Health Industry Cybersecurity Practices (HICP) Quick Start Guide - Medium & Large Healthcare Organizations

My Organization's Information Technology Department Handles Cybersecurity. Isn't that Good Enough?

As a result of the Cybersecurity Act of 2015, the U.S. Department of Health and Human Services brought together over 150 cyber-experts, clinicians and healthcare administrators to develop the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. The HICP publication provides practical, cost-effective practices that will help strengthen your organization against cyber criminals, seamlessly integrate cybersecurity into your team's day-to-day operations, and outline an effective strategy to **reduce your enterprise's cybersecurity risk**.

There was an average of one health data breach per day in 2016 and 27 million patient records were compromised. This problem—that shows no indication of simply "going away"—costs the healthcare industry $5.6 **billion** a year. Ransomware and extortion attacks can have drastic consequences on a healthcare organization's ability to care for patients, as well as cause reputational harm and severe impacts to the bottom line.

Despite having strong Information Technology departments and cybersecurity resources, many healthcare organizations still fall victim to cyber-attacks. Cyber threats are becoming more frequent and more sophisticated. Organizations that widely adopt a "culture of cybersecurity" and work together on the cybersecurity front with other leaders in the industry are more likely to stay ahead of the game, protecting their organization's enterprise, reputation, and patients.

What is the HICP Publication? It's Not Just "Another" Cybersecurity Document

WHAT IS HICP?

The HICP publication identifies five current cybersecurity threats and provides ten practices that can be used to mitigate them. It's comprised of a common set of cost-effective best practices based on widely accepted and used frameworks, standards, methodologies, processes, and procedures vetted by healthcare and security professionals. Recommendations in the HICP are based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework—the gold standard of cost-effective cybersecurity best practices.

WHAT ARE THE FIVE THREATS?

The five current threats detailed in the main document are: E-Mail Phishing Attacks; Ransomware Attacks; Loss or Theft of Equipment or Data; Insider, Accidental, or Intentional Data Loss; and Attacks Against Connected Medical Devices.

WHO DOES HICP BENEFIT?

Medium/Large Organizations like yours! HICP is designed to strengthen the cybersecurity posture of the Healthcare and Public Health Sector and help medium/large organizations prioritize what is important for their own protection. By using HICP, medium/large organizations can do their part to support the national Health Sector's cyber preparedness.

WHAT ARE THE TEN BEST PRACTICES?

HICP identifies ten best practices to mitigate the current threats: E-Mail Protection Systems; Endpoint Protection Systems; Access Management; Data Protection and Loss Prevention; Asset Management; Network Management; Vulnerability Management; Incident Response; Medical Device Security; and Cybersecurity Policies.

How is the HICP Publication Organized?

The HICP Publication includes a main document, two technical volumes, and a Resources and Templates Volume:

- The **Main Document (MD)** discusses the current cybersecurity threats facing the healthcare industry.
- **Technical Volume 1 (TV1)** discusses 10 Cybersecurity Practices for small healthcare organizations.
- **Technical Volume 2 (TV2)** discusses 10 Cybersecurity Practices for medium-sized and large healthcare organizations.
- The **Resources and Templates Volume** provides additional resources, templates, and supplementary materials.

How Can I Use this Quick Start Guide?

The HICP Publication encourages good cyber hygiene across your organization. After reading this quick start guide, you will understand which HICP documents are most applicable to each role at your organization and what to do next. Look up your role in the below matrix so you know what you should read—and what you should delegate.




What's your role	Leadership (Executives, Board of Directors)	IT Professionals	Healthcare Technology Management (HTM)	Staff/Clinicians/Users
What part of HICP you should read	MD – pages 5-10 MD – page 28 T2 – page 3	MD – page 11 MD – page 28-30 T2 – Medium Organizations: page 4-13. Large Organizations: page 7-13.	MD – pages 15–26 T2– pages 31-41, 52-100	MD – pages 15–26
What part of HICP you should pass along and to whom	**To Your Organization's Technology Professionals:** MD – page 11 MD – page 28 T2 – 4-13	**To Your Organization's Leadership & Management:** MD – pages 5-10 MD – page 28 T2 – pages 3	**To Your Organization's Leadership & Management:** MD – pages 5-10 MD – page 28 T2 – pages 3	**To Your Organization's Leadership & Management:** MD – pages 5-10 MD – page 28 T2 – pages 3
	To Your Organization's HTM: MD – pages 15–26 T2 – pages 31-41, 52-100	**To Your Organization's HTM:** MD – pages 15–26 T2 – pages 31-41, 52-100	**To Your Organization's Technology Professionals:** MD – page 11 MD – page 28 T2 – pages 5-13	**To Your Organization's Technology Professionals:** MD – page 11 MD – page 28 T2 – pages 4-13
	To Your Organization's Staff/Users: MD – pages 15–26	**To Your Organization's Staff/ Users:** MD – pages 15–26	**To Your Organization's Staff/ Users:** MD – pages 15–26	**To Your Organization's HTM:** MD – pages 15–26 T2 pages – 31-41, 52-100

Visit us on Social Media: @ask405d facebook.com/ask405d
Want more information or need to obtain a copy of the HICP Publication? Please visit the 405(d) website at www.405d.hhs.gov, or email us at CISA405d@hhs.gov.