405(d) Task Group created by HHS as part of the Cybersecurity Act of 2015 Legislative Mandate

405(d) guidance focuses on most common attack vectors against U.S. domestic hospitals

Top 5 Threats:

1. Social Engineering
2. Ransomware
3. Loss/Theft
4. Data Loss
5. Med Device Attack

Implementing HICP Using the CPGs (Cybersecurity Performance Goals)

Align with new industry guidance & best practices

In response to the rising numbers of cyber-attacks across critical infrastructure, the U. S. Health and Human Services created the 405(d) Task Group to align and improve the security posture of the healthcare sector. The Task Group published the Health Industry Cyber Practices (HICP) to serve as a guide for aligning and improving healthcare cyber resilience and securing the continuum of patient care.

The HICP 2023 Edition outlines the top 5 cyber threats healthcare organizations face and provides a framework of 10 best Practices to address and mitigate those threats. To help prioritize core HICP Practices, the Cybersecurity Performance Goals (CPGs) were published as a focused subset of high-impact HICP Practices.

HICP Cyber Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection & DLP
5. Asset Management
6. Network Management
7. Vulnerability Management
8. SOC & Incident Response
9. Connected Medical Devices
10. Cyber Oversight & Governance

10 HICP Practices

2 CPG Levels: Essentials Enhanced

1-4 HICP Sub-Practices per CPG

28 HICP Sub-Practices in Essential Goal

21 HICP Sub-Practices in Enhanced Goal

Why Align with the HICP

The HICP Practices are voluntary and are the new standard of best practices for healthcare cybersecurity. Developed as a consensus-based collaboration between both public and private organizations, HICP proposes flexible, practical, and cost-effective means to mitigate against the top 5 threats. Healthcare organizations are encouraged to leverage HICP to improve their cybersecurity posture, reduce threats against patient care delivery, patient data, and patient safety.

Cybersecurity Performance Goals

Essential

1. Mitigate Known Vulnerabilities
2. Email Security
3. Multifactor Authentication
4. Basic Cybersecurity Training
5. Strong Encryption
6. Revoke Credentials
7. Basic Incident Planning and Preparedness
8. Unique Credentials
9. Separating User and Privileged Accounts
10. Vendor / Supplier Cybersecurity Requirements

Enhanced

1. Asset Inventory
2. Third-Party Vulnerability Disclosure
3. Third-Party Incident Reporting
4. Cybersecurity Testing
5. Cybersecurity Mitigation
6. Detect and Respond to Relevant Threats
7. Network Segmentation
8. Centralized Log Collection
9. Centralized Incident Planning and Preparedness
10. Configuration Management

How to Leverage the CPGs

The HICP Practices are flexible and not set in any priority order. This allows security teams to define relevance and weigh risks based on their own unique organization needs and resources. In contrast, the CPGs focus in and organize high-impact HICP Sub-Practices that drive cyber resilience and strengthen preparedness to face cyber threats.

Instead of tackling all of the HICP Sub-Practices at once, organizations can start with the first CPG level and work through assessing their existing safeguards within the Essential Goals before tackling the Enhanced Goals tier. After this assessment, develop a plan of action based on key gaps, existing resources, and risk tolerance.

Right Sizing

HICP divides Practices by Small, Medium, & Large Health Organizations

Healthcare delivery is not a one-size fits all, and neither is cybersecurity guidance. Therefore, HICP guidance is broken down by the "t-shirt size" of the organization. The size drives which set of HICP Sub-Practices are recommended for a strong security posture. Factors such as IT capability, cyber investments, and scale of provider attributes contribute to the sizing. The "Best Fit" Table 1 acts as a sizing guide.

	Small	Medium	Large
Physicians	1-10 Physicians	11-50 Physicians	>50 Physicians
Providers	1-25 Providers	26-500 Providers	>500 Providers
Beds	1-50 Beds	51-300 Beds	>300 Beds
Complexity	Single Practice or Care Site	Multiple Sites	Integrated Delivery Networks (IDNs); Participate in Accountable Care Organizations (ACOs) or Clinically Integrated Network (CINs)

Table displays "Fit" based on Provider Attributes only. See HICP 2023 Edition for additional organizational attributes that support Best Fit groupings.

HICP & CPGs map to NIST 800-53, NIST CSF, & HIPAA

Start with a CPG gap assessment

CPGs are a guidepost to implement a strong cyber hygiene baseline

Get Started

The new cybersecurity guidance provided by HHS outlines a new framework of practical and cost-effective security practices for the healthcare industry. By aligning with HICP and prioritizing high-impact Practices outlined between the two CPG tiers, healthcare organizations now have actionable recommendations to improve their security posture and mature their programs to defend against the biggest threats facing patient safety, patient care delivery, and patient data.