NIH Security Best Practices for Controlled-Access Data Repositories

Updated July 25, 2024

Purpose

This document establishes National Institutes of Health's (NIH) standards for protecting and maintaining privacy of controlled-access data stored at NIH controlled-access data repositories.

NIH Security Standard

NIH controlled-access data repositories that store and share controlled-access data are obligated to protect the confidentiality, integrity, and availability of the data in accordance with NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations", Moderate baseline[1]. NIH controlled-access data repositories choosing a third-party IT system and/or Cloud Service Provider (CSP) for data storage and distribution should provide NIH with an attestation that the third-party system affirming compliance with NIST SP 800-53. Compliance with FedRAMP Moderate[2] or FISMA Moderate[3] satisfy meeting the NIST SP 800-53 Moderate baseline controls.

NIH controlled-access data repositories must provide NIH with reasonable assurances that the repositories are operating at an acceptable level of risk. Managing the oversight and governance of downstream security posture and risk management for organizations external to the NIH is a unique circumstance, which requires the tailoring of federal information technology and security guidance to fit non-federal systems. If adhering to NIST SP 800-53 prevents NIH controlled-access data repositories from meeting their program objectives, NIH can consider the application of NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"[4] and NIST SP 800-171A "Assessing Security Requirements for Controlled Unclassified Information".[5] When an exception request is made to NIH to deploy the NIST SP 800-171 controls for a controlled-access data repository, an independent third-party assessment must be conducted to attest that the repository's application of NIST SP 800-171 provides sufficient protection.

[1] National Institutes of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53). U.S. Department of Commerce, National Institutes of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[2] FedRAMP Program Management Office. (2017). Understanding Baselines and Impact Levels in FedRAMP. https://www.fedramp.gov/understanding-baselines-and-impact-levels/

[3] National Institutes of Standards and Technology. (2017). NIST Risk Management Framework: Federal Information Security Modernization Act (FISMA) Background. U.S. Department of Commerce, National Institutes of Standards and Technology. https://csrc.nist.gov/Projects/risk-management/fisma-background

[4] National Institutes of Standards and Technology. (2020). Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (NIST Special Publication 800-171). U.S. Department of Commerce, National Institutes of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

[5] National Institutes of Standards and Technology. (2018). Assessing Security Requirements for Controlled Unclassified Information (NIST Special Publication 800-171A). U.S. Department of Commerce, National Institutes of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-171a/final

For non-U.S. data repositories with controlled-access data, the protection can align with ISO/IEC 27001[6]/27002[7] ("Information security, cybersecurity and privacy protection — Information security management systems — Requirements" and "Information security, cybersecurity and privacy protection — Information security controls") as a comparable standard to NIST SP 800-53.

To reduce the burden on researchers' access to data and to delegate certain identity and access controls to NIH, controlled-access data repositories are strongly recommended to plan and integrate with the NIH Researcher Auth Service (RAS)[8,9] for authentication and authorization services.

[6] International Organization for Standardization. (2022). Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001). ISO. https://www.iso.org/standard/82875.html

[7] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Information security controls. (ISO/IEC 27002:2022). ISO. https://www.iso.org/standard/75652.html

[8] National Institutes of Health, Office of Data Science Strategy. (n.d.). About the Researcher Auth Service Initiative. NIH ODSS. https://datascience.nih.gov/researcher-auth-service-initiative

[9] For additional information regarding RAS please see: Research Auth Service (RAS) Frequently Asked Questions.