CMS 2024 Quality Conference

Resilient and Ready Together

Creating an Optimal Environment for Quality Healthcare for Individuals, Families, and Communities

Cybersecurity Performance Goals

Strengthening the Cybersecurity of the Healthcare Sector and Keeping Patients Safe and Secure

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES

CMS 2024 Quality Conference

Resilient and Ready Together

Creating an Optimal Environment for Quality Healthcare for Individuals, Families, and Communities

Brian Mazanec, PhD

Deputy Director, Office of Preparedness
Department of Health and Human Services,
Administration for Strategic Preparedness and Response

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Advancing HHS's Vision for Healthcare and Public Health Sector Cybersecurity

HHS recently released a concept paper on how it will support Healthcare and Public Health (HPH) Sector Cybersecurity. The HHS concept paper for HPH Sector Cybersecurity overviews HHS' proposed framework to help the HPH Sector address cybersecurity threats and protect patients. The concept paper rests on four pillars of enhancing cybersecurity for the Sector.

Voluntary **Cybersecurity Performance Goals** for the Sector

Incentives and resources to implement cybersecurity best practices

HHS Cybersecurity Strategy to increase enforcement and accountability

ASPR as the **One-Stop-Shop** for healthcare cybersecurity

Why Cybersecurity Performance Goals (CPGs) now?

Based on industry-specific analysis, the CPGs set a baseline for cybersecurity expectations for all healthcare and public health organizations, no matter their size or cyber maturity. The CPGs map directly to existing cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Healthcare Industry Cybersecurity Practices (HICP), and the National Cybersecurity Strategy.

Increasing attacks

Between 2018-2022, the HPH Sector saw a **93% increase in large, reported breaches** and a **278% increase** in large **breaches involving ransomware.**

Chronic underfunding

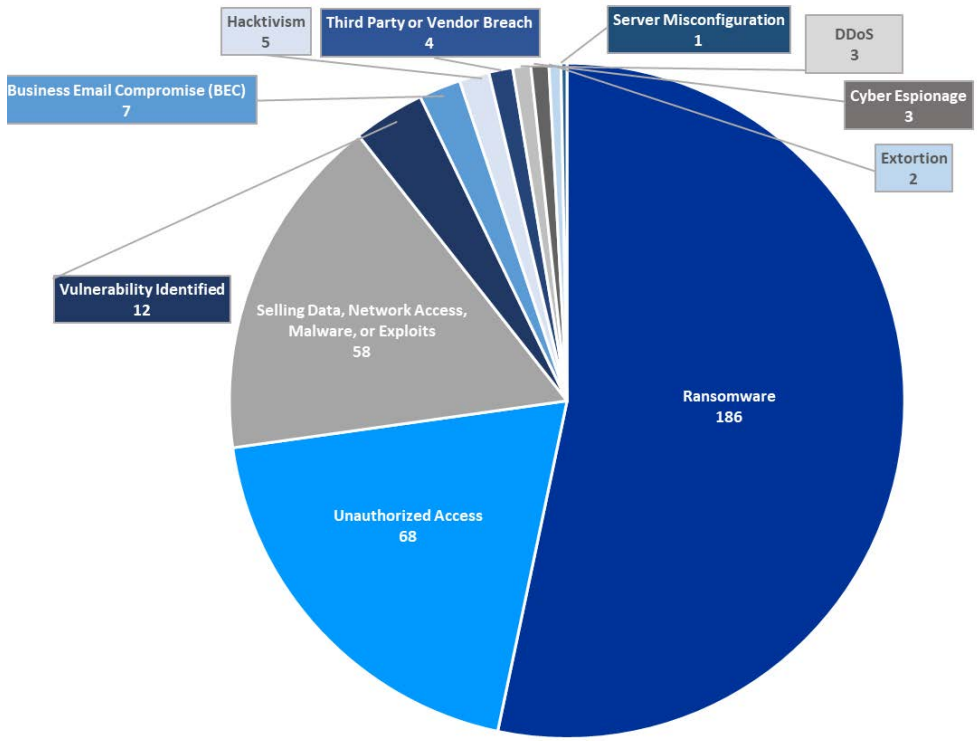
Cybersecurity planning efforts are chronically underfunded, leaving the Sector vulnerable and unable to address, or mitigate, cybersecurity risks.

Evolving threat landscape

The type, size, frequency, and scale of impact of cybersecurity attacks is continuously evolving and, due to a myriad factors, the HPH Sector cannot keep up.

Requests for clear guidance

The HPH Sector has asked for help prioritizing most impactful practices to enhance cybersecurity tailored to their needs.

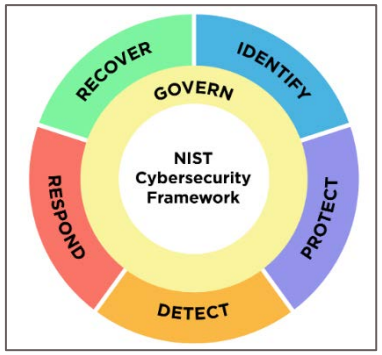


# of cyberattacks on the HPH Sector, by type: Q3, 2023

CMS 2024 Quality Conference
Resilient and Ready Together

What are existing sources of cybersecurity guidance?

