NIST security compliance update

Draft: Feb 06 2025

NIH expects that Approved Users of NIH controlled-access data under the GDS Policy systems comply with NIH Security Best Practices for Users of Controlled-Access Data and maintain such data on institutional IT systems, cloud service providers, and/or third-party IT systems with security standards that meet or exceed NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards. *Note that this policy applies to all controlled- access NIH Brain Development Cohorts (NBDC) data, not just genomic data.* You and your institution will be required to attest to security compliance in order to access the data.

Institutions with Plans of Action and Milestones (POAMs; see links below) to mitigate security risks will be considered compliant (meaning that you can attest to security compliance). Institutions and investigators are expected to protect controlled access data using standards that meet or exceed NIST SP 800-171 or the equivalent ISO/IEC 27001/27002. *These standards follow a risk management framework which allows for security controls under NIST SP 800-171 to be deviated from when institutions have, to the best of their ability, implemented security controls and when there is a POAM to further mitigate the risk.* Institutions and investigators can refer to NIST 800-171 section 03.11.04 Risk Response for more information on how to manage the risk of partially implemented or planned security controls.

Investigator Attestation Language for NBDC Platform (when available):

By checking this box, I, as the PI requesting access to this data, attest that data will be secured, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data. Institutions with Plans of Action and Milestones (POAMs) to mitigate security risks will be considered compliant.

By checking this box, I attest that the cloud service provider and/or third-party IT system used for data analysis and/or storage will secure data, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data.

Signing Official Attestation Language for NBDC Platform (when available):

By checking this box, I attest on behalf of this institution that all institutional IT systems, cloud service, providers, and/or third-party IT systems used for data analysis and/or storage will secure the requested data, at a minimum, in accordance with NIST SP 800-171 or the equivalent ISO/IEC 27001/27002 standards as stipulated by the NIH Security Best Practices for Users of Controlled-Access Data. Institutions with Plans of Action and Milestones (POAMs) to mitigate security risks will be considered compliant.

Links:

1) NIH security practices for controlled-access data repositories: https://sharing.nih.gov/sites/default/files/flmngr/NIH-Security-BPs-for-Controlled-Access-Repositories.pdf
2) NIH security practices for users of controlled-access data repositories: https://sharing.nih.gov/sites/default/files/flmngr/NIH-Security-BPs-for-Users-of-Controlled-Access-Data.pdf
3) Implementation update for data management and access practices under the genomic data sharing policy: https://grants.nih.gov/grants/guide/notice-files/NOT-OD-24-157.html
4) See FAQ number 8 and 9 on extensions and Plans of Action and Milestones in lieu of fully implemented security controls: https://sharing.nih.gov/faqs#/genomic-data-sharing-policy.htm?anchor=57458. NOTE – FAQs will be continually updated.