (7.M.B)
- Basic Endpoint Protection (2.M.A)

NIST Controls

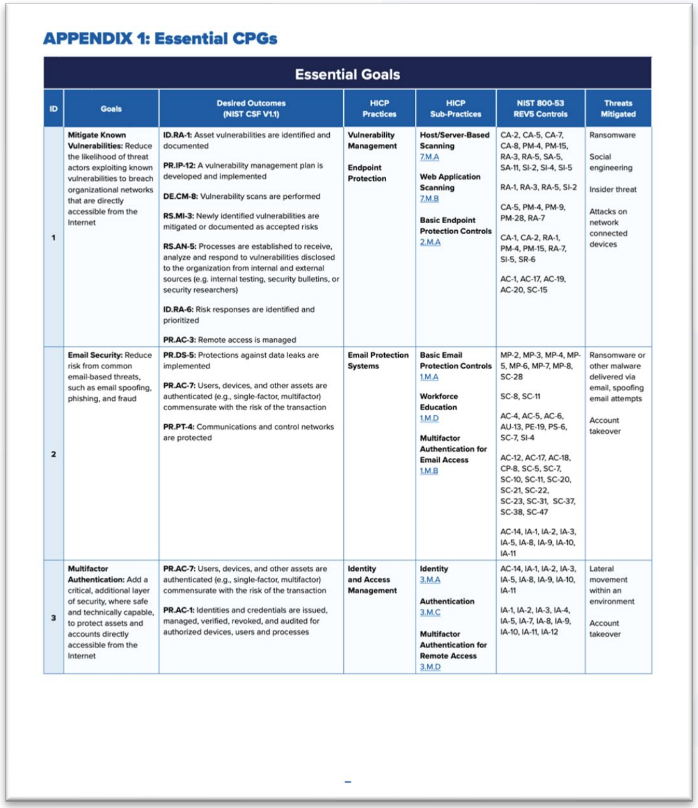
CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, RA-1, RA-3, RA-5, SI-2, CA-5, PM-4, PM-9, PM-28, RA-7, CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 AC-1, AC-17, AC-19, AC-20, SC-15

CISA CPG IDs

- Mitigating Known Vulnerabilities (1.E)
- No Exploitable Services on the Internet (2.W)

Additional Resources:

- CISA's Vulnerability Scanning (VS)
- Known Exploited Vulnerabilities Catalog



APPENDIX 1: Essential CPGs

Essential Goals						
ID	Goals	Desired Outcomes (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
1	**Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented **DE.CM-8:** Vulnerability scans are performed **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) **ID.RA-6:** Risk responses are identified and prioritized **PR.AC-3:** Remote access is managed	**Vulnerability Management** **Endpoint Protection**	**Host/Server-Based Scanning** 7.M.A **Web Application Scanning** 7.M.B **Basic Endpoint Protection Controls** 2.M.A	CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 RA-1, RA-3, RA-5, SI-2 CA-5, PM-4, PM-9, PM-28, RA-7 CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 AC-1, AC-17, AC-19, AC-20, SC-15	Ransomware Social engineering Insider threat Attacks on network connected devices
2	**Email Security:** Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud	**PR.DS-5:** Protections against data leaks are implemented **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction **PR.PT-4:** Communications and control networks are protected	**Email Protection Systems**	**Basic Email Protection Controls** 1.M.A **Workforce Education** 1.M.D **Multifactor Authentication for Email Access** 1.M.B	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28 SC-8, SC-11 AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4 AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47 AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11	Ransomware or other malware delivered via email, spoofing email attempts Account takeover
3	**Multifactor Authentication:** Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet	**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**Identity and Access Management**	**Identity** 3.M.A **Authentication** 3.M.C **Multifactor Authentication for Remote Access** 3.M.D	AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11 IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12	Lateral movement within an environment Account takeover

Each CPG is mapped to related HICP practices and sub-practices, CISA CPGs, NIST CSF Subcategories, and NIST 800-53 Controls.