With many existing sources of cybersecurity guidance, it can be difficult for HPH Sector organizations to know where to start implementing cybersecurity measures.



What are the Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (CPGs)?

The HPH CPGs were developed and adapted from the 2023 DHS/CISA-led Cross-Sector CPGs and provide HPH Sector-specific cybersecurity guidance to healthcare and public health organizations at all levels of technical competency and resource-availability.

Overview

A **baseline set of recommended cybersecurity controls and best practices** with known risk-reduction values

Developed by HHS, DHS/CISA, and the private sector community for information technology (IT) and operational technology (OT) owners and operators to improve the state of cybersecurity within HPH entities

HHS CPGs **work to simplify the confusion** of multiple frameworks and recommendations and **support compliance** with other regulatory requirements

Benefits

- Strengthen cyber preparedness
- Improve cyber resilience
- Protect patient information and safety

CMS 2024 Quality Conference
Resilient and Ready Together

How can your organization take immediate action?

The HPH CPGs help provide layered protection at different points of potential exploitation in healthcare digital systems. Layered protection at key points along the cybersecurity attack chain are crucial to mitigating the impacts of cybersecurity attacks when they occur. The HPH CPGs are divided into two categories supporting this layered approach:

Essential Goals

Essential Goals **set a floor of safeguards** to help healthcare organizations **address common vulnerabilities**, improve response when events occur, and minimize residual risk.

Examples of Essential Goals

- Mitigate known vulnerabilities
- Enhance email security
- Implement multifactor authentication
- Promote strong encryption
- Use unique credentials
- Separate user and privileged accounts
- Establish both vendor and supplier cybersecurity requirements

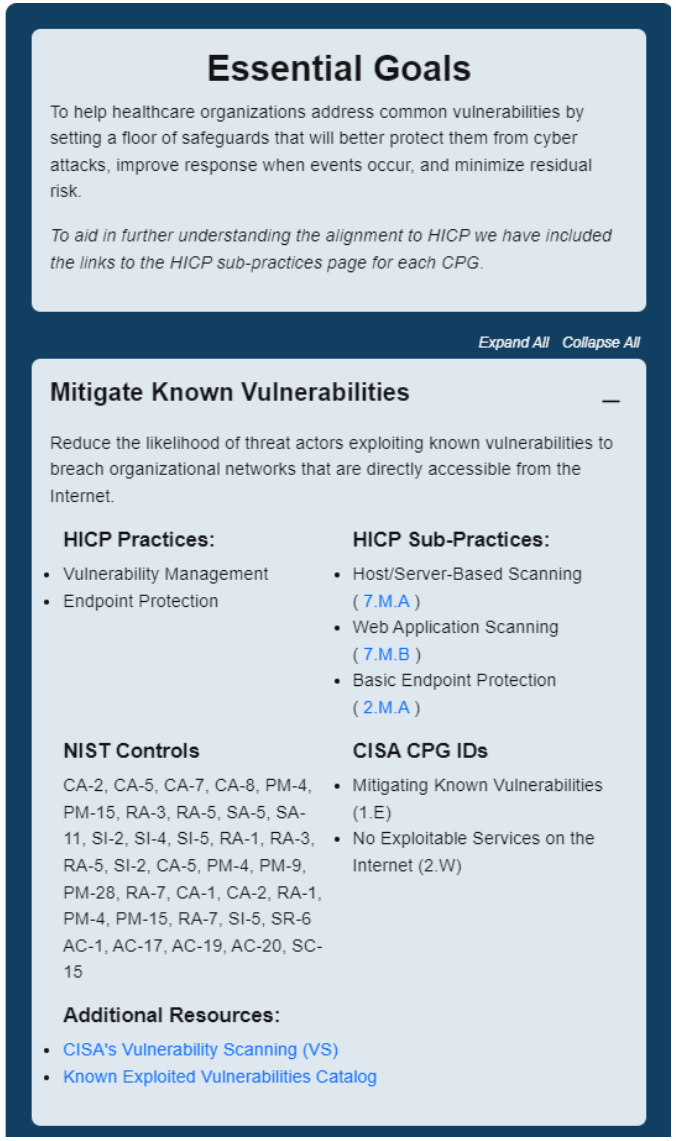
Enhanced Goals

Enhanced Goals **enable organizations to mature their cybersecurity capabilities** and improve the defenses needed to protect against less common, but potentially more impactful, attack vectors.

Examples of Enhanced Goals

- Develop and oversee an asset inventory
- Implement third party vulnerability disclosures
- Establish cybersecurity testing procedures and norms
- Segment networks, especially mission critical assets
- Centralize log collection
- Centralize incident planning and preparedness
- Manage device and systems settings in a consistent manner

What are the Essential 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 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

- **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.
- **Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers:** 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.
- **Separate 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.

Where can your office go for more information?

Visit us at HPHcyber.hhs.gov.

Questions? Reach out to CIP@hhs.gov.