COGR

Advancing Effective Research Policy

# Summary of Recent Significant Updates to the NIH Genomic Data Sharing Policy

# UPDATED to Reflect Additional Information Provided by NIH on December 31, 2024

## Quick Links

1. **NEW Information Provided by NIH after this Summary was Initially Published on December 16, 2024**

***(Major changes highlighted in yellow)***

**NIH Clarifications:** In mid-December, COGR staff sent NIH questions and concerns regarding the agency's updates to its Genomic Data Sharing Policy ("GDS Policy") as set forth in following notices: Implementation Update for Data Management and Access Practices Under the Genomic Data Sharing Policy (NOT-OD-24-157) (Jul. 25, 2024) and Standard Language for Developer Terms of Access in the Terms and Conditions of Award (NOT-OD-25-021) (Dec. 2, 2024) (collectively the "Notices"). On December 31, 2024, NIH responded to COGR's inquiries, and the major points from this response are summarized below:

- **NIH Provided Additional Information that Narrows the Scope of Projects to which the Developer Terms of Access will Apply: First, NIH clarified that the developer terms of access will apply only when individuals are conducting "Developer Activities"[1] on a federally funded research project that "relate to developing or maintaining an NIH controlled-access data repository" listed here.** Second, NIH provided additional information that clarifies the scope of the activities it considers to be "research," which is not subject to the developer terms of access. The Notices state that "methods development" constitutes research that is exempt from the developer terms of access. **NIH stated that "methods development" includes researchers' development of tools that are unrelated to developing or maintaining NIH controlled-access data repositories. Accordingly, a researcher's use of controlled-access data from an NIH controlled-access repository to develop a novel tool that the researcher will use in their own research does not constitute a Developer Activity unless the work was funded by NIH (or another federal agency) for the specific purpose of being incorporated into an NIH controlled-access repository. NIH stated that it does not anticipate that developer terms of access will apply to a large number of awards.**

[1] *As discussed in more detail below, Developer Activities are defined as "testing platforms, pipelines, analysis tools, and user interfaces that store, manage, and interact with human genomic data from NIH controlled-access data repositories, as well as providing infrastructure development and repository maintenance, but does not include research (e.g., methods development)."*

- **NIH will Specify When the Developer Terms of Access Apply in Funding Instruments: Going forward, any applicable Notice of Funding Opportunity (NOFO), contract, or Other Transaction supporting Developer Activities will indicate the applicability of the Notices and the developer terms of access to ensure awardees understand when the developer access terms apply**.

NIH will be holding webinars on these notices on January 8, 2025, 9:45 - 11:00 a.m. (ET) and January 10, 2025, 9:45 - 11:00 a.m. (ET). COGR anticipates that these clarifications will be discussed during these webinars, and if not, COGR staff attending the webinars will raise these items during any Q&A portion of the webinars and/or ask NIH to provide written clarification in FAQs.

**New NIH GDS FAQS:** After this initial publication of the Summary, NIH also posted two new FAQs regarding compliance with the NIST SP 800-171 cybersecurity standard. As stated in the Notices, researchers accessing human genomic data from NIH controlled-access repositories must attest that any institutional systems they use to access or store the data meet the requirements of NIST SP 800-171. COGR asked NIH to consider granting an extension of the January 25, 2025, effective date to afford institutions additional time to bring their systems into compliance. NIH did not grant an extension, but per these new FAQS NIH will permit institutions to "deviate" from security controls under NIST SP 800-171 "when institutions have, to the best of their ability, implemented security controls and where there is a Plan of Action and Milestones (POAM) to further mitigate the risk." [GDS FAQs, M.8] NIH states in the GDS FAQs that to be considered in compliance, at a minimum, institutions must:

- "Assess their security posture" against NIST SP 800-171 (or equivalent standards at ISO/IEC 27001/27002) to identify gaps where additional risk mitigation is needed.
- Develop a POAM to address identified areas where additional risk mitigation is needed. In developing this POAM, institutions should refer to NIST 800-171, §03.11.04 for "information on how to manage the risk of partially implemented or planned security controls."

**The remainder of this summary has been updated to reflect this new information provided by NIH.**

## 2. Major Impact of the Updates for Institutions

NIH recently made significant updates to the data security requirements ("Updated Requirements") for researchers who want to access controlled-access human genomic data stored in NIH controlled-access data repositories ("Covered Data") such as dbGaP,

and for individuals who assist in building the tools, platforms, and interfaces that are used to develop, manage, and maintain the NIH controlled-access repositories listed here ("Developers"). **The Updated Requirements take effect on January 25, 2025, and NIH is not expected to extend this deadline.**

The Updated Requirements **made two major changes** to requirements for accessing Covered Data:

