Censinet RiskOps™ for HICP

No-cost Access to Automation and Reporting for the Health Industry Cybersecurity Practices

The HHS 405(d) Health Industry Cybersecurity Practices (HICP), published in 2019, outlines a healthcare-specific approach to cybersecurity. Developed by the HHS in partnership with organizations across the healthcare industry, HICP provides "practical, understandable, implementable, industry-led, and consensus-based voluntary cybersecurity guidelines to cost-effectively reduce cybersecurity risks" for any healthcare organization. Under Health Information Technology for Economic and Clinical Health Act (HITECH), demonstrated use of HICP is considered by the OCR to be a "recognized security practice" which may reduce potential fines or other remedies for resolving potential violations of HIPAA during an investigation, compliance review, or audit.

Censinet RiskOps for HICP simplifies the process of implementing and assessing coverage of these recognized security practices. It is designed for healthcare IT, Security, Risk and GRC teams at large and small organizations (e.g. practice, clinic, hospital, system). An easy-to-use and no-cost solution, Censinet RiskOps for HICP enables you to assess and improve your organization's cybersecurity posture while demonstrating the use of HICP in accordance with the law. It provides robust tools to capture all the evidence needed to demonstrate the 12 months of healthcare industry cybersecurity practices as required by HITECH. Censinet RiskOps for HICP enables another layer of cyber protection which helps you mitigate the impact of cyberattacks by focusing on the prevalent threats to patient safety and data.

HICP Cybersecurity Threats

- E-mail phishing attack
- Ransomware attack
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices that may affect patient safety

HICP Practice Areas

- E-mail Protection Systems
- Endpoint Protection Systems
- Access Management
- Data Protection and Loss Prevention
- Asset Management
- Network Management
- Vulnerability Management
- Incident Response
- Medical Device Security
- Cybersecurity Policies

SOLUTION BRIEF

Everything Needed for Full HICP Support

Censinet streamlines the 200+ pages of HICP documentation into an easy-to-use and powerful workflow that ensures you have a clear picture of your HICP coverage, and the actions needed to improve your organization's cybersecurity posture.

- HICP-based questionnaires aligned to organization size
- Automated generation and tracking of findings and remediations
- Evidence capture to demonstrate best practice adoption
- Coverage reports for Department of Health and Human Services (HHS), Office for Civil Rights (OCR), and for cyber insurance
- Assessment segmentation for evaluating regional or practice area risk exposure
- Custom scheduling of assessments and reassessment to match organizational requirements
- Import of previous assessments for establishing a single repository
- Executive dashboard that reports on overall cyber posture

The assessment workflow guides your organization through an internal audit that maps directly to the 405(d) HICP documentation. It automatically generates a report for your board or HHS that demonstrates your cyber posture. The Censinet RiskOps for HICP Command Center dashboard, automatically populated by assessment activity, provides an executive-level ready view of your HICP coverage, along with progress tracking and a clear indication of investment opportunities.

Get Started Today

Censinet is available at no cost to all qualified healthcare organizations. This freemium license enables everything you need to implement HICP in your organization today and assess HICP coverage over time, identify areas for investment, and capture required evidence needed for the OCR – all with one solution.

To get started today with your no-cost access to Censinet RiskOps for HICP, or to learn more, contact us at hicp@censinet.com.

> "The Health Sector Coordinating Council (HSCC) Cyber Working Group (CWG) established HICP to reduce cybersecurity risk cost-effectively, support organizational adoption, and deliver actionable guidance for protecting patient safety and data. A freely available solution such as Censinet RiskOps™ for HICP paves the way for all healthcare providers, regardless of size, to deploy HICP and reduce risks to patient safety and care delivery."
>
> *- Erik Decker,*
> *Chief Information Security Officer*
> *at Intermountain Healthcare,*
> *Co-Lead of the 405(d) Task Group,*
> *and Chair of the HSCC CWG*

Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.