National Institutes of Health (NIH) Controlled-Access Data Repository Guidebook to Adhere to "Required Security and Operational Standards for NIH Controlled-Access Data Repositories" (NOT-OD-25-159)

VERSION 1.0

September 2025

RECORD OF DOCUMENT CONTROL

Modifications made to this document are recorded in the version history below. This document history shall be maintained throughout the life cycle of this implementation guide.

Version	Implementation Date	Summary of Changes	Section(s) Updated	Changes Approved By
1	09.22.2025	First Release	All	OCIO, OSP

Table of Contents

This page left intentionally blank

A. Purpose

To help meet the requirements stated in "Required Security and Operational Standards for NIH Controlled-Access Data Repositories" (NOT-OD-25-159), NIH is providing this Guidebook. This NIH CADR Guidebook provides a detailed explanation of the procedures for meeting the requirements in NOT-OD-25-159 and a description of all responsible parties. For the purposes of this NIH CADR Guidebook, both NIH CADRs and access management systems subject to these requirements will be referred to as NIH CADRs.

B. Instructions

For each standard, the Guidebook provides details on **Applicability**, **Steps to Comply**, **Additional Guidance**, **Acceptable Evidence**, and the **Effective Date**.

1. **Applicability**: Check this first to determine if the standard applies to NIH Institutes, Centers, and Offices (ICO) staff only, repositories, access management systems, or a combination. Note that access management systems can operate independently of a repository, while integrated access management systems are considered part of the repository.
2. **Requirement** and **Steps to Comply**: Review these for detailed information on the standard and how to meet it.
3. **Additional Guidance**: Links or references further reading when applicable.
4. **Acceptable Evidence**: Check this for details about what must be sent to the ICO Information System Security Officer (ICO ISSO) as proof of fulfilling the requirement.

C. Options for Satisfying Requirements

Standards can be satisfied by:

- Directly adopting standards or partnering with systems that have met these standards. For example, repositories partnered with separate access management systems can rely on those systems to satisfy standards applicable to access management systems. Direct adoption requires:
    - A signed attestation by the ICO Senior Official affirming compliance with all standards. This attestation (see page 9) must be sent to OCIO at securenihdatasciencesupportservicesteam@mail.nih.gov.
    - All evidence, including information security artifacts, be sent to the ICO ISSO prior to each deadline. Intramural NIH CADR staff can find their ICO ISSO here. External NIH CADR staff who do not know their corresponding ICO ISSO can inquire by emailing OCIO with NIH CADR details at securenihdatasciencesupportservicesteam@mail.nih.gov.
- Disabling all access to controlled-access data and ceasing processing new requests until standards can be met.
- Migrating controlled-access data to another NIH CADR that has met all standards.
- Recommending specific controlled-access data to OCIO for decontrolling.
    - If this option results in the NIH CADR no longer meeting the NIH CADR criterion, follow SOP for Maintaining and Modifying the NIH CADR List in Appendix A.

A standard operating procedure (SOP) detailing these options can be found in Appendix B. NIH CADRs systems that provide unrestricted- or tiered-access may continue offering these access models; however, their controlled-access components must fully comply with all applicable standards.

D. Glossary of Terms

Access Management System: Systems and processes that control and manage permissions to ensure that only authorized individuals or systems can perform specific actions on a particular resource, i.e., accessing data in a repository. For the purposes of these standards, access management systems refer only to those systems that can exist independently of a repository. If a repository has an integrated access management system, standards for both access management systems and repositories are applicable.

Cloud Workspaces: Secure virtual environments that provide authorized users with access to computing resources, applications, and data over the internet. Cloud workspaces are not designed for long-term storage or archiving of data. Instead, they support active data processing and computation of data pulled from permanent data repositories.

Data Coordinating Centers (DCCs): An organizational entity responsible for the central management, integration, and dissemination of data across multiple sites or projects within a research consortium or program. DCCs are project-specific and time-limited and are not intended for long-term data access and preservation.

Data Access Requester: The individual who prepares and submits requests, Project Renewals, and Project close-outs. A Data Access Requester is a permanent employee of their institution at a level equivalent to, but not limited to, that of an academic professor (e.g., assistant, associate, or non-tenure or tenure-track professor) or senior researcher; has oversight responsibility for others named on the request who will be granted access to the data; and can be accountable for ensuring that all aspects of data usage align with the terms of the agreement and institutional requester policy. This individual cannot be a lab technician or trainee, e.g., post-doc or graduate student.

