The 405(d) Advantage: What Healthcare Leaders Should Know

July 18, 2024

Clearwater

Logistics

- All attendees in “Listen Only Mode”
- Please ask content-related questions in Q&A
- Recording, final slides, and resources shared within 24 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Today’s Experts

Lisa Munro

Program Engagement Lead,
HHS 405(d)

- Over 10 years in strategic communications and program development for government and private sector clients.
- Specializes in developing and implementing marketing and communication plans, stakeholder engagement, and content creation.
- Expertise leading initiatives for the U.S. Department of Health and Human Services, managing cybersecurity awareness programs, and creating branding strategies for government agencies and private sector clients.
- Specializes in digital campaigns, conference strategies, and legislative communications, with a focus on enhancing visibility and driving behavioral change in cybersecurity practices.

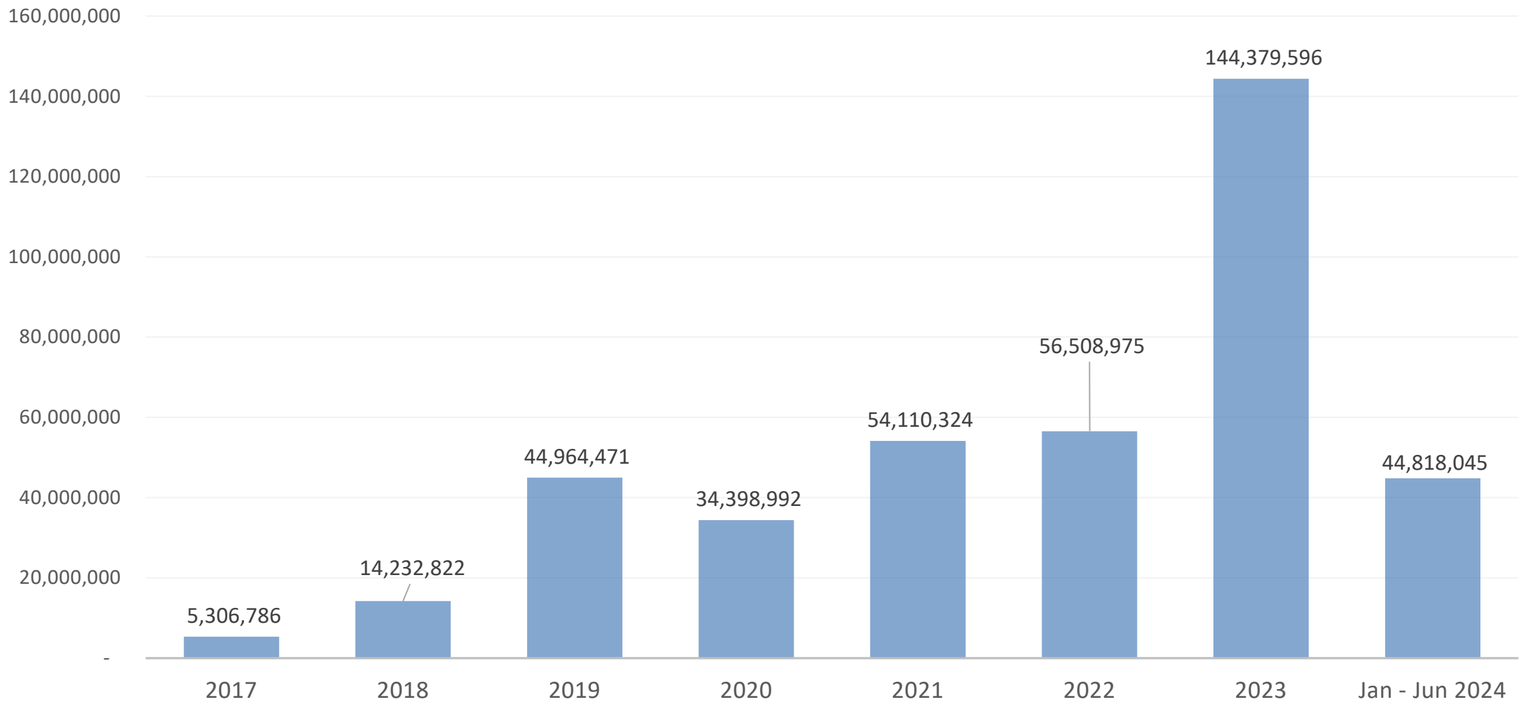
Steve Cagle

CEO, Clearwater

- 20 years growing and scaling private equity-backed healthcare companies
- 15 years B2B Software & Consulting Services
- 10 years OTC, Rx pharmaceutical
- Former CEO for Moberg Pharma North America, a subsidiary of Moberg Pharma AB (OMX:MOB)
- Former CEO of Alterna LLC
- Former Founding member and VP of Product Management & Marketing of Sparta Systems, Inc.
- Board of Directors of CMP Pharma Inc.

