A Guide to HITRUST Certification

Streamlining Compliance in Healthcare and Beyond

By Janine Griffiths

🏷 Guides & Datasheets 🏷 Healthcare

Download the rest of NCC Group's Guide to HITRUST Certification.

Download The eBook

Introduction

Healthcare is a top industry targeted by cyber thieves due to a wealth of patient data and an exorbitant number of integrated technologies. One wouldn't have to look far to read about ransomware attacks on hospital systems - in 2018 alone there was at least one healthcare breach per day and 15 million patient records lost.

Then came the Health Insurance Portability and Accountability Act's (HIPAA) Security and Privacy Rules, which mandated "reasonable and appropriate" protections for healthcare data but didn't necessarily specify a way for organizations to prove compliance. Even still, the Office for Civil Rights (OCR) conducted their first audits in 2011 by "covered entities" and their "business associates."

80% of hospitals 81% of health plans adopted the HITRUST CSF in 2019.

The HITRUST CSF is now the most widely adopted framework in the US health industry - more than 80% of hospitals and health plans have adopted this resource or as the basis for their overall program.

23,000 CSF Assessments were conducted in 2019, and that number grows significantly each year.

What is HITRUST?

Lacking a framework and certifying body, HIPAA compliance quickly became an obstacle for healthcare companies. In 2007, a committee of security professionals from various healthcare organizations came together to form an organization called the Health Information Trust Alliance (HITRUST). The organization had a single goal in mind: to standardize security controls around electronic protected health information (ePHI) to create a verifiable path to HIPAA compliance.

Since 2007, HITRUST has carefully selected and assessed controls from federal and industry best practices that support the information protection requirements of HIPAA, funneling them into a certifiable control framework now known as the HITRUST CSF.

> If you want to have something that people can trust, it needs to address new threats and risks when they come up and adapt to the regulations that come from the oversight bodies.

Michael Frederick
VP of Operations, HITRUST

The HITRUST CSF

HITRUST sought to provide healthcare organizations guidance on how to apply security controls with regard to HIPAA. But going further, HITRUST recognized a need for one unified and consistent approach on how to apply security in a global marketplace with varying data protection standards.

HITRUST turned to ISO/IEC 27001 as the foundation for the HITRUST CSF, as its high-level controls are designed to suit almost any organization, in any industry, and in any country. The CSF builds on this foundation with each new release, moving towards its promise of "One Framework, One Assessment" by encompassing requirements from multiple standards and regulations (e.g. HIPAA, HITECH, PCI, ISO/IEC, COBIT, SOC, NIST, and GDPR).

Learn more about achieving HITRUST Certification.

Download the rest of the eBook, or reach out to NCC Group's compliance experts.

Download The eBook   **Reach Out**

nccgroup

Call us on:

General Number:
+44 161 209 5200
24/7 Emergency Incident Response:
+44 161 209 5148

Terms and Conditions

Privacy Policy

Contact Us

Accessibility

Assessment & Advisory

Detection and Response

Compliance

Remediation

Training

Software Resilience

Latest from
@NCCGroupplc

There's been no recent tweets