IC Authorizing Official: A senior official within the Institute of Center (IC) who holds budget authority for the IC system and is responsible for the mission/business operations supported by the system (definition adopted from the National Institute of Standards and Technology (NIST), Special Publication 800-37, Appendix D, page 114). Typically, an IC Executive Officer (EO) or Chief Information Officer (CIO) will serve as the IC Authorizing Official.

ICO Senior Official: An NIH federal employee within an NIH Institute, Center, or Office (ICO) who holds responsibility for overseeing the operations and compliance of NIH-controlled-access data repositories (NIH CADRs) within their respective ICO. The ICO Senior Official ensures adherence to the "Required Security and Operational Standards for NIH Controlled-Access Data Repositories" (NOT-OD-25-159), manages communication and coordination with the Office of the Chief Information Officer (OCIO), and is accountable for the registration, monitoring, and decontrolling of CADRs. The ICO Senior Official is the IC Authorizing Official by default, however, ICOs may designate an alternative if such an official does not exist or if the ICO has determined a more suitable alternative such as the ICO Chief Information Officer or Data Science Program Senior Official.

ICO Information System Security Officer (ISSO): The principal contact for coordination, implementation, communication, and application of IT security policies within their specific NIH Institute, Center, or Office (ICO). The ISSO works in conjunction with the NIH Chief Information Security Officer (CISO) and is the primary contact for receiving and reporting notifications from HHS and the NIH Information Security Program, including abnormal alerts and scan reports, security incidents and compromises. The ISSO is responsible for collecting, assessing, and

submitting security artifacts within the Governance, Risk, and Compliance (GRC) Tool Cyber Security Assessment and Management (CSAM). If the ICO does not have an ISSO, the ICO will designate an alternative.

Institutional Signing Official (SO): The label, "Institutional Signing Official" refers to the individual that has institutional authority to legally bind the institution in administrative matters. The individual fulfilling this role may have any number of titles in the institution but is typically located in its Office of Sponsored Research or equivalent.

Lead Developer: Lead Developer is the Principal Investigators (PI) listed as the Project Directors (PD) or PI on the funding application; for intramural, the Lead Developer is the developer team lead at the managing NIH ICO repository. Lead Developers work includes testing platforms, pipelines, analysis tools, and user interfaces that store, manage, and interact with human data from NIH CADRs, as well as providing infrastructure development and repository maintenance, but does not include research (e.g., methods development). See NOT-OD-24-157 for additional information.

NIH Controlled-Access Data Repositories (NIH CADRs): NIH data repositories and data access management systems that meet the following criteria must therefore adhere to these standards:

- Are part of the Intramural Research Program or are supported by an NIH cooperative agreement, intramural funding, contract, Other Transaction, or grant;
- Provide long-term storage for, or provide access to, data for research purposes (hereafter, "data");
- Control access to data by prospective review of data access requests or partner with access management systems that control access by prospective review of requests; and
- Use federal employees to conduct reviews of requests and authorize access or partner with access management systems that use federal employees for those purposes.

Repositories that only facilitate direct sharing between investigator teams, **cloud workspaces** that only temporarily store data, **data coordinating centers**, and similar activities that do not manage data sharing beyond specific programs or initiatives, are not considered NIH CADRs.

National Institutes of Health, Office of the Director, Office of the Chief Information Officer: The Office of the Chief Information Officer (OCIO) is the principal NIH Office responsible for NIH IT governance, guidance, and protection of NIH IT capabilities, scientific and research computing services to support NIH's mission as the Nation's steward of medical and behavioral research.

National Institutes of Health, Office of the Director, Office of Science Policy: The NIH Office of Science Policy (OSP) works across the biomedical research enterprise to ensure NIH policy evolves in tandem with national security interests, science and technology, agency priorities, data security, and participant protections.

Repository: A database capable of storing and enabling the retrieval of information from a specific domain of science or multiple domains. Repositories are designated for the stable retention of data, as opposed to a temporary storage site with a sunset date intended for interim data holding prior to transfer. Data repositories hold data that researchers make available for others to reuse. They may make data open to the public or restrict access to protect privacy and confidentiality of data from human research participants.