Threats to Healthcare Continue to Grow

Healthcare Records Breached



[1]HHS Breach Portal (data for 2023 pulled March 21, data for 2024 pulled July 3, 2024).

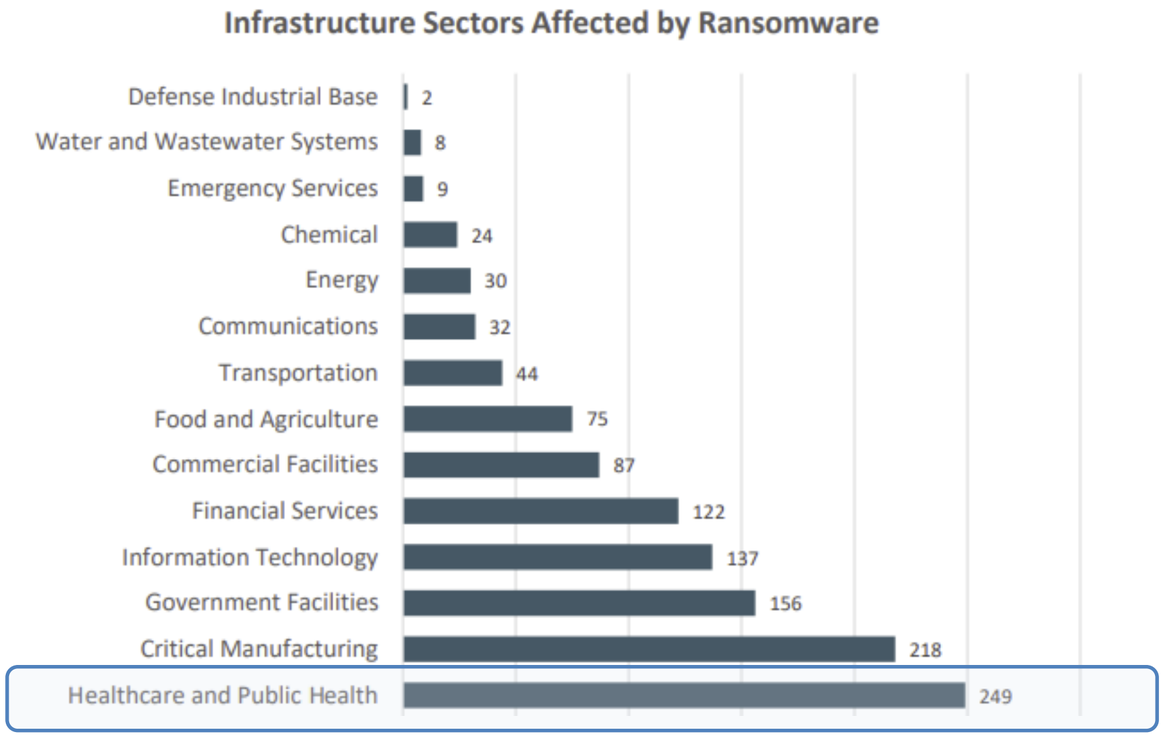
12% decrease in the number of records breached first 6 months 2023; however, increase of 7% in number of breaches reported

Key factors include:

- Growing attack surface
- Highly valuable data
- Highly targeted
- Low level of maturity
- Limited resources