Sources:

- *https://www.cisa.gov/cross-sector-cybersecurity-performance-goals*
- *https://hphcyber.hhs.gov/performance-goals.html*
- *https://hphcyber.hhs.gov/documents/cybersecurity-performance-goals.pdf*

HHS's CPGs include Essential and Enhanced Goals

These CPGs are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizations in particular, can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety.

Essential Goals

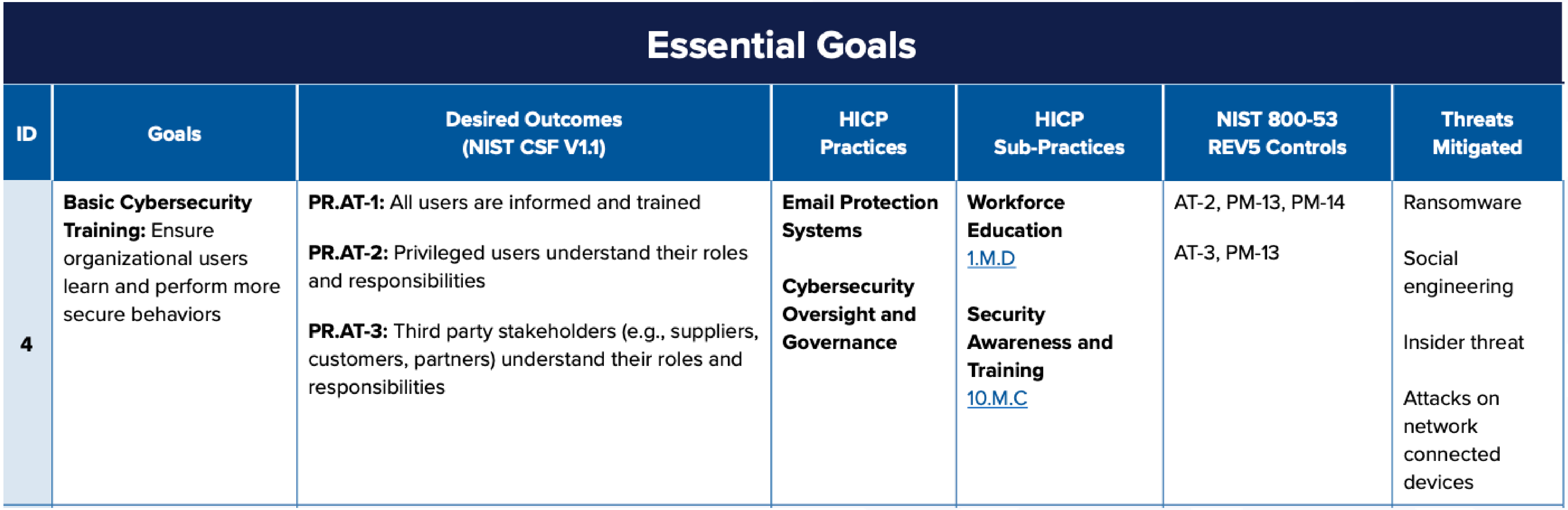
To help healthcare organizations address common vulnerabilities by setting **a floor of safeguards** that will better protect them from cyber attacks, improve response when events occur, and minimize residual risk.

Enhanced Goals

To help healthcare organizations **mature their cybersecurity capabilities** and reach the next level of defense needed to protect against additional attack vectors.

HHS Provides Goal Statements and Mappings

HHS' Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals document includes statement of the goal and mappings to NIST CSF 1.1, HICP Practices and Sub-Practices, NIST 800-53 Rev 5 and mitigated threats.