Submitting Investigator – The individual responsible for assuring to NIH that the data are appropriate to share as signatory to the data submission form or certification.

E. Attestation Statement

On each effective date, NIH CADRs are required to confirm compliance with the relevant categories of requirements by having their ICO Senior Official sign the attestation statement and submit it to the OCIO at securenihdatasciencesupportservicesteam@mail.nih.gov.

NIH CADRs pursuing alternative compliance options, such as migrating controlled-access data to another NIH CADR or disabling access to controlled-access data, are not required to submit this attestation.

I have reviewed the security and operational standards required by NOT-OD-25-159 as of **[Effective Date]** and assert that:

1. The risk to the **[Name of NIH CADR(s)]** operations, assets, and datasets it protects are ACCEPTABLE;
2. All required security and operational standards required by **[corresponding effective date]** have been met; and
3. All corresponding technical risks and weaknesses have been mitigated and resolved thus ensuring, to the best of our abilities, unauthorized access within the **[Name of NIH CADR(s)]** system will not occur.

X_____

ICO Senior Official

The attestation statement above should be signed by an ICO Senior Official responsible for the operations of the NIH Controlled-Access Data Repository. Examples of senior officials include the IC Authorizing Official, ICO Chief Information Officer, or the Data Science Program Senior Official. Please feel free to complete through Adobe Acrobat before signing if that is easier.

F. Security and Operational Standards

1. NIH Controlled-Data Access Data Repository Registration and Immediate Steps

Effective Date: Immediately upon issuance of NOT-OD-25-159

1.1 Nomination of ICO Senior Official

Standard: Each NIH Institute, Center, or Office (ICO) that has the primary responsibility for operating or supporting an NIH CADR must identify an NIH ICO Senior Official who will be responsible for overseeing the operations of NIH CADR(s) and ensuring they meet all the requirements stated in "Required Security and Operational Standards for NIH Controlled-Access Data Repositories" (NOT-OD-25-159) and explained in the NIH CADR Guidebook. The ICO Senior Official must be an NIH federal employee and should have knowledge of NIH CADR operations. A single ICO Senior Official may be appointed for multiple NIH CADRs. For a definition of ICO Senior Official, please refer to the glossary.

Applicability	NIH Institutes, Centers, or Offices.
Steps to Comply	1. Identify eligible ICO Senior Official. 2. Include name, title, and contact information of ICO Senior Official as part of information submitted to OCIO as part of step 1.2.
Acceptable Evidence	See 1.2.
Additional Guidance	N/A

1.2 Registration with NIH CADR Catalogue

Standard: NIH ICO Senior Official(s) responsible for overseeing each NIH CADR must contact OD for registration of NIH CADRs and inclusion on the NIH CADR list.

Applicability	Both repositories and access management systems
Steps to Comply	1. The NIH ICO Senior Official should email NIH CADR details to the ICO ISSO,OSP at sciencepolicy@nih.gov, and OCIO at securenihdatasciencesupportservicesteam@mail.nih.gov. NIH CADR details to include: • Name of NIH CADR • Access Management System used by NIH CADR if separate from repository • ICO supporting or operating the NIH CADR

	• Name, title, and contact information of ICO Senior Official responsible for the NIH CADR • Any other relevant points of contact (e.g., CIO)
Acceptable Evidence	Email Correspondence
Additional Guidance	Appendix A

1.3 Prohibit Specified User Access

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must implement NOT-OD-25-083 for enhancing security measures and prohibiting access to specified users.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Contact ICO ISSO and visit National Institute of Health Controlled Access Data Repository (NIH CADR) - NIH Usage and Security Overview - NIH InfoSec Wiki for additional instruction. Note only NIH staff can access wiki. 2. Adopt all prohibitions and follow ICO ISSO instructions.
Acceptable Evidence	The ICO ISSO will communicate what is required as evidence
Additional Guidance	Implementation Update: Enhancing Security Measures for NIH Controlled-Access Data (NOT-OD-25-083)

2. Documentation of Adherence to Relevant Laws and Policies

Effective Date: November 1, 2025

2.1 Determination of coverage by NIH Certificates of Confidentiality

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must maintain documentation demonstrating determination of coverage of the NIH CADR by a Certificate of Confidentiality.