Clearwater

Ransomware Threat Continues to Increase

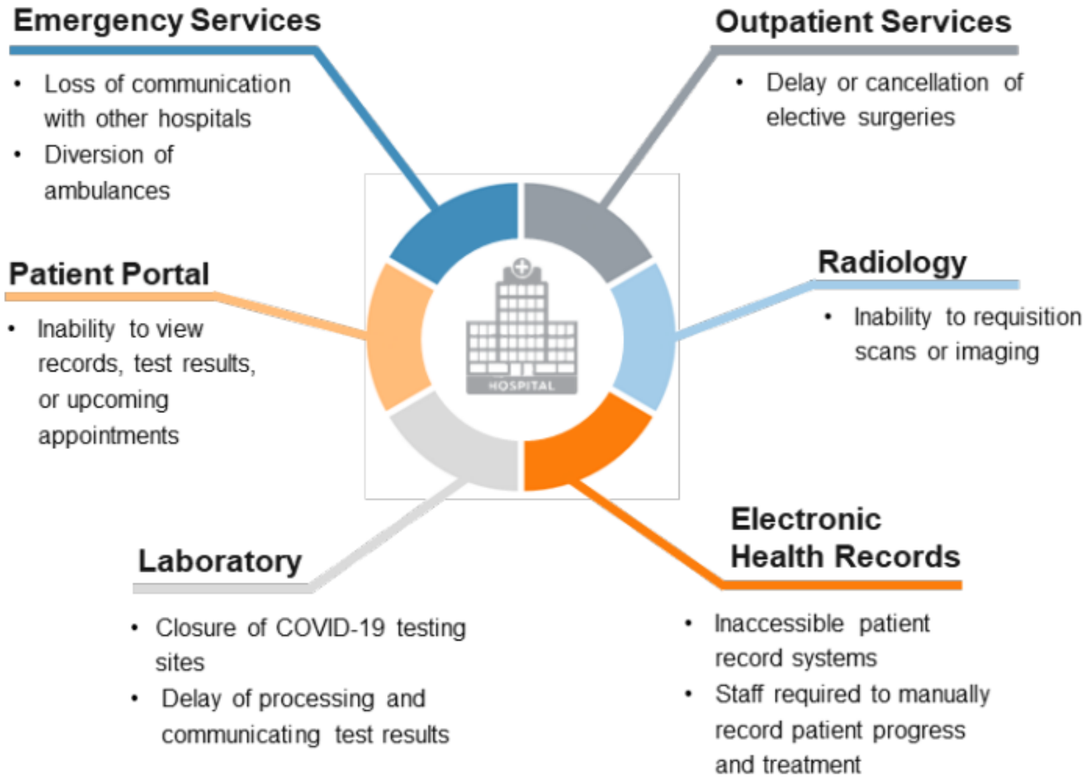


- 95% increase in ransomware in 2023[1]
- 13% Increase in Insurance Claims – increase primarily driven by ransomware 2023[2]
- Healthcare is the most targeted critical infrastructure industry by ransomware gangs[3]
- Total losses from internet crime increased in the U.S. by 22% in 2023 to $12.5 Billion[3]
- 20% increase in reported victims in Q1 2024 vs Q1 2023[4]

[1] *At Least 141 Were Hospitals Directly Affected by Ransomware Attacks in 2023 (hipaajournal.com)*
[2] *Ransomware triggers cyberinsurance claims increase | SC Media (scmagazine.com)*
[3] *2023 FBI Internet Crime Report.pdf*
[4] *GuidePoint Security Q1 2024 Ransomware Report*

Clearwater

Cybersecurity Is Patient Safety



2021: CISA reported ransomware causes, worsened health outcomes as measured in **excess deaths** due to disruption.[1]

2022: Of all providers who had a **ransomware** attack, **22% reported increased in mortality rates** following the attack.[2]

2023: JAMA study found hospitals adjacent to others affected by ransomware attacks may see disruptions in patient care and **risks to increased mortality**.[3]

2023: FBI and DOJ now treating patient cyber-attacks as "**threat to life**" crimes.[4]

