UNIVERSITY OF DELAWARE
RESEARCH OFFICE

research.udel.edu

January 21, 2025

Important Update to NIH Genomic Data Sharing Policy

The National Institutes of Health ("**NIH**") has issued NOT-OD-24-157 which implements heightened security requirements for controlled-access human genomic data, effective January 25, 2025. The updated NIH Security Best Practices for Controlled-Access Data Subject to the NIH Genomic Data Sharing (GDS) Policy ("**NIH Security Best Practices**") requires compliance with NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations ("**NIST SP 800-171**") for accessing, handling, and storing applicable datasets.

The NIH Genomic Data Sharing Policy (NOT-OD-14-124) issued in 2014 sets forth the federal agency's expectations for the sharing of large-scale human and non-human genomic data. It is important to note that the new NIH Security Best Practices is only applicable to **human** genomic data accessed from an NIH controlled-access repository ("**Covered Repository**") listed here.

Beginning January 25, 2025, NIH Security Best Practices will apply to NIH competing and continuation proposals which include proposed access to human genomic data in a Covered Repository; the security requirements should be taken into consideration when preparing a Data Management and Sharing Plan. The heightened security requirements will also apply to new and renewed NIH Data Use Certification Agreements ("**DUCAs**") for access to the controlled data.

Applicable awards will include an award term requiring NIH Security Best Practices. Investigators who are approved to access controlled datasets ("**Approved Users**") must secure the human genomic data in compliance with NIST SP 800-171, and a Technology Control Plan ("**TCP**") must be established at UD prior to accessing the controlled data. Please submit TCPs to the Research Office for review and approval.

Approved users will also be required to attest to protecting the controlled data in accordance with NIST SP 800-171. Approved Users utilizing a third-party IT system and/or cloud service provider for data analysis and/or storage must provide NIH with an attestation affirming that the third-party system is compliant with NIST SP 800-171.

NIH Security Best Practices requirements do NOT apply to the following:

- Existing NIH DUCAs unless renewed on or after January 25, 2025. Approved Users operating under an existing DUCA signed prior to that date may continue under the terms of access and data security standards detailed in the agreement until the project ends or the DUCA is renewed.
- Data repositories not included in the list posted here.
- Large-scale human genomic data generated by UD as part of an award and stored either by UD or a third-party vendor.
- UD systems which do not interact with the controlled data.

Approved users may utilize UD's third-party vendor for NIST SP 800-171 compliance, TetherView, which provides a cloud-based virtual environment for information security. TetherView's monthly data management fee is $125 per user.

Questions? Please contact RO-Agreements@udel.edu. Additional NIH learning resources are available here.