(1) **Stricter Cybersecurity Standards:** When individuals want to access Covered Data (e.g., deidentified phenotypes and genotypes for individual study subjects) for research (including the creation of analytical tools for that research), **they will need to attest that their institution's IT systems that are used to access and/or store this data meet the cybersecurity standard at NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (NIST SP 800-171). The requirements of NIST SP 800-171 are much stricter than those of NIH's previous security guidance for genomic information. The costs for implementing this cybersecurity standard are substantial, particularly for institutions that do not have any existing data enclaves or third-party/CSP systems that meet NIST SP 800-171.**

**Institutions must assess their IT systems that will be used to access or store Covered Data against NIST SP 800-171. In this assessment they must identify any areas that deviate from the NIST SP 800-171 standard and develop a POAM to mitigate security risks arising from these deviations as described in GDS FAQS M.8. & M.9.**

NIH controlled-access repositories must follow the cybersecurity standards at NIST SP 800-53, Security and Privacy Controls for Information Systems. Developers that manage NIH controlled-access repositories (e.g., performing repository maintenance and infrastructure development) must adhere to this cybersecurity standard.

(2) **Terms of Access Requirements for Developers**: NIH has long required investigators who want to obtain Covered Data for research to agree to NIH-specified data security requirements and terms of access. The Updated Requirements impose similar requirements on individuals who seek to access Covered Data for Developer Activities. Developer Activities are defined as "testing platforms, pipelines, analysis tools, and user interfaces that store, manage, and interact with human genomic data from NIH controlled-access data repositories, as well as providing infrastructure development and repository maintenance"

***that relate to developing or maintaining NIH controlled-access data repositories listed here.***

**Developer Activities do not include research. NIH considers researchers who access data from NIH-controlled access repositories to develop and share analytical tools *that have no relationship to the NIH controlled-access data repository* to be involved in research, as opposed to conducting Developer Activities. However, when a federally funded research project involves access to Covered Data for use in Developer Activities, the PI on the funding application must submit a Developer Use Statement (DUS) to NIH in which they agree that they and the individuals they directly supervise that perform Developer Activities will abide by NIH requirements for accessing the Covered Data**. Among the most significant of these requirements are the obligations for Developers to take NIH-specified data security training and to report to NIH violations of the terms of access or unauthorized data releases within 24 hours of the becoming aware of the incident and providing a follow-up report within three business days of the initial report.

## 3. The Scope of this Summary

NIH has long imposed access requirements on investigators that seek access to Covered Data for research. However, the Notices focus on **(a) the new cybersecurity standards for researchers; and (b) the new access requirements for developers, which did not previously exist. The scope of this summary is limited to the new requirements described in the Notices.**

This summary does not discuss all the GDS Policy's existing requirements for the access and sharing of Covered Data for research. Institutions should take care to assess all applicable GDS Policy requirements when developing processes and policies in this area.

## 4. What Steps should Institutions Consider Taking Now?

**Determine Scope of Projects/Data that may be Subject to the Updated Requirements**: Identify research or Developer Activity projects that access/plan to access Covered Data. For existing projects, determine if the project has an existing Data Use Certification or similar agreements that control access to Covered Data, and if so, when that certification/agreement must be renewed. Institutions should also consider what processes they will need to develop to ensure that new projects subject to the Updated Requirements will be identified and assessed on an ongoing basis. Sponsored programs,

research office, and IRB personnel may need to work together to identify these projects. **As noted, going forward, NIH plans to include notice of when developer access requirements apply in the terms of funding instruments**.

**Assess IT Infrastructure**: Researchers, sponsored programs office personnel, and IT personnel should work together to determine what institutional systems (including any existing third-party systems or cloud service providers [CSP]) meet NIST SP 800-171 and the capacity of those systems to handle the number and types of projects subject to the Updated Requirements. Institutions should compare their IT systems against the standards at NIST SP 800-171. For any areas they identify that deviate from those standards, they must develop a POAM to further mitigate risk arising from those deviations. Institutions should refer to NIST 800-171, §03.11.04 – Risk Response, for information on managing "the risk of partially implemented or planned security controls." [GDS FAQs, M.8 & M.9].

Institutions should also consider what new or amended policies and processes are needed to ensure that new research projects covered by the Updated Requirements are evaluated to ensure they utilize IT systems that comply with NIST SP 800-171.

Incorporating this review as part of research planning efforts is critical because in many cases PIs will be making attestations as to the compliance status of institutional systems in requests that they submit to NIH to gain access to Covered Data. **Importantly, PIs will need to plan for additional costs to address security requirements in proposal budgets. These costs may be substantial**.

**Inform PIs of their Responsibilities and Attestations under the Updated Requirements**: As described below in more detail, PIs performing research and/or Developer Activities may be required to make attestations as to their institution's capacity to meet applicable cybersecurity standards.

PIs performing research work must be made aware of their responsibilities under the applicable NIH terms of access to human genomic data in NIH controlled-access repositories. PIs who lead federally funded projects that involve Developer Activities will also have significant responsibilities and attestations under the developer access terms, including mandatory training and rapid reporting of security incidents.