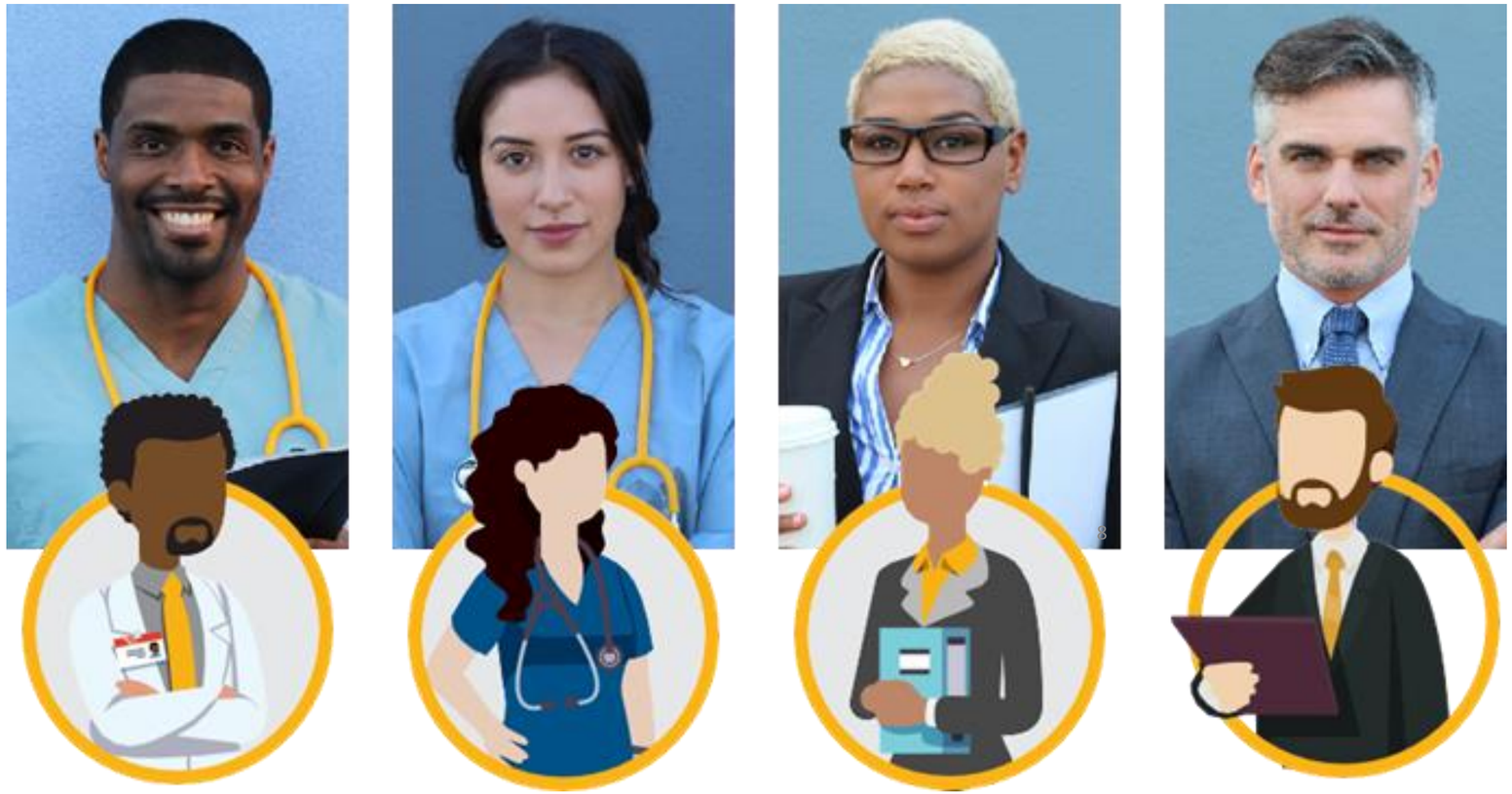
1 CISA Insights Report: Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm
2 Cyberattacks against U.S. hospitals mean higher mortality rates, study finds (nbcnews.com)
3 Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US | Emergency Medicine | JAMA Network Open | JAMA Network (UC San Diego study pre and post Scripps Health ransomware attack published in JAMA).
4 *"Hospital Resiliency Landscape Analysis." Healthcare and Public Health Sector Coordinating Council, Office for Civil Rights, Centers for Medicare and Medicaid Services, and HHS 405(d) Working Group. Joint Publication. March 2023."*

Clearwater

What We Do & Who We Are

The HHS 405(d) Program is a collaborative effort between The Health Sector Coordinating Council and the federal government to align healthcare industry security practices. The 405(d) Program is focused on providing organizations across the nation with useful and impactful Healthcare and Public Health (HPH) focused resources, products, and tools that help educate, raise awareness, and provide vetted cybersecurity best practices which drive behavioral change and strengthen the sector's cybersecurity posture against cyber threats.

405(d) Task Group



The core of the 405(d) program is it's task group members. Convened by HHS in 2017, the 405(d) task group is comprised of over 230 + information security officers, medical professionals, privacy experts, and industry leaders.

The task group members help drive all aspects of the 405(d) program, to include official program products, awareness campaigns, engagements, and outreach channels.

