SmartSuite

Framework / Cybersecurity / Other

HICP 2018 – Medium

U.S. HICP provides voluntary cybersecurity practices to help healthcare organizations protect clinical systems, medical devices, and patient information.

What it is

U.S. HICP (Medium Practice) is a cybersecurity framework that helps healthcare organizations identify and implement best practices to reduce cyber risks and protect sensitive health information. It provides tailored guidance for medium-sized healthcare entities, focusing on the practical realities and threats facing the sector.

Developed by the U.S. Department of Health and Human Services (HHS) in collaboration with industry stakeholders, HICP aims to address the evolving threat landscape impacting healthcare organizations. The framework outlines key cybersecurity controls, risk management strategies, and incident response processes relevant to medium-sized providers, clinics, and health systems.

At a glance

PUBLISHER U.S. Department of Health and Human Services (HHS)	TYPE Guidance	VERSION HICP 2023
EFFECTIVE January 2019	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Security Baseline
IMPLEMENTATION COMPLEXITY Moderate		

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

Why it matters

- **Strengthen information security governance** Establish clear roles, responsibilities, and oversight processes for cybersecurity management in healthcare settings.
- **Enhance regulatory compliance support** Promote alignment with HIPAA requirements and foster readiness for audits and enforcement actions.
- **Improve incident detection and response** Enable organizations to identify, contain, and recover from cyber threats and data breaches more effectively.
- **Promote operational resilience** Reduce the likelihood and impact of service disruptions or patient care delays caused by cyber incidents.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HICP 2018 Medium

HICP Security Practices Library

Organize HICP cybersecurity practices aligned to the top healthcare cybersecurity threats.

Asset and System Risk Visibility

Track medical devices, EHR systems, clinical applications, and supporting infrastructure requiring protection.

Security Risk Assessment and Mitigation Planning

Identify cybersecurity risks affecting healthcare operations and track mitigation strategies.

Identity, Access, and Endpoint Security Governance

Manage authentication controls, endpoint protection, and privileged access to clinical systems.

Vendor and Third-Party Risk Oversight

Monitor cybersecurity risks associated with healthcare vendors, software providers, and connected medical devices.

Healthcare Cybersecurity Incident and Program Maturity Reporting

Track cybersecurity incidents, remediation actions, and program maturity across healthcare security operations.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | HIPAA (NIST SP 800-66 Rev. 2) | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Provides the official HHS publication describing HICP practices and threat mitigation matrix.

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

HPH Sector Cybersecurity Framework Implementation Guide

Describes how to implement the NIST Cybersecurity Framework for healthcare using HICP alignment.

aspr.gov/readiness-response/healthcare-readiness/cip/resources/hph-cybersecurity-framework-implementation-guide

Frequently asked questions

What is the U.S. HICP (Medium Practice) used for?

The U.S. Health Industry Cybersecurity Practices (HICP) Medium Practice is designed to assist healthcare organizations in identifying and implementing cybersecurity practices that address common threats. Its goal is to improve organizational cyber resilience and better protect sensitive health information and systems.

Is U.S. HICP required for healthcare organizations?

U.S. HICP is not a mandatory or certifiable standard but is a voluntary set of cybersecurity guidelines. However, adopting HICP may demonstrate reasonable security practices under regulatory scrutiny, such as during HIPAA audits, and can serve as evidence of due diligence regarding information protection.

Who should use the U.S. HICP (Medium Practice)?

The HICP Medium Practice is intended for mid-sized healthcare providers and organizations with moderate resources and cybersecurity maturity. Organizations should assess their environment, resource availability, and risk tolerance to determine if Medium Practice aligns with their needs.

What are the key concepts and controls in HICP (Medium Practice)?

Medium Practice focuses on five top threats: email phishing, ransomware, loss/theft of equipment, insider threats, and attacks against network-connected medical devices. It provides actionable controls, such as multi-factor authentication, endpoint protection, regular backups, access management, and security training.

 © 2026 SmartSuite Inc. All rights reserved.

How do organizations implement HICP (Medium Practice)?

Implementation involves reviewing organizational risks, mapping HICP's suggested practices against current controls, and closing identified security gaps. Engagement from leadership, documented policies, technology updates, and employee awareness are critical steps in operationalizing Medium Practice recommendations.

How does U.S. HICP relate to other healthcare cybersecurity frameworks?

HICP complements regulatory and industry standards like HIPAA Security Rule and NIST Cybersecurity Framework. While it doesn't replace these requirements, it provides practical, threat-informed guidance that can support compliance with broader regulatory obligations.

What are the ongoing compliance requirements for HICP?

While not subject to certification, maintaining alignment with HICP involves continually assessing risks, updating controls, training staff, and reviewing cyber incidents. Documenting adherence to HICP practices provides a defensible position during audits or investigations.

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

SmartSuite can help organizations manage U.S. HICP by enabling effective risk tracking, control implementation, and evidence collection. Its workflow tools support audit readiness, continuous monitoring, and generate reports that facilitate proactive compliance and assurance activities.

License included / downloadable: Yes HICP is published by HHS and is publicly available for free from official HHS and NIST websites. License included with platform

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