Institutions need to ensure that PIs are aware of their responsibilities and are prepared to, and do, carry them out. Further, PIs are responsible for ensuring that the people they

supervise are aware of their obligations under applicable NIH terms of access for researchers or developers.

## 5. General Overview of the Updates

The GDS Policy[2] applies to all NIH-funded research that generates or uses "large-scale human or non-human genomic data," and requires the submission of a data sharing plan. This policy requires researchers to deposit Covered Data in an appropriate repository for sharing for research purposes in accordance with GDS Policy requirements and, in the case of human genomic data, informed consent limitations.[3] NIH controls access to individual-level human genomic data contained in NIH repositories. Researchers must submit a request to NIH to access this Covered Data. As part of the request, they must agree to adhere to the Data Use Certification Agreement that contains the terms and conditions of use and follow the Genomic Data User Code of Conduct. If NIH grants their request, they become **Approved Users** and are permitted access to the Covered Data.[4]

As of January 25, 2025, NIH will add the cybersecurity requirements described in the following chart to the GDS Policy:

| Overarching Statement of Practices | Cybersecurity Standard Included in Statement of Practices | Persons/Entities that must Follow the Statement of Practices | Additional Requirements |
|---|---|---|---|
| NIH Security Best Practices for Controlled-Access Data | NIST SP 800-53, Security and Privacy Controls for | NIH controlled-access data repositories on this list [6] and Lead Developers managing these repositories (e.g. | All third-party systems and CSPs that a Lead Developer uses must follow the NIH Security |

[2] *See, generally, NIH, Scientific Data Sharing, Genomic Data Sharing Policy website.*

[3] *Researchers that submit large-scale human genomic data to NIH controlled-access data repositories must provide an institutional certification that has been reviewed by an IRB, which among other things, determines if the institutional certification accurately reflects the terms of participants' informed consent and "adequacy of the consent process for the generation and sharing of data for secondary research use . . ." [NIH, Scientific Data Sharing, About Institutional Certifications website; see, generally, NIH, Scientific Data Sharing, Institutional Certifications website].*

[4] *See, e.g., dbGaP Data Download.*

[6] *The criteria for being considered a NIH controlled-access repository are: (a) support from an NIH funding mechanism or intramural support; (b) provision of long-term storage for, or controlled access to, human genomic data generated/shared under the GDS Policy; (c) review of requests to access the human genomic data directly or via a partner; and (d) use of federal employees in performing that review. [NOT-OD-24-157].*

| | | | |
|---|---|---|---|
| Repositories ("Repository Best Practices") | Information Systems and Organizations.[5] | performing repository maintenance or infrastructure development). | Best Practices and cybersecurity standard to which the Lead Developer attests. |
| NIH Security Best Practices for Users of Controlled-Access Data ("User Best Practices") | NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. | ° All persons that seek and receive approval from NIH to access Covered Data for research ("Approved Users").<br>° Lead Developers who are not managing repositories (e.g., not performing repository maintenance or infrastructure development). | °All institutional systems, third-party IT systems, and CSPs that are used to access/store Covered Data must follow the NIH Security Best Practices and cybersecurity standard to which the Approved User or Lead Developer attests.<br>°Any deviations from the NIST SP 800-171 standard require a POAM to further mitigate security risks arising from the deviations. |

This summary focuses on NIH's User Best Practices because they will have the most significant impact on institutions and their personnel. Individuals involved in the development, management, and/or maintenance of NIH controlled-access data repositories must follow the Repository Best Practices.

The Updated Requirements' provisions on cybersecurity standards will apply to both new and continuing grants and contracts that support activities using Covered Data. **Any individual that seeks, and receives NIH approval, to access Covered Data for research (no matter how funded) will be consider an Approved User and required to certify that the systems they use to access or store the Covered Data comply with the User Best Practices**. The User Best Practices mandate that institutional systems (as well as third-party systems or CSPs) that access or store the Covered Data comply with the cybersecurity standard at NIST SP 800-171. For example, an investigator who wants to access Covered Data from dbGaP for a research project must submit a data access

[5] *If adhering to NIST SP 800-53 would cause a NIH controlled-access repository to be unable to meet program objectives, then NIH can consider permitting the application of NIST SP 800-171 and NIST SP 800-171A instead. In this case, an independent third-party assessment must attest that the alternate proposed standard provides sufficient protection. [Repository Security Best Practices at p. 1].*

request[7] to the appropriate NIH Data Access Committee (DAC) and attest that any institutional, third-party, or CSP systems the investigator will use to store/access the Covered Data meet the requirements of NIST SP 800-171. [NOT-OD-25-021]. However, NIH has stated that if an institution assesses its systems against NIST SP 800-171 and finds gaps, it can develop a POAM to further mitigate the risks arising from deviations from the NIST SP 800-171 standard. [GDS FAQs M.8. & M.9].

