

HICP v1.0 – Small Practice

U.S. Health Industry Cybersecurity Practice (Small Practice) provides prioritized, practical cybersecurity guidance to help small healthcare providers reduce cyber risks.



What it is

U.S. HICP (Small Practice) — Health Industry Cybersecurity Practice is a cybersecurity guideline developed to help small healthcare organizations identify and mitigate the most common cyber threats facing the healthcare sector. The framework provides practical, industry-tailored recommendations for improving data protection and reducing cybersecurity risks specific to smaller medical practices.

Developed by the U.S. Department of Health and Human Services (HHS) in collaboration with industry stakeholders, HICP targets healthcare providers and their support organizations who require scalable and actionable security measures. It focuses on key areas such as phishing, ransomware, loss or theft of devices, insider threats, and the management of medical devices.

At a glance

<div>PUBLISHER</div> <div>Health & Public Health Sector Coordinating Council (HSCC) (official publisher in partnership with the U.S. Department of Health and Human Services for HICP) ([healthsectorcouncil.org] (https://healthsectorcouncil.org/hicp/?utm_source=openai))</div>	<div>TYPE</div> <div>Guidance</div>	<div>VERSION</div> <div>2018</div>
<div>EFFECTIVE</div> <div>December 28, 2018</div>	<div>DOMAIN</div> <div>Cybersecurity</div>	<div>FAMILY</div> <div>NIST Special Publications</div>
<div>REGION</div> <div>United States</div>	<div>INDUSTRY</div> <div>Healthcare & Life Sciences</div>	<div>ADOPTION MODEL</div> <div>Industry Requirement</div>
<div>IMPLEMENTATION COMPLEXITY</div> <div>Moderate</div>		

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

Why it matters

- **Strengthen security governance** Establish clear security roles, responsibilities, and oversight to improve organizational risk management and accountability.
- **Enhance regulatory support** Align internal security practices with HIPAA and other health sector regulations, reducing gaps during compliance assessments.
- **Protect health data and systems** Implement targeted controls to safeguard electronic health records, medical devices, and networks from unauthorized access and breaches.

How SmartSuite supports HICP v1.0 Small Practice

HICP Control Library for Small Practices Organize recommended cybersecurity practices tailored for small healthcare providers and clinics.	Healthcare Asset and System Inventory Track medical devices, workstations, cloud systems, and applications supporting patient care operations.	Security Risk Assessments and Mitigation Identify cybersecurity risks affecting small healthcare environments and track mitigation actions.
Endpoint Protection and Patch Management Monitor endpoint security status, system updates, and vulnerability remediation across clinical systems.	Healthcare Cybersecurity Awareness Training Manage cybersecurity awareness training and track staff participation across healthcare teams.	Security Monitoring and Incident Response Track cybersecurity incidents and response actions affecting healthcare systems and patient data.

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

Health Industry Cybersecurity Practices (HICP) Main Document Provides strategic guidance for healthcare organizations to manage cybersecurity threats. 405d.hhs.gov/information	Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations Describes specific cybersecurity practices for small healthcare environments. 405d.hhs.gov/Documents/HICP-Main-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

- What is U.S. HICP (Small Practice) used for?**
U.S. HICP (Health Industry Cybersecurity Practice) provides practical cybersecurity guidelines specifically tailored for small healthcare practices. Its purpose is to help organizations address prevalent cybersecurity threats affecting the healthcare sector and improve the protection of patient health information.
- Is compliance with U.S. HICP (Small Practice) required or certifiable?**
U.S. HICP is not a mandatory or certifiable framework. However, it serves as recognized industry guidance and can demonstrate a good faith effort towards cybersecurity and HIPAA compliance during audits or investigations.
- What is the scope of U.S. HICP (Small Practice)?**
The HICP Small Practice scope is designed for healthcare organizations with fewer than 10 providers or under 50 employees. It focuses on practical, implementable measures that address the unique constraints and typical risk profiles of smaller healthcare entities.

What are the key concepts or controls required by U.S. HICP (Small Practice)?

Key concepts in HICP Small Practice include implementing strong access controls, regular backups, endpoint protection, security awareness training, and incident response plans. The guidance outlines specific technical and procedural controls appropriate for smaller, resource-limited healthcare settings.

How should a healthcare practice implement U.S. HICP (Small Practice)?

Implementation involves reviewing the HICP guide, performing a risk assessment, and adopting the recommended best practices in manageable phases. Practices should prioritize controls based on assessed risks and resource availability, ensuring foundational cybersecurity hygiene is established.

How does U.S. HICP relate to other healthcare compliance frameworks like HIPAA?

U.S. HICP is complementary to HIPAA, providing actionable guidance for addressing security rule requirements. While HIPAA establishes regulatory obligations, HICP offers practical steps for mitigating cybersecurity risks in accordance with those legal requirements.

What are the ongoing compliance requirements for U.S. HICP (Small Practice)?

Ongoing efforts involve periodically reviewing and updating risk assessments, conducting regular staff training, testing incident response plans, and monitoring system security. Maintaining documentation of these activities helps demonstrate continuous improvement and diligence.

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

SmartSuite can help organizations manage U.S. HICP (Small Practice) compliance by enabling centralized risk tracking, automated control management, and structured evidence collection. It supports audit readiness through customizable reporting and workflows that map directly to HICP's recommended practices and controls.

License included / downloadable: Yes The U.S. Health Industry Cybersecurity Practices (HICP) for Small Practices is published by the U.S. Department of Health and Human Services and is publicly available free from HHS. License included with platform

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