MEDITOLOGY SERVICES

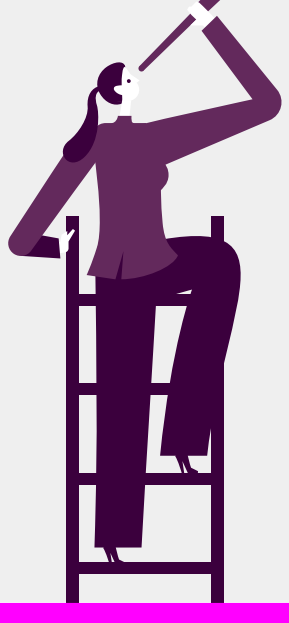
HOW TO COMPLY WITH

OCR'S RECOGNIZED SECURITY PRACTICES (RSPs)

Did you know that the HITECH Act has been amended to require OCR to reduce HIPAA penalties for healthcare organizations that comply with certain "recognized security practices" (RSPs)?[1]



ORIGINS OF OCR'S RECOGNIZED SECURITY PRACTICES (RSPs)



- HITECH Act Amendment HR 7898
- Signed into law by President Biden
- Mitigates OCR civil money penalties and investigations
- RSPs must be fully implemented for the previous 12 months
- Voluntary participation model

WHAT ARE THE RSPs?

Standards, guidelines, best practices, methodologies, procedures, and processes developed under the NIST Act & Cybersecurity Act of 2015

- Aligned with recognized frameworks NIST CSF, NIST 800-53, HICP, & HITRUST[2]
- Evidence of implementation *throughout the enterprise*
- Delivered to OCR via an RSP data request



[1] https://www.congress.gov/bill/116th-congress/house-bill/7898/text

[2] The HITRUST CSF is a validated NIST Informative Reference, with mappings to the NIST Cybersecurity Framework. HITRUST CSF can therefore serve as the foundation for documentation of Recognized Security Controls in alignment with the NIST Cybersecurity Framework

WHY ADOPT RSPs?

REDUCE potential civil money penalties from OCR

OBTAIN early or favorable termination of OCR audits

SUPPORT compliance with the HIPAA Security Rule

STRENGTHEN cybersecurity controls to limit breach impacts

MEDITOLOGY'S RSP COMPLIANCE SERVICES

- NIST CSF Security Risk Assessments documenting compliance with RSPs
- HITRUST certifications validating implementation of RSPs for prior 12 months



- AICPA-level audits to validate RSP implementation throughout the enterprise
- Approach based on decades of experience with HIPAA security and reasonable practices for healthcare entities
- Incorporates our years of experience delivering HIPAA expert witness testimony for OCR

More information about OCR's Recognized Security Practices can be found in Meditology's blog post, New HITECH Amendment Provides HIPAA Safe Harbor for HITRUST Adoption, and the OCR Recognized Security Practices Video Presentation from HHS.

Contact us to learn more about how Meditology can help you document your compliance with OCR's Recognized Security Practices (RSPs).

Meditology is the healthcare industry's preeminent cybersecurity consulting firm and certification body. Our extensive knowledge of the healthcare ecosystem uniquely positions us to address the cybersecurity challenges presented by today's intense threat landscape.

We are proud to serve many of healthcare's most respected providers, payors, and business associates; and to act as expert advisors to the Office for Civil Rights (OCR) and the U.S. Department of Health and Human Services (HHS) on matters of security, privacy, and HIPAA compliance. Together with our sister company CORL Technologies, we are headquartered in Atlanta and maintain offices across the country servicing our national client base.

MEDITOLOGY SERVICES

info@meditologyservices.com
MEDITOLOGYSERVICES.COM