**The Updated Requirements also impose new terms of access on Developers** – individuals that access Covered Data to undertake Developer Activities that relate to developing or maintaining NIH-controlled access data repositories. PIs listed on funding applications that include Developer Activities will be considered **Lead Developers.** Lead Developers will be required to submit a **Developer Use Statement** (DUS) to the NIH Developer DAC for approval to access Covered Data.[8] If the Lead Developer is managing a repository (e.g., performing repository maintenance or infrastructure development) then they must attest to NIH Security Best Practices for Controlled-Access Data Repositories, including the cybersecurity standard at NIST SP 800-53. If the Lead Developer is not managing a repository, they must attest to the NIH Security Requirements for Users of Controlled Access Data, including the cybersecurity standard at NIST 800-171. If the Lead Developer is using any third-party or CSP systems, they must attest that those systems meet the cybersecurity standard that the Lead Developer has attested it will follow.

Additionally, NIH will require that the Lead Developer and the individuals they directly supervise who are conducting the work described in the DUS ("Supervisees") agree to abide by the DUS and all other terms of access. These terms include taking prescribed NIH research security training modules, protecting the data against unauthorized use/access, and reporting any security incidents to NIH within 24 hours after their identification (and providing follow-up reports in three business days). Once NIH approves the DUS, the Lead Developer and their Supervisees are considered "**Approved Developers**."

**It is important to remember that the roles of Approved User (e.g., an investigator who requests Covered Data for research) and Approved Developer are not mutually exclusive, and an Approved Developer can also be an Approved User**. Accordingly, it is possible that an individual listed as the lead PI on a Data Access Request for research

[7] *See, e.g., NIH, Scientific Data Sharing, How to Request and Access Datasets from dbGaP website.*

[8] *For grants and cooperative agreements, the DUS must be submitted at Just in Time. For contracts and Other Transactions, it must be submitted at the time of proposal or application for funding.*

may also be separately listed as the Lead Developer on a Developer Use Statement.[9] However, NIH has clarified that for activities to constitute "Developer Activities," they must relate to "developing or maintaining NIH controlled-access data repositories."

**In short, any person that seeks access to Covered Data for any purpose must agree to the applicable NIH terms of access (i.e., terms of access for researchers or for developers) through the submission of the required attestations/certifications. Terms of access for Approved Users that access Covered Data for research include the cybersecurity requirement that any institutional or third-party systems used to access or store the Covered Data meet NIST SP 800-171.[10]**

### 6. Effective Date

The Updated Requirements take effect on January 25, 2025 ("Effective Date"). On that date, any new or renewing agreements that involve projects requiring access to Covered Data will contain the new cybersecurity standards and the new developer terms of access.

The Updated Requirements will apply to:

- Competing grant applications (new or continuing) and proposals for contracts submitted on/after the Effective Date;
- Other Transactions executed on/after the Effective Date; and
- Continuing grants/contracts/Other Transactions that are ongoing as of the Effective Date.

**Approved Users who are operating under existing Data Use Certifications or similar agreements that were signed before the Effective Date can continue under the terms of access and data security standards detailed in those certification/agreements; they will not need to address the new security standards until their certifications/agreements require renewal.** [GDS FAQs, M.3].

**COGR asked NIH if it would consider a blanket extension of the Effective date, and NIH advised it would not be issuing an extension**. NIH confirmed in the GDS Policy FAQs that it would not provide an extension. However, in those FAQs, NIH also states

[9] *"If the Approved Developers plan to conduct research (e.g., methods research), they must submit a Data Access Request for research to the appropriate NIH DAC for review and approval." [NOT-OD-25-021].*
[10] *As noted, NIST SP 800-53 is the cybersecurity standard that applies to the NIH controlled-access repositories themselves, and the Developers that manage these repositories must attest to this standard.*

that if an institution assesses its systems against NIST SP 800-171 and finds gaps, it can develop a POAM to further mitigate the risks arising from deviations from the NIST SP 800-171 standard. [GDS FAQs M.8. & M.9].

### 7. Detailed FAQs Regarding New Cybersecurity Requirements and New Terms of Access for Developers

The remainder of this summary provides greater detail on the major points of the Updated Requirements in FAQ form. **These FAQs focus on the new cybersecurity standard for research and the Developer terms of access because those items are the focus of the Updated Requirements. Individuals seeking access to Covered Data for non-Developer Activities must meet similar terms of access set forth in the NIH Data Use Certification Agreement and Genomic Data User Code of Conduct.**

### 8. What cybersecurity requirements must Approved Users and Approved Developers attest to?

Approved Users must follow the NIH Security Best Practices for Users of Controlled-Access Data ("User Best Practices"). The User Best Practices require that Users attest that any institutional systems and third-party/CSP systems that are used to access or store Covered Data meet the NIST SP 800-171 cybersecurity standard. NIH does not expect Users to have an independent assessment of their systems performed as part of this attestation requirement. [GDS FAQs, M.7.] As noted, NIH has stated in FAQs that if an institution assesses its systems against NIST SP 800-171 and finds gaps, it can develop a POAM to further mitigate the risks arising from deviations from the NIST SP 800-171 standard. [GDS FAQs M.8. & M.9].