The task group is actively collaborating and working on a host of new resources for the sector including an update to the HICP publication and a new ERM Cybersecurity publication both of which are planned to be released in 2022/early 2023

A Brief History of 405(d)

2015

Founding Law

Cybersecurity Act of 2015 (CSA) calls upon HHS to work with industry to Align Health Care Industry Security Approaches

2017

Task Group Formed

HHS in partnership with the Health Sector Coordinating Council establish the 405(d) Task Group. The Task Group begins to develop a "best practices" publication

2018

HICP Release

After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group developed and released the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

2019

Outreach and Engagement Begins

HHS builds a federal program around the 405(d) Task Group, with a focus on HPH cyber outreach and engagement

2021

PL 116-321 (HITECH Amendment) Passes

To amend the Health Information Technology for Economic and Clinical Health Act (HITECH) to require the Secretary of Health and Human Services (HHS) to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

2023

Product Expansion and Knowledge on Demand

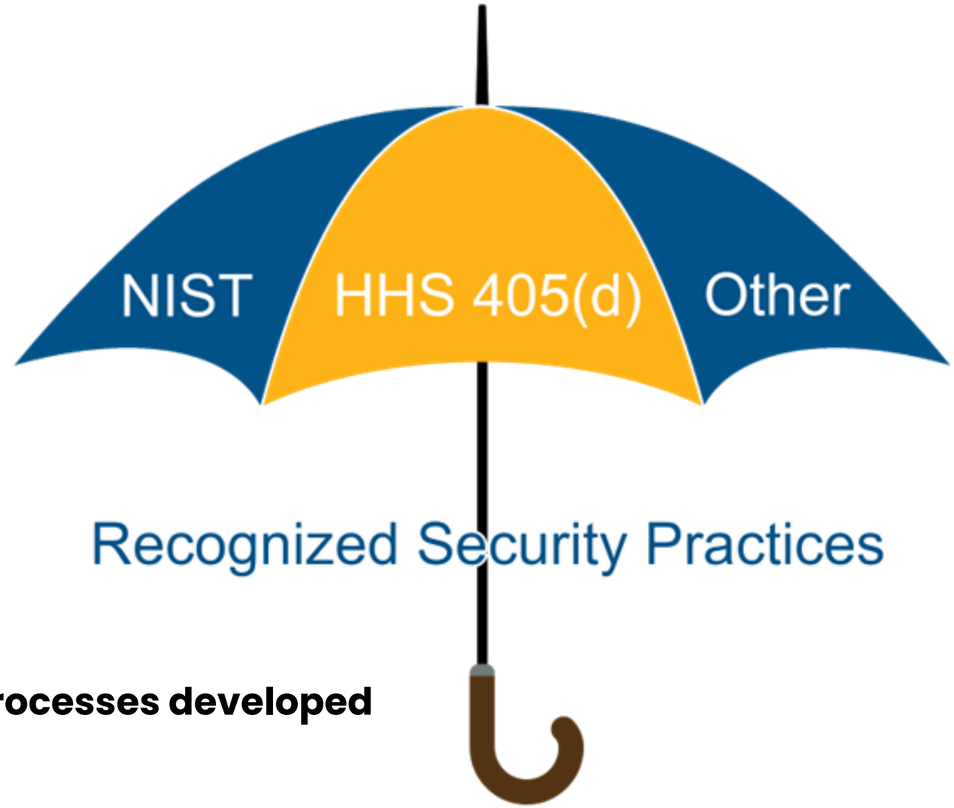
HHS 405(d) Program releases HICP 2023 Edition, Hospital Cybersecurity Landscape Analysis, and Knowledge on Demand Education Platform. Over the years the 405(d) Program has developed and released 210 products for the sector to continue to leverage.

2021 HITECH Amendment

H.R.7898 — 116th Congress (2019-2020)

To amend the Health Information Technology for Economic and Clinical Health Act (HITECH) to require the Secretary of Health and Human Services (HHS) to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

Signed January 5, 2021 | Public Law No: 116-321



What are Recognized Security Practices?