Essential Goals

ID	Goals	Desired Outcomes (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
4	**Basic Cybersecurity Training:** Ensure organizational users learn and perform more secure behaviors	**PR.AT-1:** All users are informed and trained **PR.AT-2:** Privileged users understand their roles and responsibilities **PR.AT-3:** Third party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**Email Protection Systems** **Cybersecurity Oversight and Governance**	**Workforce Education** 1.M.D **Security Awareness and Training** 10.M.C	AT-2, PM-13, PM-14 AT-3, PM-13	Ransomware Social engineering Insider threat Attacks on network connected devices

Source: https://hphcyber.hhs.gov/documents/cybersecurity-performance-goals.pdf

Clearwater

HHS CPG Essential Goals 1 - 5

Essential Goals	Goal Statement
Mitigate Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.
Email Security	Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud.
Multifactor Authentication	Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet
Basic Cybersecurity Training	Ensure organizational users learn and perform more secure behaviors.
Strong Encryption	Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion.

HHS CPG Essential Goals 6 – 10

Essential Goals	Goal Statement
Revoke Credentials	Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly.
Basic Incident planning and Preparedness	Ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents.
Unique Credentials	Use unique credentials inside organizations’ networks to detect anomalous activity and prevent attackers from moving laterally across the organization, particularly between IT and OT networks.
Separating User and Privileged Accounts	Establish secondary accounts to prevent threat actors from accessing privileged or administrative accounts when common user accounts are compromised.
Vendor/Supplier Cybersecurity Requirements	Identify, assess, and mitigate risks associated with third party products and services.

HHS CPG Enhanced Goals 1 – 5

Enhanced Goals	Goal Statement
Asset Inventory	Identify known, unknown (shadow), and unmanaged assets to more rapidly detect and respond to potential risks and vulnerabilities.
Third Party Vulnerability Disclosure	Establish processes to promptly discover and respond to known threats and vulnerabilities in assets provided by vendors and service providers.
Third Party Incident Reporting	Establish processes to promptly discover and respond to known security incidents or breaches across vendors and service providers.
Cybersecurity Testing	Establish processes to promptly discover and responsibly share vulnerabilities in assets discovered through penetration testing and attack simulations.
Cybersecurity Mitigation	Establish processes internally to act quickly on prioritized vulnerabilities discovered through penetration testing and attack simulations.

HHS CPG Enhanced Goals 6 - 10

Enhanced Goals	Goal Statement
How to Respond to Relevant Threats	Ensure organizational awareness of and ability to detect relevant threats and TTPs at endpoints. Ensure organizations are able to secure entry and exit points to its network with endpoint protection.
Network Segmentation	Mission critical assets are separated into discrete network segments to minimize lateral movement by threat actors after initial compromise.
Centralized Log Collection	Collection of necessary telemetry from security log data sources within an organization’s network that maximizes visibility, cost effectiveness, and faster response to incidents.
Centralized Incident Planning and Preparedness	Ensure organizations consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios.
Configuration Management	Define secure device and system settings in a consistent manner and maintain them according to established baselines.

The Future for HHS's CPGs

There is currently significant chatter out of Washington that the HHS CPGs will become mandatory for organizations participating in Medicare and Medicaid.

HIPAA Security Rule

It is anticipated that these CPGs will become mandatory through an amendment of the HIPAA Security Rule. It is currently anticipated that amendments to the HIPAA Security Rule, including new cybersecurity requirements, will be implemented in September 2024, but that deadline may be extended.

Promoting Interoperability Program

CMS will also likely propose new cybersecurity requirements for hospitals through Medicare and Medicaid in the form of Medicare or Medicaid conditions of participation or as part of the Medicare Promoting Interoperability Program. It is currently unknown when CMS will begin the rulemaking and comment process for proposed enforceable cybersecurity requirements.

Source: https://www.jdsupra.com/legalnews/hhs-cybersecurity-performance-goals-and-4688203/

Biden's FY 2025 Budget Includes Proposed Funding and Penalties

FY 2025

Biden Administration's FY 2025 Budget in Brief, released in March 2024, in which the administration proposed to establish "essential" and "enhanced" incentive structures to encourage hospitals, if applicable, to upgrade their cybersecurity practices. HHS also proposed penalties for certain hospitals that fail to implement "essential" and "enhanced" cybersecurity practice standards.

