SmartSuite

Framework / Cybersecurity / NIST Special Publications

Health Industry Cybersecurity Practices (HICP) — 2018 — Large Healthcare Delivery Organizations

U.S. HICP for large healthcare organizations provides [illegible] cybersecurity practices to reduce cyber risk and protect patient data.

What it is

U.S. HICP (Large Practice) — Health Industry Cybersecurity Practices is a cybersecurity framework that assists large healthcare organizations in identifying, managing, and mitigating key cybersecurity threats. Its primary goal is to provide actionable, industry-vetted practices that bolster the security and resilience of health sector operations and safeguard sensitive health information.

Developed by the U.S. Department of Health and Human Services (HHS) in collaboration with industry and government partners, HICP is tailored for entities with more than 500 employees. The framework addresses focus areas such as threat mitigation, security controls, data protection, and risk management, with specific guidance on topics like phishing, asset management, and medical device security.

At a glance

PUBLISHER Health Sector Coordinating Council, in partnership with the U.S. Department of Health and Human Services	TYPE Guidance	VERSION 2023
EFFECTIVE January 8, 2019	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY Moderate		

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

Why it matters

- **Support compliance obligations** Help organizations address HIPAA and regulatory mandates by aligning technical and administrative controls with best practices.
- **Enhance threat detection and response** Enable prompt identification and remediation of cyber incidents to minimize the impact of ransomware and other threats.
- **Strengthen data protection measures** Reduce the risk of unauthorized access and breaches involving protected health information through robust security guidelines.
- **Promote operational continuity** Mitigate risks to clinical operations by improving preparedness and recovery capabilities during cyber incidents or disruptions.

How SmartSuite supports HICP 2018 (Large HDOs)

HICP Security Practices Library

Structure recommended HICP practices aligned to major healthcare cybersecurity threats and risk domains.

Enterprise Asset and System Governance

Track clinical systems, connected medical devices, cloud platforms, and supporting infrastructure requiring protection.

Cybersecurity Risk Assessment and Mitigation

Manage enterprise risk assessments, mitigation plans, and security control implementation across healthcare environments.

Identity, Access, and Privileged Account Governance

Manage workforce identities, authentication controls, and privileged access to healthcare systems and sensitive data.

Third-Party and Supply Chain Security Oversight

Monitor cybersecurity risks associated with vendors, service providers, and connected healthcare technologies.

Security Operations and Compliance Reporting

Provide dashboards tracking cybersecurity posture, incident response activities, and program maturity across healthcare operations.

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

Health Industry Cybersecurity Practices (HICP) Large Practice

Provides official practices and guidelines to mitigate cybersecurity threats in large healthcare organizations.

405d.hhs.gov/information

Frequently asked questions

What is HICP (Health Industry Cybersecurity Practices) used for?

HICP provides voluntary cybersecurity guidelines tailored for the U.S. healthcare sector, aiming to reduce cybersecurity risks to patient safety and organizational operations. It offers practical recommendations and best practices focused on protecting electronic protected health information (ePHI) and critical infrastructure.

Is HICP required or mandatory for large healthcare practices?

HICP is a voluntary framework and is not a regulatory requirement. However, adopting HICP practices may demonstrate reasonable security procedures under HIPAA and can provide defensible evidence of due diligence in the event of regulatory scrutiny or breaches.

Who does HICP apply to in the healthcare industry?

HICP is designed primarily for healthcare organizations, with specific guidance for both small and large practices—the Large Practice guidance applies to healthcare entities with over 500 employees. Covered entities and business associates under HIPAA often reference HICP to strengthen their cybersecurity posture.

What are the key concepts or controls required by HICP for large practices?

HICP centers on the implementation of recognized cybersecurity practices, grouped into five major threats: phishing, ransomware, loss/theft of equipment, accidental data loss, and attacks against network-connected medical devices. Large practices must implement technical, administrative, and physical controls, including network segmentation, access management, and incident response plans.

How should large practices implement HICP in their cybersecurity programs?

Large practices should begin by conducting a risk assessment to identify gaps against HICP recommendations, then prioritize mitigation activities based on risk. Implementation typically includes developing policies, training staff, updating technical controls, and periodically reassessing threats and vulnerabilities.

How does HICP relate to other healthcare compliance frameworks like HIPAA or NIST?

HICP is complementary to HIPAA Security Rule requirements and maps well to guidance from NIST SP 800-53 and NIST Cybersecurity Framework (CSF). It does not replace regulatory obligations, but helps organizations operationalize best practices and demonstrate recognized security measures in line with federal expectations.

What are the ongoing compliance requirements for organizations using HICP?

While HICP itself does not impose formal certification or ongoing audits, organizations should continuously review and update cybersecurity policies, conduct periodic risk assessments, provide workforce training, and monitor the effectiveness of implemented controls to maintain alignment with HICP guidance.

How would SmartSuite support U.S. HICP (Large Practice)?

SmartSuite enables organizations to manage HICP compliance through configurable risk tracking, centralized control management, and streamlined collection of evidence for each cybersecurity practice. It supports audit readiness with integrated task monitoring, automated reminders, and robust reporting, helping organizations maintain documentation and demonstrate ongoing alignment with HICP requirements.

License included / downloadable: Yes HICP (Large Practice) is published by HHS and HSCC and is publicly available from HHS/HSCC websites. License included with platform

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