SmartSuite

Framework / Cybersecurity / Other

Health Industry Cybersecurity Practices (HICP) — 2023 Edition — Medium and Large Organizations

HICP 2023 Edition, Technical Volume 2, gives medium and large healthcare organizations ten voluntary cybersecurity practices against five threats, from the HHS 405(d) Program.



What it is

Health Industry Cybersecurity Practices (HICP), 2023 Edition, Technical Volume 2 sets out ten voluntary cybersecurity practices, with sub-practices for medium-sized and large U.S. healthcare organizations, to reduce five threats: social engineering, ransomware, loss or theft of equipment or data, insider data loss, and attacks on network-connected medical devices. The HHS 405(d) Program published the 2023 Edition on April 17, 2023, as an update of the 2018 first edition.

At a glance

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

TYPE
Guidance

VERSION
HICP 2023 Edition, Technical Volume 2 (medium and large organizations)

EFFECTIVE
April 17, 2023 (2023 Edition; first edition 2018)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Healthcare & Life Sciences

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
Medium

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

Why it matters

- **Practices tied to named threats** Each practice ends with Key Mitigated Threats and Suggested Metrics, and the Threat-to-Practice Matrix on 405d.hhs.gov relates the five threats to the ten practices.
- **Sized to the organization** Technical Volume 2 splits every practice into sub-practices for medium-sized organizations and for large organizations, for example 3.M.A Identity and 3.L.A Federated Identity Management.
- **Recognized security practices under HITECH** HITECH section 13412 requires HHS to consider whether recognized security practices were in place for at least 12 months when it decides fines, audit length and remedies (Public Law 116-321).
- **A starting point, not a mandate** HHS states that the publication is a series of recommended practices to consider as risk mitigation techniques and advises beginning with a risk assessment.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HICP 2023 (Medium and Large)

Practice and Sub-Practice Register

Record each of the ten practices and its medium or large sub-practices with status, owner and evidence (Technical Volume 2).

Threat-to-Practice Map

Link the five threats to the practices you rely on, starting from the Threat-to-Practice Matrix, and record the residual risk and owner.

Asset and Medical Device Inventory

Track endpoints, servers and network-connected medical devices with owners, open vulnerabilities and decisions about contacting the FDA (practices 5 and 9).

Access and Identity Reviews

Schedule provisioning, transfer and deprovisioning reviews and multi-factor authentication coverage checks for email and privileged access (practices 1 and 3).

Incident and Response Log

Keep incident records, response exercise results and information sharing contacts, with follow-up actions assigned to owners (practice 8).

Recognized Practices Evidence File

Keep dated evidence that each practice has been in place, with governance sign-off and suggested metrics, to support a HITECH section 13412 position (practice 10).

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | HITRUST CSF v11.5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

HICP 2023 Edition — Technical Volume 2: Medium and Large Organizations

The 2023 Edition practices for medium and large healthcare organizations, published by the HHS 405(d) Program.

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

HHS 405(d) Program

About the 405(d) Program, its place under ASPR and its joint work with the Health Sector Coordinating Council.

405d.hhs.gov/information

HICP 2023 Edition: Main Document

The Main Document of the 2023 Edition: the five threats, the ten practices, Table 1 organization sizes and the 405(d) history.

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

Public Law 116-321: Recognition of Security Practices

The law that added HITECH section 13412 and names Section 405(d) approaches as recognized security practices.

govinfo.gov/content/pkg/STATUTE-134/html/STATUTE-134-Pg5072.htm

Frequently asked questions

Is HICP mandatory?

No. HICP is voluntary, consensus-based guidance, and HHS says it is not a list of controls that every organization must implement. It recommends starting with a risk assessment and tailoring the practices. It can still matter in HIPAA enforcement, because HITECH section 13412 recognizes approaches promulgated under Section 405(d).

What are the five threats and ten practices in HICP?

The 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. The practices are Email Protection Systems, Endpoint Protection Systems, Access Management, Data Protection and Loss Prevention, Asset Management, Network Management, Vulnerability Management, Security Operations Centers and Incident Response, Network Connected Medical Devices, and Cybersecurity Oversight and Governance.

Which HICP volume applies to a medium or large organization?

Technical Volume 2 applies. The Main Document's Table 1 helps choose a size: medium is 51 to 299 hospital beds or 11 to 50 physicians, and large is over 300 beds or over 50 physicians. Medium-sized organizations start with the medium sub-practices, and large organizations consider both the medium and the large sub-practices.

How does HICP relate to HIPAA penalties?

HITECH section 13412, added by Public Law 116-321 on January 5, 2021, requires HHS to consider whether recognized security practices were in place for at least the previous 12 months when it decides fines, audit length and agreed remedies. Recognized security practices include approaches promulgated under Section 405(d). HHS cannot increase fines because an organization lacked them.

Which HICP edition is current?

The 2023 Edition, published by the HHS 405(d) Program on April 17, 2023, is the edition on the program's resources page. It updated the first edition of 2018 and keeps a Main Document, two Technical Volumes and a Resources and Templates volume.

License included / downloadable: Yes HICP is published free of charge by the HHS 405(d) Program at 405d.hhs.gov and is a U.S. government publication.

Full framework page and mappings: smartsuite.com/frameworks/hicp-2018-large-healthcare-delivery-organizations

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.