Source: https://natlawreview.com/article/hhs-health-care-cybersecurity-performance-goals-proposed-incentives-penalties-and

FY 2027-28

FY 2027 and FY 2028, HHS would transfer $800 million from the Medicare Hospital Insurance Trust Fund to approximately 2,000 high-needs hospitals that would be used to implement "essential" cybersecurity practice standards. In connection with hospitals' participation in the Promoting Interoperability Program, acute care hospitals that do not adopt essential cybersecurity practices would be responsible for penalties.

FY 2029-30

During FY 2029 and FY 2030, HHS would transfer $500 million from the Medicare Hospital Insurance Trust Fund to all hospitals to implement "enhanced" cybersecurity practices. CMS has the opportunity to transition the "enhanced" cybersecurity practice standards to being required under the Promoting Interoperability Program as of FY 2031, and hospitals that do not adopt CMS-chosen enhanced cybersecurity practices would be responsible for penalties.

Small Organizations Will Need to Do More to Achieve the CPGs

The CPGs align to primarily the Health Industry Cybersecurity Practices recommended for Medium and, in some cases, Large organizations.

Essential CPG	HICP Reference
Mitigate Known Vulnerabilities	7.M.A, 7.M.B, 2.M.A
Email Security	1.M.A, 1.M.D, 1.M.B
Multifactor Authentication	3.M.A, 3.M.C, 3.M.D
Basic Cybersecurity Training	1.M.D, 10.M.C
Strong Encryption	1.M.C, 2.M.A, 4.M.C
Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers	3.M.B, 3.M.C
Basic Incident Planning and Preparedness	8.M.B, 10.M.A, 4.M.D
Unique Credentials	3.M.A, 3.M.B, 3.M.C, 3.M.D
Separate User and Privileged Accounts	3.M.A, 3.M.B, 3.M.C, 3.M.D
Vendor/Supplier Cybersecurity Requirements	10.M.B

Enhanced CPG	HICP Reference
Asset Inventory	5.M.A, 5.M.B, 5.M.C, 7.M.C
Third Party Vulnerability Disclosure	10.M.B
Third Party Incident Reporting	10.M.B, 7.M.D, 8.M.C
Cybersecurity Testing	7.L.A, 7.L.C, 8.M.C
Cybersecurity Mitigation	8.M.C, 7.M.D, 7.L.B
Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures	2.L.C
Network Segmentation	6.M.B
Centralized log Collection	8.M.A, 8.M.B
Centralized Incident Planning and Preparedness	8.M.A, 8.M.B
Configuration Management	7.M.D

Raises the Question of What Achieving a Goal Means and What Might be Required to Demonstrate It

If the Cybersecurity Performance Goals become something more than voluntary for at least a portion of the healthcare industry, how will they be enforced, by whom, and what will be required to demonstrate achievement of each goal?

Enforcement

- Will they be enforced by OCR as part of HIPAA and if so, will it only be because of an audit or investigation?
- Will the HIPAA Audit protocol also receive an update?
- If part of Promoting Interoperability will CMS require an attestation similar to what they do with Risk Analysis?
- HHS Strategy calls for greater enforcement and accountability.