Presently, NIH permits Approved Users to attest to compliance with either revision 2 or revision 3 of NIST SP 800-171. [GDS FAQs, M.5]. Non-U.S. users who cannot attest to NIST SP 800-171 may attest to the equivalent ISO/IEC 27001/27002 standard. **The process for submitting the attestation may vary by repository or access system.** In some cases, the Approved User may make the attestation as part of their request for access to Covered Data, and in other cases it may be obtained through other agreements. [NOT-OD-24-157].

NIH controlled-access repositories on this list, and the Developers that manage these repositories[11] (e.g., perform maintenance and infrastructure development for the repository) must follow the NIH Security Best Practices for Controlled-Access Data Repositories ("Repository Practices"). [GDS FAQs, M.2.] The Repository Best Practices require the repositories to meet the NIST SP 800-53 cybersecurity standard. [NOT-OD-25-021].

### 9. What are the defined roles under the Updated Requirements, i.e., what is an "Approved User," "Developer," and "Lead Developer"?

"**Users**" are U.S. and non-U.S. individuals who seek to access Covered Data from NIH controlled-access repositories. When NIH approves a User's request to access the Covered Data, the User becomes an "**Approved User.**" Approved Users and their institutions are responsible for maintaining the confidentiality, integrity, and availability of Covered Data. [NOT-OD-24-157]. Approved Users must adhere to the terms and conditions of the data access request, Data Use Certification Agreement, and Genomic Data User Code of Conduct. Additionally, if the research is federally funded, Approved Users and their institution must abide by any data terms and conditions contained in the funding mechanism.

For example, Investigator X, as PI, wants to access Covered Data from dbGaP for a research project. On January 26, 2025, Investigator X submits a data access request to the appropriate NIH DAC. As part of this request, Investigator X must agree to abide by the applicable terms of access, including attesting that the institutional systems and third-party/CSP systems used to access and store Covered Data, meet NIST SP 800-171.

"**Developers**" are individuals who build tools and are involved in "testing platforms, pipelines, analysis tools, and user interfaces that store, manage and interact" with Covered Data and/or who provide infrastructure development and repository maintenance that relate to NIH controlled-access repositories (Developer Activities). Developer Activities do not include research, including "methods development." [NOT-OD-24-157]. NIH has clarified that "methods development" includes researchers access to Covered Data to develop tools that they use in their own research unless the work was

[11] *As noted, Lead Developers that are NOT managing a NIH controlled-access repository (e.g., not performing repository maintenance or infrastructure development, must follow the User Best Practices, including adherence to NIST SP 800-171. [NOT-OD-25-021].*

funded by NIH (or another federal agency) for the specific purpose of being incorporated into an NIH controlled-access repository.

A "**Lead Developer**" is the PI (or PD) listed on a funding application that involves Developer Activities. Each Lead Developer must be associated with an institution that is applying for/receiving federal support through a "funding mechanism that has incorporated the developer terms of access." The Lead Developer must submit a Developer Use Statement (DUS)[12] to the NIH Developer Data Access Committee (DAC). Once NIH approves the DUS, the Lead Developer and their Supervisees are "**Approved Developers."** [NOT-OD-24-157, NOT-OD-25-021]. Controlled-access repositories may provide access to Approved Developers in accordance with the DUS. The approval lasts for two years.

For example, Investigator Y plans to access Covered Data from dbGaP for use in developing the infrastructure of an NIH controlled-access repository as part of specific activities funded under a grant proposal submitted to NIH on January 26, 2025. Investigator Y is the PI on the grant proposal, which NIH funds. At JIT, Investigator Y submits a DUS to the NIH Developer DAC. As part of the DUS, Investigator Y must agree to abide by the applicable terms of access, including attesting that all institutional and third-party/CSP systems used to access or store the Covered Data meet NIST SP 800-053. If NIH approves the request, then Investigator Y and Investigator Y's Supervisees are Approved Developers and can access and use the Covered Data in accordance with the terms and conditions of the DUS, the Developer Terms of Access, the Developer Code of Conduct and applicable grant terms and conditions.

**The roles of Developer and researcher are not mutually exclusive. Based on the text of NOT-OD-25-021,**[13] **a Developer conducting research can be both an Approved User and Approved Developer**. Thus, a PI may assume the role of Approved User to access Covered Data to conduct research, as well as assuming the role of Lead Developer to supervise the conduct of Developer Activities with that same data. So, in the previous example concerning Investigator X, if Investigator X intends to use the Covered Data from dbGaP both for methods development for research and as part of a project funded by an NIH grant for the creation analysis tools that will be incorporated into an NIH

[12] *The DUS must be submitted no later than JIT for grants/cooperative agreements, with the proposal for a contract, or with the application for funding via an Other Transaction.*

[13] *Approved Developers that plan to conduct research must submit a Data Access Request.*

controlled-access database, then under the language of NOT-OD-25-021, Investigator X would:

- Submit a data access request/Data Use Certification Agreement to the appropriate NIH DAC to conduct the research activities, and once approved become an Approved User; and
- Submit a Data Use Statement to the NIH Developer DAC (discussed below) as the Lead Developer to conduct the Developer Activities and once approved, the Lead Developer and any Supervisees would become Approved Developers.

