AMPCUS CYBER

Zero Trust Compliance Service Provider

HIPAA VS HITRUST

HIPAA		HITRUST
Introduced in 1996, a U.S. federal law that mandates privacy and security standards for certain health data.	INTRODUCED & NATURE	Introduced in 2007, a private framework established by the HITRUST Alliance, integrating multiple security standards (NIST, PCI, ISO, etc.).
Enforced by the U.S. Department of Health and Human Services (HHS), specifically the Office for Civil Rights (OCR).	GOVERNING BODY	Developed and maintained by the HITRUST Alliance, a non-governmental, industry-led organization.
Applies to covered entities (healthcare providers, health plans, clearinghouses) and business associates handling Protected Health Information (PHI).	SCOPE	Can be adopted by any organization handling sensitive data (commonly used in healthcare to demonstrate compliance with HIPAA and other frameworks).
Mandatory for U.S. healthcare entities and their business associates under federal law.	LEGAL REQUIREMENT	Voluntary adoption but widely recognized; often pursued to demonstrate higher-level compliance and security rigor in healthcare and related fields.
Requires risk analysis and ongoing risk management under the HIPAA Security Rule; controls are broadly stated.	RISK ASSESSMENT & CONTROLS	Utilizes detailed, prescriptive controls referencing recognized standards, offering a formal process to either accept, transfer or mitigate.
No official government "HIPAA Certification"; compliance is monitored via complaints or random HHS audits.	CERTIFICATION & AUDIT	Offers HITRUST CSF Certification after a formal assessment by accredited CSF assessors; typically i1 and e1 certification lasts for 1 yr and for r2 for 2 years.
Non-compliance can lead to civil penalties ranging from $100 to $50,000 per violation (capped at $1.5 million annually for repeated violations), and criminal penalties of up to $250,000 and/or 10 years in jail for willful neglect or malicious intent.	PENALTIES	No direct financial penalties for non-compliance; however, lack of certification can affect business partnerships, trust, and market competitiveness.
Compliance is continuous, as there is no fixed start-to-finish certification pathway.	IMPLEMENTATION TIMELINE	Typically 6-12 months to implement and prepare for a HITRUST audit, depending on organizational size and complexity.
U.S. centric regulation focused on protecting health data of U.S. individuals.	COVERAGE & MARKET	Recognized primarily in the U.S. healthcare market but can be leveraged globally to showcase a robust security and compliance posture.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com