

HHS 405(d) Resources Cheat Sheet – June 2023

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP 2023 Edition)

405(d)'s cornerstone publication is called HICP (pronounced "hiccup"). HICP was recently updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate current cybersecurity threats the healthcare and public health (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 an appendix of resources and templates. You can find a one-page rundown [here](#).

Document Overview:

- [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.

Importantly, under a law ([P.L. 116-321](#)) passed in Jan. 2021, Congress gave the Office for Civil Rights (OCR) the authority to shorten the length of audits and sizes of fines related to healthcare breaches if a provider had been using recognized cyber best practices (including those found in HICP) for at least one year.

Landscape Analysis

The HPH sector has faced dramatic increases in cyber-attacks intended to cause disruption to the care continuum. In response, the HHS 405(d) Program conducted a [Landscape Analysis](#), which reviewed active threats attacking hospitals and the cybersecurity capabilities of U.S. hospitals.

Document Overview:

- Executive Summary: overview of key observations, HICP Practice Adoption and a note on Data sources
- Threat Analysis: overview of the evolving threat of ransomware and links between threats and mitigations
- Capabilities and Performance Assessment: covers staff analysis, cyber expense, coverage to NIST and HICP
- Adoption of HICP Practices: covers practices in HICP that have significant progress, need improvement, and need additional research, and non-urgent items

Knowledge on Demand

The 405(d) Program, in collaboration with industry, launched a new cybersecurity training platform on its website – [Knowledge on Demand](#). The platform includes five cybersecurity awareness training courses that align with the top five cybersecurity threats outlined in HICP and its accompanying two volumes.

Please email the Public Policy team at policy@chimecentral.org with questions.

Source: <https://405d.hhs.gov/>