### 10. What other terms of access must the Lead Developer and other Developers adhere to?

They must meet the "Minimum Standard Operating Procedures for Developer Oversight" set forth in NOT-OD-24-157, which include the following requirements:

- Lead Developer submits a DUS to the NIH Developer DAC.
- Lead Developers and their Supervisees (collectively "Developers") and the Lead Developer's institution agree to abide by the **Developer Terms of Access** (discussed below), which are incorporated into the funding mechanism.

### 11. What are the Minimum requirements for a DUS?

The DUS must include the following information and attestations:

- Justification as to why development access is necessary.
- Description of intended Developer Activities.
- If the Lead Developer is managing a repository, attestation that they understand and will adhere to Repository Security Best Practices and list the cybersecurity standard being implemented (i.e., NIST 800-53).
- If the Lead Developer is not managing a repository, attest that they understand and will adhere to the User Security Best Practices and list the cybersecurity standard being implemented (i.e., NIST 800-171).
- If Lead Developer is using a third-party IT system or CSP, provide the name of the third-party system/CSP and attest that the third-party system/CSP complies with Security Best Practices to which the Lead Developer attested and list the cybersecurity standard being implemented.
- Acknowledgement that the Lead Developer's Supervisees and institution will adhere to the terms of access and any additional NIH program, institute, or center (IC) specific requirements for controlled access.

- Acknowledgement that the Lead Developer and Supervisees have reviewed the IT Administrator or Developer role-based NIH Security Awareness Course at https://irtsectraining.nih.gov/publicUser.
- If the Lead Developer works with a developer partner that requires access to the Covered Data, provide the name of the partner's institutions and partner's program manager.[14] [NOT-OD-24-157]

### 12. What are the Developer Terms of Access?

The Developer Terms of Access are a part of the terms and conditions of an award. They include the following requirements grouped by the party/parties responsible for the requirement:

Lead Developer's Institution:

- The Lead Developer's institution agrees that if the Lead Developer's DUS is approved, then the Lead Developer and the Lead Developer's Supervisees will become Approved Developers. All Approved Developers must abide by the DUS and terms of access.[15]
- The Lead Developer's institution and the Lead Developer acknowledge they are responsible for ensuring that all uses of the Covered Data are consistent with all applicable laws and regulations and relevant institutional policies.

Lead Developer:

- Data must be used as described in the DUS and any new use requires submission and approval of a revised DUS.
- The Lead Developer acknowledges they are responsible for ensuring that all uses of the Covered Data are consistent with all applicable laws and regulations and relevant institutional policies.
- The Lead Developer agrees to notify the NIH Developer DAC of any actual or suspected violation of the Developer Terms of Access or any additional program or

[14] *Note, if the partner is not directly funded by the federal government, then NIH will only provide access to Covered Data if (a) the Lead Developer and developer partner enter into a contract containing the terms of access.; (b) NIH approves the partner, as listed in the Lead Developer's DUS; (c) the partner submits its own DUS to NIH; and (d) the partner and institutional signing official co-sign the DUS agreement and any additional program or IC specific requirements. [NOT-OD-25-021].*

[15] *As noted, if Approved Developers plan to conduct research (as opposed to just conducting Developer Activities) they must submit a Data Access Request (DAR) for research to the appropriate NIH DAC. [NOT-OD-25-021].*

IC-specific requirements, within 24 hours of the time the incident is identified (discussed below).
- The Lead Developer will complete appropriate forms and provide appropriate reports when renewing a DUS, closing out a DUS, or reporting any violations of the Terms of Access.

Approved Developers (i.e., the Lead Developer and Supervisees):
- Approved Developers must abide by the DUS and terms of access.
- Approved Developers must agree that they reviewed, understand, and will abide by the Security Best Practices for Repositories or Users, as applicable.
- Approved Developers agree that they will not attempt to identify or contact (directly or indirectly) any individual participant or their families.
- Covered Data in NIH controlled-access repositories are protected by Certificates of Confidentiality. Approved Developers agree to abide by the terms of any Certificate of Confidentiality that protects the Covered Data they access, including protecting participants' identifiable, sensitive information from compelled disclosure and defending the authority of the Certificate of Confidentiality against legal challenges.
- Approved Developers agree that they will not distribute Covered Data or data derivatives to any person/entity not identified in the approved DUS without NIH's written approval.
- Approved Developers agree that they will never sell any Covered Data or data derivates at any time, for any reason.
- Approved Developers must review the NIH Security Awareness Course training for IT Administrator or Developer.
- Approved Developers agree to notify the NIH Developer DAC (DeveloperAccessDAC@od.nih.gov) of any unauthorized data access or sharing breaches of data security or inadvertent data releases that may compromise data confidentiality within 24 hours of the time the incident is identified (discussed below).
- Approved Developers acknowledge that NIH disclaims all warranties of any type regarding the Covered Data; that no party provides any indemnification of any type; and that each party will be liable for any loss, claim, damage, or liability that the party incurs as a result of its activities under the DUS, except that NIH's liability is subject to the limits of the Federal Tort Claims Act.
- Approved Developers agree to follow the **Developer Code of Conduct** (discussed below).

