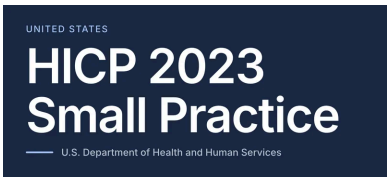
SmartSuite

Framework / Cybersecurity / Other

Health Industry Cybersecurity Practices (HICP) 2023 Edition, Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations

HICP Technical Volume 1 (2023 Edition) is HHS 405(d) and HSCC voluntary guidance: five threats, ten practices and 21 sub-practices for healthcare organizations of 1 to 10 physicians.



What it is

HICP Technical Volume 1, Cybersecurity Practices for Small Healthcare Organizations (2023 Edition), is the small-organization volume of Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, the voluntary, consensus-based guidance that the U.S. Department of Health and Human Services (HHS) 405(d) Program publishes with the Health Sector Coordinating Council under section 405(d) of the Cybersecurity Act of 2015. It is written for practices that generally have no dedicated IT or security staff, which the Main Document sizes as 1 to 10 physicians, 1 to 25 providers in acute or post-acute care, or hospitals of 1 to 50 beds at a single site.

At a glance

PUBLISHER
U.S. Department of Health and Human Services (HHS) 405(d) Program, under ASPR, with the Health Sector Coordinating Council (HSCC)

TYPE
Guidance

VERSION
HICP 2023 Edition, Technical Volume 1 (Cybersecurity Practices for Small Healthcare Organizations)

EFFECTIVE
April 2023 (2023 Edition; voluntary guidance, applies on publication)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Healthcare & Life Sciences

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
Low

Source: 405d.hhs.gov/Documents/tech-vol1-508.pdf

Why it matters

- **Sized for a practice without IT staff** Technical Volume 1 assumes no dedicated IT or security personnel and devotes its first pages to managed IT services and vendor selection (Introduction), so the sub-practices are things a practice can ask a vendor to do.
- **Threats mapped to practices** Each practice section ends with Key Mitigated Threats, tying the ten practices back to the five threats of the Main Document; the Threat-to-Practice Matrix on 405d.hhs.gov is offered as the start of a risk assessment.
- **A HIPAA Security Rule credit** Under Public Law 116-321 (HITECH section 13412), twelve months of documented 405(d) practices may mitigate fines under section 1176 of the Social Security Act, end an audit early and mitigate remedies in a settlement.
- **Free, government-published text** The Main Document, both Technical Volumes and the Resources and Templates volume are published by HHS at 405d.hhs.gov at no cost, with executive and quick-start cards for small organizations.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HICP 2023 Small Practice

Sub-Practice Library (1.S.A to 10.S.D)

Load the 21 small-organization sub-practices with the practice they belong to, the Key Mitigated Threats, an owner, implementation status and linked evidence.

Risk Assessment (10.S.B)

Run the cybersecurity risk assessment and management process as records of threats, assets and treatment decisions, linked to the sub-practices that mitigate each of the five threats.

Asset Inventory and Decommissioning (5.S.A to 5.S.C)

Keep the inventory of devices, software and medical devices with procurement and decommissioning steps in IT Asset Management (ITAM), including 9.S.A medical device security notes.

Managed Service Provider Oversight

Record which sub-practices a managed IT vendor performs, the contract terms and the evidence received, in Third Party Risk Management, since the practice remains responsible.

Policies, Training and Phishing Simulations (4.S.A, 10.S.A, 10.S.C, 1.S.C)

Publish the policies, schedule security awareness training and phishing simulations and log completion per staff member.

Incident Response Plan and Twelve-Month Record (8.S.A, 8.S.B)

Keep the plan, the Table 7 team roles, incident logs and information-sharing contacts, and report the months each sub-practice has been in place for the Public Law 116-321 record.

Common framework mappings

CIS Controls v8.1 | HIPAA (NIST SP 800-66 Rev. 2) | HITRUST CSF v11.5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5 | PCI DSS 4.0.1

Official resources

HICP 2023 Edition: Main Document (PDF)

The main publication: the five threats, the ten cybersecurity practices and the 405(d) program history.

405d.hhs.gov/Documents/HICP-Main-508.pdf

HICP 2023 Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations (PDF)

The volume this page describes: the ten practices and their sub-practices for small organizations.

405d.hhs.gov/Documents/tech-vol1-508.pdf

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

Outlines advanced practices tailored for medium and large healthcare providers.

405d.hhs.gov/Documents/tech-vol2-508.pdf

Frequently asked questions

Who is HICP Technical Volume 1 written for?

Small healthcare organizations, which the Main Document's sizing table defines as 1 to 10 physicians, 1 to 25 acute or post-acute providers or hospitals of 1 to 50 beds, usually a single practice or care site with limited or no cybersecurity funding. Technical Volume 1's Introduction adds that such organizations generally have no dedicated IT or security staff and often rely on managed IT services, while remaining HIPAA covered entities. Medium and large organizations use Technical Volume 2.

Is HICP mandatory or certifiable?

Neither. The Cybersecurity Act of 2015, section 405(d), called for voluntary, consensus-based, industry-led guidelines, and the Main Document says HICP is not a list of controls that all organizations must implement but recommended practices to consider after a risk assessment. There is no HICP certification. Public Law 116-321 (January 5, 2021) gives adopters a benefit instead: HHS must consider documented 405(d) practices of at least twelve months when deciding HIPAA fines, audit length and remedies.

What are the five threats and ten practices?

The five threats are social engineering; ransomware attacks; loss or theft of equipment or data; insider, accidental or malicious data loss; and attacks against network connected medical devices that may affect patient safety. The ten Cybersecurity Practices are email protection systems, endpoint protection systems, access management, data protection and loss prevention, asset management, network management, vulnerability management, incident response, network connected medical devices, and cybersecurity oversight and governance (Main Document, How to Use this Publication).

What are the small-organization sub-practices?

Technical Volume 1, Table 2 lists 21: email system configuration, education and phishing simulations (1.S.A to 1.S.C); basic endpoint protection controls (2.S.A); basic access management (3.S.A); data protection policies, procedures and education (4.S.A to 4.S.C); inventory, procurement and decommissioning (5.S.A to 5.S.C); network segmentation, physical security and guest access, and intrusion prevention (6.S.A to 6.S.C); vulnerability management (7.S.A); incident response and information sharing (8.S.A, 8.S.B); medical device security (9.S.A); and policies, risk assessment and management, security awareness and training, and cyber insurance (10.S.A to 10.S.D).

Which edition of HICP is current, and who publishes it?

The 2023 Edition, as of this review; the first edition was released in 2018 after HHS convened the 405(d) Task Group in May 2017, and the Task Group began the update in 2019 (Main Document, Appendix B). It is published by the HHS 405(d) Program, which operates under the Administration for Strategic Preparedness and Response in collaboration with the Health Sector Coordinating Council, whose Joint Cybersecurity Working Group hosts the Task Group. The documents are free at 405d.hhs.gov.

License included / downloadable: Yes The HICP Main Document, Technical Volumes 1 and 2 and the Resources and Templates volume are U.S. government publications available free from HHS at 405d.hhs.gov; the platform links to the official PDFs.

Full framework page and mappings: smartsuite.com/frameworks/us-hicp-small-practice-health-industry-cybersecurity-practice