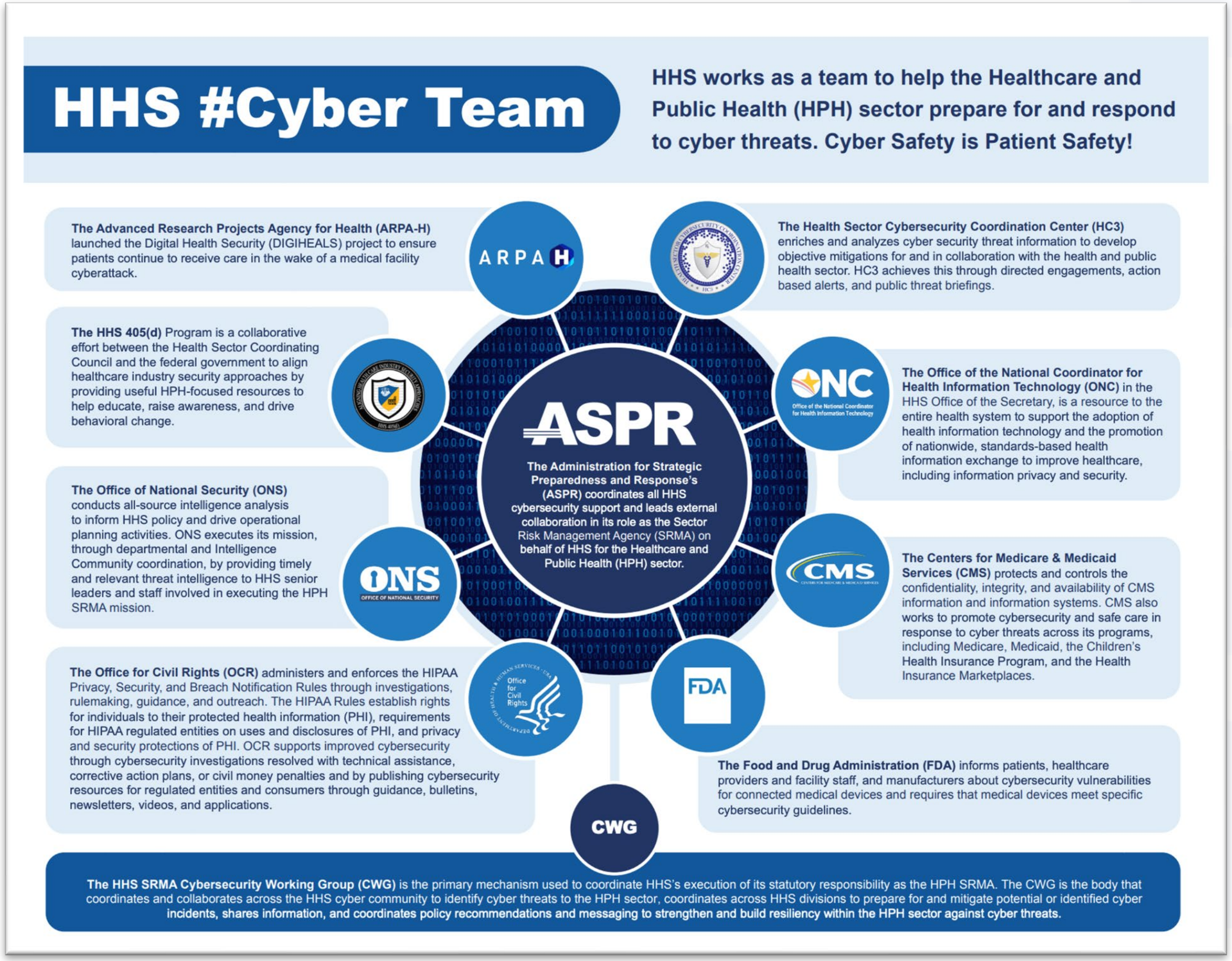
Compliance

- What evidence can and should be provided to demonstrate goal achieved?
- Will it be the same for all organizations regardless of size and segment?
- How will small healthcare organizations fund be coming compliant?
- HHS Strategy calls for resources to incentivize implementation of cybersecurity practices.

Penalties

- Will the proposed penalties see adoption?
- What about requirements for business associates?
- Will the CPGs be irrelevant by the time they are required?

The Federal Healthcare Cybersecurity Ecosystem is Growing


ARPA H
ASPR
ONC
Office of the National Coordinator for Health Information Technology
ONS
OFFICE OF NATIONAL SECURITY
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
FDA
Office for Civil Rights
CWG

HHS #Cyber Team

HHS works as a team to help the Healthcare and Public Health (HPH) sector prepare for and respond to cyber threats. Cyber Safety is Patient Safety!