Additional Requirements:

- NIH may publicly post Information about Developer Activities (i.e., name of Lead Developer's institution, intended Developer Activities, de-identified information about inadvertent data releases, breaches of data security or other violations). [NOT-OD-25-021]

**Note:** The Data Use Certification Agreement includes similar terms and conditions of access for individuals obtaining Covered Data for non-Developer Activities.

### 13. What does the Developer Code of Conduct require?

The elements of the Developer Code of Conduct from NOT-OD-25-021 are listed below. (NOTE: Many of these elements are also elements of the Developer Terms of Access):

- *Use data for the sole purposes of developing, testing, and implementing the environment and building the infrastructure during both development and production phases of deployment (these functions include software development to enable researchers to access and analyze data);*
- *The Approved Developers agree to make no attempt to identify or contact, either directly or indirectly, individual participants or their families.;*
- *Maintain the confidentiality of the data and not distribute data or derivative data (e.g., imputed datasets and single nucleotide polymorphisms) to any entity or individual without appropriate written approvals from the NIH;*
- *Implement administrative and technical safeguards to prevent unauthorized access to the data and adhere to the NIH Security Best Practices for Controlled-Access Data Repositories, or if applicable, NIH Security Best Practices for Users of Controlled-Access Data;*
- *Ensure that only authenticated and authorized users can gain access to data files, as appropriate;*
- *Report any actual or suspected inadvertent data access or release, breach of data security, or other DMIs in accordance with the terms described herein to the NIH Developer DAC (DeveloperAccessDAC@od.nih.gov) with a copy to the GDS mailbox (GDS@nih.gov) within 24 hours of when the incident is identified;*
- *Allow information about its use of controlled-access data to be publicly posted. The information may include the name of the Lead Developer's institution, intended developer activities, in both a scientific and lay format, and de-identified information about inadvertent data releases, breaches of data security, or other violations;*
- *Acknowledge that no ownership rights of the datasets (including derived or derivative data) are granted to developers or their affiliates.*

- *Lead Developers who want to perform research must submit a Data Access Request (DAR) to a relevant NIH DAC for review and approval.* [NOT-OD-025-121].

**Note**: The Genomic Data User Code of Conduct contains similar terms and conditions for individuals accessing data for non-Developer Activities.

### 14. What happens when a DUS expires or is closed out?

When a DUS expires after two years, it may be renewed or closed out. To renew the DUS, the Lead Developer must submit a renewal request to the NIH Developer DAC that sets forth:

- A description of how access contributed to Developer Activity and why additional access is needed.
- Affirmation that the Lead Developer and Supervisees adhered to any program or IC specific requirements for access.
- Reports of any data misuse, breach, unauthorized disclosure of data, or security incident.

If the renewal is granted, the DUS is renewed for two years.

When access to the Covered Data is no longer required, the Lead Developer must close-out the DUS by submitting a close-out request to the NIH Developer DAC. The request must address all the aforementioned elements except for specifying why additional access is needed.

At the time of close-out, the Approved Developer agrees to "destroy all copies, versions, and data derivatives (e.g., imputed datasets and single nucleotide polymorphisms) of the data retrieved from NIH controlled-access repositories, on both local servers and hardware." If CPS were used, then Covered Data and cloud images must be deleted from cloud storage, "virtual and physical machines, databases, and random-access archives." [NOT-OD-25-021]. Institutions will need to consider how they will be able to definitively identify/document where and by whom all records of the data were kept and confirm/document the destruction of this data.

**Note**: The Data Use Certification Agreement contains similar close-out requirements for individuals access Covered Data for non-Developer Activities.

### 15. What types of data security and unauthorized access/release issues must Developers report to NIH?

NOT-OD-25-021 describes two categories of reportable events: **Unauthorized Data Releases** and **Term of Access Violations**. It also uses the term "**Data Management Incident**" **(DMI)** in discussing each of these categories of reportable events. The notice does not define "DMI," but it does state that a DMI constitutes one example of a Term of Access violation. Accordingly, a Term of Access Violation that also constitutes a DMI involving an Unauthorized Data Release should meet the more stringent reporting requirements for Unauthorized Data Releases (i.e., initial report in 24 hours and follow-up report in three business days). For example, a violation of the requirement to store Covered Data in an institutional system that meets NIST SP 800-171 that leads to an unauthorized individual accessing the Covered Data would meet the criteria for a Term of Access Violation, an Unauthorized Data Release, and a DMI. Alternatively, if an Approved Developer fails to review the required NIH training module but this violation does not result in unauthorized Covered Data access, then this would constitute a Term of Access violation but not an Unauthorized Data Release (and presumably not a DMI).