The standards, guidelines, best practices, methodologies, procedures, and processes developed under the:

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**
- **HHS 405(d) Program approaches**
- **Other programs and processes that address cybersecurity and are developed, recognized, or promulgated through regulations under other statutory authorities**

Health Industry Cybersecurity Practices Publication 2023 Edition

11

HICP 2023 Edition

405(d)'s Cornerstone Publication

Cybersecurity threats evolve each year and with them comes new mitigating practices. The HICP 2023 Edition has been updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate the current cybersecurity threats the HPH sector is facing. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

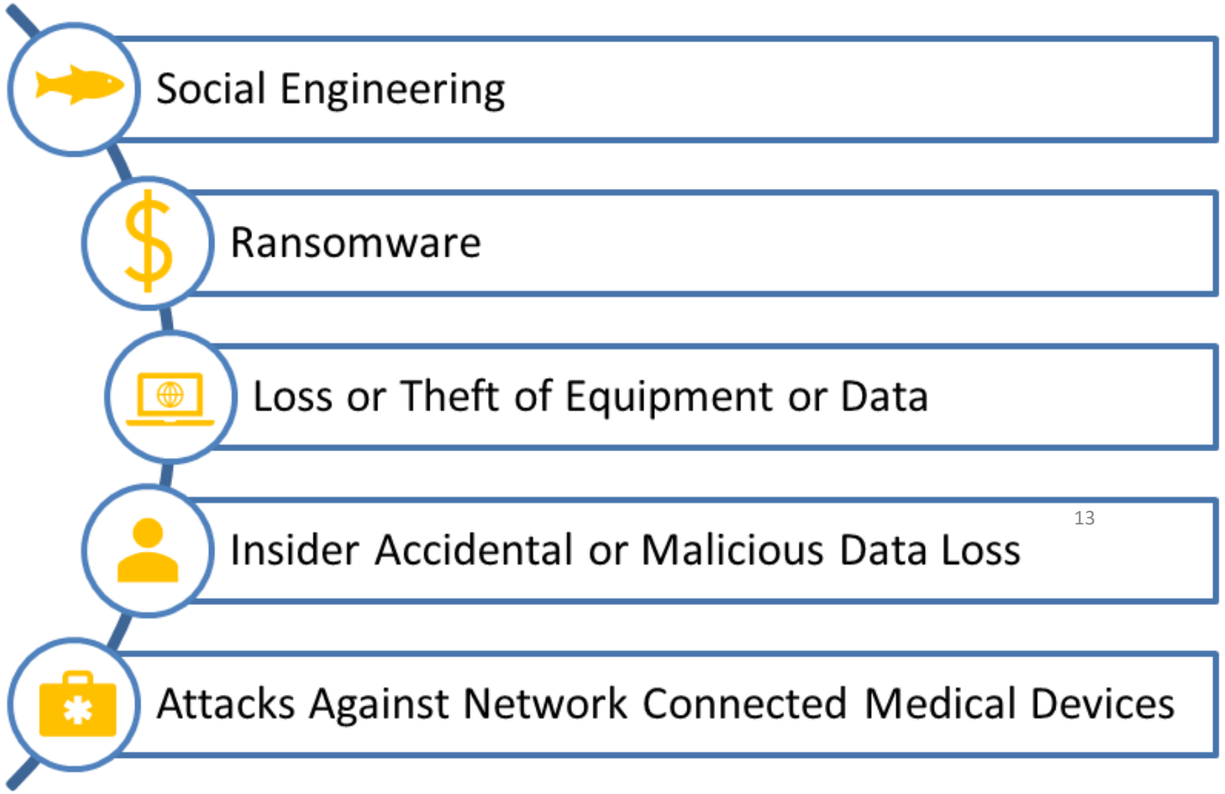
The **Main Document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.

12

Top 5 Cybersecurity Threats and 10 Mitigating Practices



1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

What's New in HICP 2023

Main Document Updates

The HICP Main Document has been updated to renew our call to action to maintain patient safety and includes new cybersecurity strategies such as Zero Trust and Defense in Depth.

Email Phishing is now Social Engineering

Top Ten Practices Updates

Cybersecurity Practice #9 on Network

Connected Medical Devices has been fully updated 14

Cyber Practice #10 is now Cybersecurity Oversight and Governances

Additional NEW Sub-Practices

Cyber insurance

Cybersecurity Risk Assessment and Management

Attack Simulations

Medical Devices (Major Updates)

Benefits of 405(d) HICP

405(d) HICP fosters awareness, helps prioritize cybersecurity practices, and moves towards consistency within the HPH sector in mitigating the current most impactful cybersecurity threats.

Starting point for implementing basic cybersecurity practices	Communicates to threats to the organization and helps establish goals.	Practices are aligned to the top 5 threats facing the healthcare sector.
Flexible to meet the needs and resources of different size organizations.	Can demonstrate recognized security practices are implemented.	Maps to other established frameworks and requirements.

Use Cases: Healthcare Organizations

Clearwater recommends 405(d) HICP and leverages it in many ways to support its healthcare clients to become more secure and resilient.