The Administration for Strategic Preparedness and Response's (ASPR) coordinates all HHS cybersecurity support and leads external collaboration in its role as the Sector Risk Management Agency (SRMA) on behalf of HHS for the Healthcare and Public Health (HPH) sector.

The Advanced Research Projects Agency for Health (ARPA-H) launched the Digital Health Security (DIGIHEALS) project to ensure patients continue to receive care in the wake of a medical facility cyberattack.

The HHS 405(d) Program is a collaborative effort between the Health Sector Coordinating Council and the federal government to align healthcare industry security approaches by providing useful HPH-focused resources to help educate, raise awareness, and drive behavioral change.

The Office of National Security (ONS) conducts all-source intelligence analysis to inform HHS policy and drive operational planning activities. ONS executes its mission, through departmental and Intelligence Community coordination, by providing timely and relevant threat intelligence to HHS senior leaders and staff involved in executing the HPH SRMA mission.

The Office for Civil Rights (OCR) administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules through investigations, rulemaking, guidance, and outreach. The HIPAA Rules establish rights for individuals to their protected health information (PHI), requirements for HIPAA regulated entities on uses and disclosures of PHI, and privacy and security protections of PHI. OCR supports improved cybersecurity through cybersecurity investigations resolved with technical assistance, corrective action plans, or civil money penalties and by publishing cybersecurity resources for regulated entities and consumers through guidance, bulletins, newsletters, videos, and applications.

The Health Sector Cybersecurity Coordination Center (HC3) enriches and analyzes cyber security threat information to develop objective mitigations for and in collaboration with the health and public health sector. HC3 achieves this through directed engagements, action based alerts, and public threat briefings.

The Office of the National Coordinator for Health Information Technology (ONC) in the HHS Office of the Secretary, is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide, standards-based health information exchange to improve healthcare, including information privacy and security.

The Centers for Medicare & Medicaid Services (CMS) protects and controls the confidentiality, integrity, and availability of CMS information and information systems. CMS also works to promote cybersecurity and safe care in response to cyber threats across its programs, including Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplaces.

The Food and Drug Administration (FDA) informs patients, healthcare providers and facility staff, and manufacturers about cybersecurity vulnerabilities for connected medical devices and requires that medical devices meet specific cybersecurity guidelines.

The HHS SRMA Cybersecurity Working Group (CWG) is the primary mechanism used to coordinate HHS's execution of its statutory responsibility as the HPH SRMA. The CWG is the body that coordinates and collaborates across the HHS cyber community to identify cyber threats to the HPH sector, coordinates across HHS divisions to prepare for and mitigate potential or identified cyber **incidents, shares information, and coordinates policy recommendations and messaging to strengthen and build resiliency within the HPH sector against cyber threats.**

The Federal Healthcare Cybersecurity Ecosystem is growing quickly and extends well beyond the requirements of HIPAA and enforcement from OCR.

Source: https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

Q&A

Upcoming Webinars

OCR-Quality® Risk Analysis Working Lab 2024: Beginning August 7th @ 11:00 am CT

Register here

Making the Move to Proactive Patient Privacy Monitoring | September 10 @ 12:00 CST

Register here

OCR-Quality® Risk Response Working Lab 2024: Beginning September 18th @ 11:00am CT

Register here

Upcoming Industry Events

September 17, 2024

Compliance Auditing & Monitoring Conference

Virtual, Central Time (CT)

SCCE Compliance Auditing & Monitoring Conference | September 17, 2024

Healthtech Leader 3.0

SEP 27 - 29, 2023 | CLEVELAND, OH
Hosted by Cleveland Clinic

Breaking down silos to enhance care delivery through technology, security, data and analytics

REGISTER TODAY >

Healthtech Leader 3.0 | September 18-20, 2024

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.