Notification of an Unauthorized Data Release by Developers:

- **Events Considered to Constitute an Unauthorized Data Release**: Any unauthorized access to or sharing of Covered Data, breaches of data security, or inadvertent data releases that may compromise data confidentiality.
- **Reporting Timeframe**: Initial report - **24 hours** after incident is identified; follow-up report – **within three business days** after the initial report is made.
- **Report to**: NIH Developer DAC at DeveloperAccessDAC@od.nih.gov with a copy to GDS mailbox at GDS@nih.gov.
- **Initial Report Content**: The Approved Developers make the initial report by providing any known information regarding the incident and description of the activities/processes in place to define and fully remediate the situation.
- **Follow-up Report Content:** The Lead Developer's institution provides a detailed written, follow-up report specifying the date and nature of event, remedial actions taken or planned to be taken, and plans and processes developed to prevent further problems, including implementation timelines.
- **NIH Follow-Up:** The Lead Developer's institution must provide any additional documentation requested by the NIH Developer DAC, including verification that remediation has been implemented. NIH, or its designee, may also conduct its own investigation of any incident or policy violation, and the Approved Developers,

Lead Developer, and Lead Developer's institution must cooperate, provide any requested information, and work with NIH to implement appropriate remediation.

Notification of Terms of Access Violations by Developers:

- **Events that Constitute a Term of Access Violation**: Any violation of the terms and conditions governing access to Covered Data.
- **Reporting Timeframe**: Within 24 hours of when incident is identified.
- **Report to**: NIH Developer DAC DeveloperAccessDAC@od.nih.gov with a copy to the GDS mailbox at GDS@nih.gov.
- **Initial Report Content**: The Lead Developer provides notices of any actual or suspected violations of any terms or conditions applicable to controlled-data access.
- **Follow-Up**: The Lead Developer agrees to provide additional information as requested by NIH.

**NOTE:** Individuals who access Covered Data for non-Developer Activities must make similar reports of violations of terms of access and unauthorized data releases per the requirements of the Data Use Certification Agreement.

### 16. What sanctions may NIH impose for violations of Developer terms of access?

NIH may immediately revoke or suspend access to Covered Data if Approved Developers are found to have violated any applicable terms or requirements of the NIH controlled-access data repository or other NIH policies and procedures. NIH will consider a Lead Developer's compliance record when determining whether to approve an access request. NIH may also revoke access to Covered Data "for any reason without cause." Additionally, to the extent that requirements are incorporated into the terms and conditions of the award, NIH will be able to utilize enforcement mechanisms/sanctions that are available in cases of noncompliance with grant/contract terms.

**NOTE:** Similar sanctions apply to violations of the Data Use Certification Agreement by individuals who access Covered Data for non-Developer Activities.

### 17. Who should institutions contact at NIH with questions?

Inquiries to NIH on the GDS Policy may be directed to the Office of Science Policy at gds@mail.nih.gov. Additional information regarding the GDS Policy, including resources for determining when the policy applies, developing a GDS Plan, and preparing the

institutional certification required to access large-scale human genomic data can be found at https://sharing.nih.gov/genomic-data-sharing-policy/about-genomic-data-sharing/gds-policy-overview.

## 18. Pertinent Documents

- Standard Language for Developer Terms of Access in the Terms and Conditions of Award (NOT-OD-25-021) (Dec. 2, 2024)
- Implementation Update for Data Management and Access Practices Under the Genomic Data Sharing Policy (NOT-OD-24-157) (Jul. 25, 2024)
- NIH Security Best Practices for Users of Controlled-Access Data (updated Jul. 25, 2024)
- NIH Security Best Practices for Controlled-Access Data Repositories (updated Jul. 25, 2024) ("Repository Security Practices")
- NIH Genomic Data Sharing Policy (NOT-OD-14-124) (Aug. 27, 2014) ("GDS Policy")
- Genomic Data Sharing Policy FAQS ("GDS FAQs")
- NIST SP 800-171 (r.3); NIST SP 800-171 (r.2); NIST SP 800-171 (r.1). Note: NIH cites to NIST SP 800-171 r.3. (the current version of this standard) with regard to the development of a POAM. However, NIH states that institutions that cannot attest to NIST SP 800-171 r.3 may attest to NIST 800-171 r.2 or r.1. [GDS FAQs at M.6].

***For any questions regarding this summary, please contact Kris West, COGR's Director of Research Ethics & Compliance at kwest@cogr.edu.***