	Assess	Build	Mature
Use Case	… your cybersecurity practices to determine if they are reasonable and appropriate for the size of your healthcare organization	… a baseline cybersecurity program that prioritizes implementation of 405(d) practices	… a common minimum cybersecurity standard for independently managed business units, companies, service lines, etc.
Typical Orgs.	Hospitals, medium – large healthcare providers and business associates	Small – medium healthcare providers, digital health companies, service providers, healthcare divisions of larger companies	Private equity firms measuring portcos, Integrated Delivery Networks

Clearwater

Top 10 Practices & Sub-practices Aligned to Size

Top 10 practices, and example of variation between the small, medium & large.

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Security Operations Center and Incident Response
9. Network Connected Medical Devices
10. Cybersecurity Oversight and Governance

Small Organization	
Cybersecurity Practice	Sub-Practice
1: Email Protection Systems	**1.S.A** Email System Configuration **1.S.B** Education **1.S.C** Phishing Simulation

Medium Organization	
Cybersecurity Practice	Sub-Practice
1: Email Protection Systems	**1.M.A** Basic Email Protection Controls **1.M.B** Multifactor Authentication for Remote Access **1.M.C** Email Encryption **1.M.D** Workforce Education

Large Organization	
Cybersecurity Practice	Sub-Practice
1: Email Protection Systems	**1.L.A** Advanced and Next-Generation Tooling **1.L.B** Digital Signatures **1.L.C** Analytics Driven Education

Clearwater

Hospital Cyber Resiliency Initiative Landscape Analysis 2023

Landscape Overview

Executive Summary

Overview of key observations, HICP Practice Adoption and a note on Data sources

Capabilities and Performance Assessment

Covers staff analysis, cyber expense, coverage to NIST and HICP

Threat Analysis

Overview of the evolving threat of ransomware and links between threats and mitigations

Adoption of HICP Practices

Covers practices in HICP that have significant progress, need improvement, and need additional research, and non urgent items

Adoption of HICP Practices

No Action Required – Significant Progress Made

- Email protection systems

Urgent Improvement Needed

- Endpoint protection systems
- Access management
- Network management
- Vulnerability management
- Incident response

Additional Research Required

- Asset management
- Medical device security
- Cybersecurity policies

Further Attention Recommended – Not Urgent

- Data protection and loss prevention

HPH Cybersecurity Performance Goals

The Department of Health and Human Services (HHS) helps the Healthcare and Public Health (HPH) critical infrastructure sector prepare for and respond to cyber threats, adapt to the evolving threat landscape, and build a more resilient sector. As outlined in the HHS Healthcare Sector Cybersecurity concept paper, HHS is publishing these voluntary healthcare specific Cybersecurity Performance Goals (CPGs) to help healthcare organizations prioritize implementation of high-impact cybersecurity practices.

About HPH CPGs

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. They were built off the chassis of CISA's CPGs and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as identified in the 2023 Hospital Cyber Resiliency Landscape Analysis.

HPH Cybersecurity Performance Goals

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.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Expand All *Collapse All*

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 CPGs

- Mitigating K… …lnerabilities (1.E)
- No Exploita… …ces on the Internet (2.…)

Additional Resources:

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

Enhanced Goals

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

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Expand All *Collapse All*

Asset Inventory

Identify known, unknown (shadow), and unmanaged assets to more rapidly detect and respond to new vulnerabilities.

HICP Practices:

- IT Asset Management

HICP Sub-Practices:

- Inventory of Endpoints and Servers (5.M.A)
- Procurement (5.M.B)
- Secure Storage for Inactive Devices (5.M.C)
- System Placement and Data Classification (7.M.C)

NIST Controls

CM-8, PM-5, CM-8, AC-20, PM-5, SA-9, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

CISA CPG IDs

- Asset Inventory (1.A)

