



Solution Brief

Healthcare Security Services

Comprehensive services to secure protected health information and ensure compliance

With cybersecurity attacks on the rise, the healthcare sector must modernize data protection, security, and management practices to ensure consistency of patient care and compliance of legal regulations.

Though laws like the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) create safeguards to protect patient health information, without proper security measures, healthcare organizations are still vulnerable to malicious actors.

According to the Health Industry Cybersecurity Practices (HICP) guidelines, CISA 405(d) Task Group, which is a part of the Cybersecurity Information Sharing Act of 2015 (CISA), the top five threats common to the healthcare industry include:

1. **Email phishing attacks**
2. **Ransomware attacks**
3. **Loss or theft of equipment or data**
4. **Internal accidental or intentional data loss**
5. **Attacks against connected medical devices that may affect patient safety**

The HICP members have not only isolated the common threat vectors across the healthcare industry, they have also established 10 security strategies to help organizations mitigate those risks. Our team of experts will provide security strategies aligned with these best security practices, prioritized accordingly.

Insight Cloud + Data Center Transformation (CDCT) provides a full suite of healthcare security services and technologies to help organizations address these threats and achieve an effective security posture that meets regulatory and compliance requirements. We provide:

- **Governance, Risk, and Compliance services** that ensure HIPAA/HITECH compliance to NIST SP 800-53/30 Gold Standard and NIST Cybersecurity Framework, including:
 - HIPAA/HITECH/
 - HITRUST/HICP
 - NIST SP 800-53
 - ISO 27001,2
 - PCI DSS
 - GDPR
- **Thorough assessments** of current security practices to ensure compliance with HIPAA and HITECH requirements
- **Penetration testing and vulnerability scanning services** that offer a broad range of testing options designed to uncover potentially costly risks and vulnerabilities
- **On-premises and cloud** security consulting, design, implementation, operationalization, and optimization services
- **Managed Security services and operational support**, including security reporting and analysis, security threat management, and Managed Cloud services
- **Security controls services** to consult, design, architect, implement, operationalize, and optimize security measures for highly regulated and mission-critical healthcare environments
- **Virtual Chief Information Security Officer (vCISO)** with healthcare experience provides executive-level strategic consulting, leadership, and guidance, as well as tactical and strategic Security Program planning
- **Proactive and reactive Incident Response (IR) services**, IR retainer, tabletop exercises, and IR plan development

Why Insight

14 years

of penetration testing, vulnerability assessment, and security management



1,500+

architects, engineers, and subject matter experts in security and service delivery



168+

security products and software offered through Insight

A certified and award-winning partner

of major security solution vendors

Vast experience

developing audit- and board-ready collateral



Our Healthcare Security Services practice draws from a nationwide team of CISOs who are industry Subject Matter Experts (SMEs) in healthcare and government. Our process focuses on governance, regulation, and compliance strategy, customized to individual client threat profiles, and addresses people, process, and technology challenges while reducing cyber risk.

Work with us to:



Ensure healthcare information data privacy and compliance



Improve risk management processes and analysis



Develop operational maturity and resilience and create an effective strategy for business continuity and disaster recovery



Perform tabletop exercises to test and practice the plan, ensuring your team is ready for any potential incident



Rapidly respond to and remediate security incidents to reduce the impact to business



Learn from experienced security professionals and integrate learnings into operational practice

Healthcare areas of expertise

Our Healthcare Security Services provide first-rate support and guidance to help your organization reach and maintain certification and compliance while implementing a comprehensive cybersecurity plan. Our broad and deep expertise includes:

HIPAA expertise

Industry experts and former healthcare CISOs bring decades worth of experience and knowledge to our practice, and our Comprehensive Risk Assessment is based on HIPAA/HITECH requirements.

Health Industry Cybersecurity Practices

We're part of the CISA 405(d) Task Group, a team of public and private organizations advising on healthcare industry cybersecurity.

HITRUST readiness

We're investing resources in Health Information Trust Alliance (HITRUST) and becoming a HITRUST Readiness Assessment partner to ensure that your entire environment is compliant according to HITRUST Common Security Framework Standards.

Proven vCISO leadership

Insight offers the option of engaging a multi-certified vCISO who is experienced in developing and driving healthcare security programs to provide guidance and recommendations to develop a comprehensive cybersecurity program.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com

©2020, Insight Direct USA, Inc. All rights reserved.
All other trademarks are the property of their respective owners.
SB-HCSS-1.1.10.20