Aligning HICP to the HPH Cybersecurity Performance Goals

HHS 405(d)
Aligning Health Care Industry Security Approaches

What are the HPH CPGs?

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.

These goals 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 (e.g., Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the National Cybersecurity Strategy). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as identified in the 2023 Hospital Cyber Resiliency Landscape Analysis.

Central Components Include:

- Industry-specific based on analysis to facilitate an improvement in cyber resiliency across sector.
- Directly addresses the most significant attack vectors facing hospitals (and other healthcare entities providers).
- Provides layered or "defense in depth" protection at different stages of the potential attack chain.
- Adaptable as the cyber threat landscape evolves and new threats emerge.

To read the full HICP Publication visit: https://405d.hhs.gov/information

If you are currently using or leveraging HICP practices in your organization, you are well on your way to implementing the HPH CPGs.

Why are the HPH CPGs Important and How Do I Use Them?

If adopted, these safeguards can help better protect the sector from major cyberattacks, improve response when events occur, and minimize residual risk. Healthcare organizations are encouraged to adopt more enhanced practices that satisfy specific business needs, if applicable.

The HPH CPGs are designed to ensure layered protection at different stages of the attack chain, or points in digital systems that can be exploited, which is crucial to mitigating the impacts of cybersecurity incidents if and when they occur.

Check out the CPGs and their HICP mapping and click on their sub-practices to find out how you can start implementing these practices today!

Essential Goals

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

- Mitigate Known Vulnerabilities
  7.M.A, 7.M.B, 2.M.A
- Email Security
  1.M.A, 1.M.B, 1.M.D
- 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
  10.M.A, 8.S.A , 8.M.B, 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 Goals

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

- 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

To view the HPH CPGs, check out the new HPH Cybersecurity Gateway, visit: hphcyber.hhs.gov