HPH Cybersecurity Gateway

hphcyber.hhs.gov

CLICK HERE

The HHS 405(d) Program

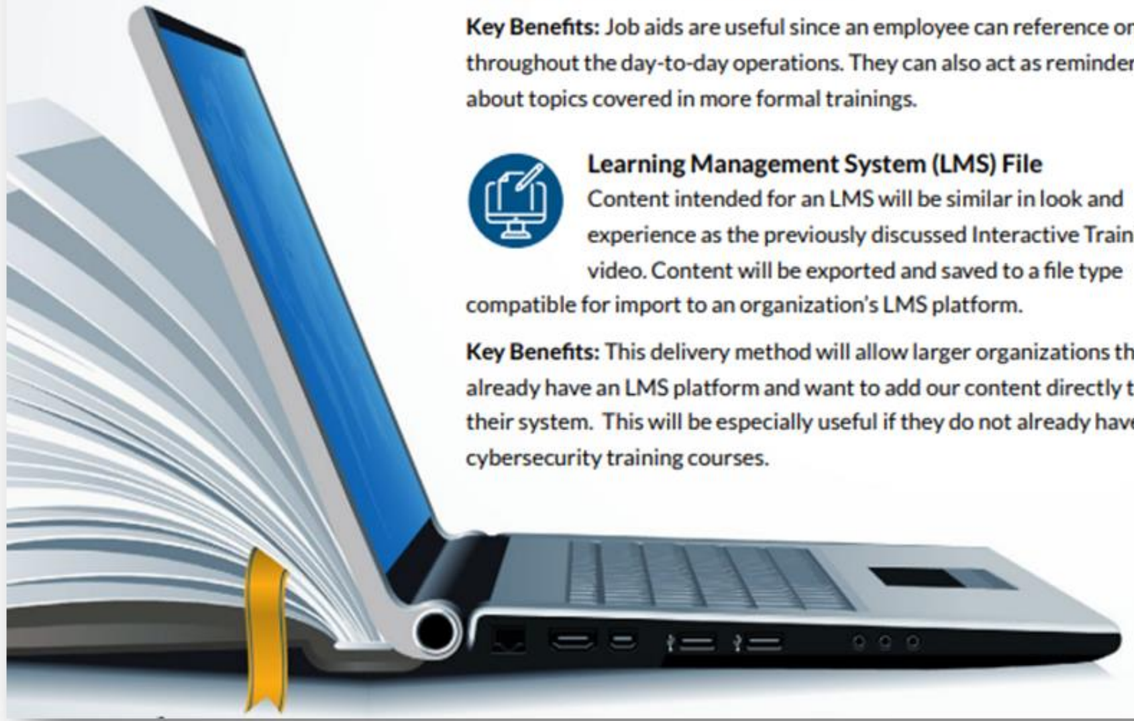
Aligning Health Care Industry Security Approaches

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

VISIT

Knowledge on Demand Education Platform 2023

Knowledge on Demand



The delivery methodologies for Knowledge on Demand include:

Job Aids

These are single documents with key tips related to the topic. This format is meant to be used as an "on-the-job" resource tool. They can provide instructional steps if necessary to meet the training objectives.

Key Benefits: Job aids are useful since an employee can reference one throughout the day-to-day operations. They can also act as reminders about topics covered in more formal trainings.

Learning Management System (LMS) File

Content intended for an LMS will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.

Key Benefits: This delivery method will allow larger organizations that already have an LMS platform and want to add our content directly to their system. This will be especially useful if they do not already have cybersecurity training courses.

Interactive Training Videos

These videos are launched from the 405(d) KOD webpage but can also be downloaded by the end user. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

Key Benefits: This interactive delivery method provides end users flexibility to access each threat topic at their own time due to the easy of access from the website.

PowerPoint Trainings

These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

Key Benefits: PowerPoint presentations are useful tools because they encourage discussion between employees and managers. It also allows the organization to better tailor their training to meet their specific needs.

Visit our website at 405d.hhs.gov/KOD to experience this new learning platform and explore the ways you can integrate this platform into the awareness education for all employees at your healthcare organization.

405(d) Outreach & Program Resources

HHS/405(d) Awareness Materials

Cyber Hygiene Posters, In Depth Infographics, Social Media Outreach

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters and Spotlight Webinars to increase cybersecurity awareness

Knowledge on Demand

Education platform offering Cybersecurity Awareness training on the top 5 cyber threats facing the healthcare sector! Interactive videos, job aids and PowerPoints with notes!.

Official Task Group Products

These resources are official products produced by the 405(d) Task Group. Examples include the HICP Publication, Quick Start Guides, New OCCI Publication, and 5 threat flyers.

Questions?

Visit Our Website
405d.hhs.gov

Do you follow us on social media?
Check us out @ask405d

Upcoming Webinars

Healthcare and the DoD: Preparing for CMMC Compliance | July 31 @ 12:00 CST

[Register here]

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

[August 1 -Register here]

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

[Register here]

Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

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.