NIH Security Best Practices for Users of Controlled-Access Data

Updated July 25, 2024

Purpose

This document establishes National Institutes of Health's (NIH) standards for users protecting and maintaining security of controlled-access data obtained from NIH controlled-access data repositories in their institutional IT systems and third-party computing infrastructures. This is intended to ensure NIH controlled-access data are kept secure by users and institutional IT systems and third-party computing infrastructures.

Security Standard

All users in possession of NIH controlled-access data must protect this data in accordance with National Institute of Standards and Technology (NIST) SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".[1] Additional security standards are provided below based on workspace location for the data analysis. Non-U.S. users of controlled access data that are unable to align to the NIST SP 800-171 are permitted to use the ISO/IEC 27001[2]/27002[3] "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.

Security Standard for Users and Institutional IT Systems

The users of NIH controlled-access data, and their institutions, are ultimately responsible for maintaining the confidentiality, integrity, and availability of data to which it is entrusted by the NIH. To provide NIH with reasonable assurances, all users must attest their institution is compliant with the NIST SP 800-171. The process for submitting an attestation will vary by repository or access system and may be through agreements or when requesting access to controlled-access data. Non-U.S. users that are unable to attest to the NIST SP 800-171 may attest to the equivalent ISO/IEC 27001[2]/27002[3] standard.

Security Standard for Users of Third-party IT Systems or Cloud Service Providers

Users choosing a third-party IT system and/or Cloud Service Provider (CSP) for data analysis and/or storage for their project should provide the NIH controlled-access repository or access system with an attestation that the third-party system is compliant with NIST SP 800-171.[1] The processes for submitting an attestation will vary and may be through agreements or when requesting access to controlled-access data. Users who choose a NIH-supported third-party IT system or CSP should indicate that in their

[1] National Institutes of Standards and Technology. (2024). 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/pubs/sp/800/171/r3/final

[2] 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

[3] 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

attestation to NIH. NIH-supported third-party IT systems or CSPs should meet the expectation of this security document.

Glossary

Users: any investigator, individual, and requesting institution working with and/or responsible for securing NIH's controlled-access data.