Applicability	Repository
Steps to Comply	1. Review repository activities to determine whether the NIH CADR is covered by a Certificate of Confidentiality. See Determining if NIH-Funded Research is Covered by a CoC. • Direct Certificate of Confidentiality questions to NIH-CoC-Coordinator@mail.nih.gov.

	2. Ensure that agreements are updated per standard 3.1 based on the determination. 3. Email documentation and description of the determination (covered/not covered) to ICO ISSO.
Acceptable Evidence	• Documentation can be satisfied by demonstrating either the inclusion or absence of the Certificate of Confidentiality provision in agreements (see Appendix C for agreement standard terms) or email confirmation of determination coverage
Additional Guidance	• NIH Certificate of Confidentiality Policy • Determining if NIH-Funded Research is Covered by a CoC

2.2 Compliance with NIH Certificate of Confidentiality Policy

Standard: If the NIH CADR is determined to be covered by a Certificate of Confidentiality per the standard in 2.1, intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations are to maintain a Standard Operating Procedure (SOP) to consult with relevant legal counsel when compelled to disclose information covered by a Certificate.

Applicability	Repository **Note:** This standard is only applicable to repositories determined to be covered by a Certificate of Confidentiality in 2.1.
Steps to Comply	1. If the NIH CADR is covered by a Certificate of Confidentiality, create a SOP to consult with legal counsel when compelled to disclose information covered by a Certificate of Confidentiality. The SOP should include the following: • For NIH Intramural CADRs, consult the NIH Branch of the HHS Office of the General Counsel (OGC). • For Extramural CADRs, consult institutional legal counsel. 2. Familiarize relevant NIH CADR staff to comply with SOP. 3. Email ICO ISSO with evidence.
Acceptable Evidence	• For NIH Intramural CADRs, the SOP Document • For NIH CADRs managed by NIH-funded entities and contractors, acknowledgement from an institutional official of the standard.
Additional Guidance	• NIH Certificate of Confidentiality Policy

	• Frequently Asked Questions (FAQs) | Certificates of Confidentiality

2.3 Compliance with Section 2013 of the 21st Century Cures Act, 42 U.S.C. 241(f)

Standard: NIH intramural repository staff responsible for NIH CADR operations must maintain a SOP to respond to Freedom of Information Act (FOIA) requests.

Applicability	Repository. **Note**: This standard is only applicable to federal information systems.
Steps to Comply	1. Develop a SOP to ensure NIH intramural repository staff refer FOIA requests for controlled-access data to the NIH FOIA office or appropriate FOIA coordinator. 2. Familiarize relevant NIH CADR staff to comply with SOP. 3. Email ICO ISSO with evidence.
Acceptable Evidence	SOP document
Additional Guidance	N/A

2.4 Documentation of compliance with the Privacy Act of 1974 and/or E-Government Act of 2002

Standard: Intramural repository staff, along with NIH contractors from applicable* repositories, who are responsible for NIH CADR operations must maintain privacy compliance documentation in accordance with the Privacy Act of 1974 and/or E-Government Act of 2002 when applicable.

Applicability	Repository. ***Note**: This standard is only applicable to federal information systems and contractor owned/operated systems maintaining federal information.
Steps to Comply	1. Contact the NIH Privacy Program at the Office of Management Assessment at privacy@mail.nih.gov to assess applicability of the Privacy Act and E-Government Act to the NIH CADR. 2. If it is determined that the NIH CADR is subject to the Privacy Act and/or E-Government Act, ensure that the NIH CADR has a: • Systems of Record Notice (SORN) • Privacy Act Statement (PAS), and/or • Privacy Threshold Analysis/Privacy Impact Assessment 3. Email ICO ISSO with evidence.

Acceptable Evidence	Up to date: • System of Records Notice (SORN) • Privacy Act Statement (PAS) and/or • Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA)
Additional Guidance	Privacy Act; E-Government Act

2.5 Documentation of determination of whether the repository constitutes human subjects research requiring Institutional Review Board (IRB) review

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must seek and maintain documentation of determination of whether the repository constitutes human subjects research requiring an IRB review.

Applicability	Repository
Steps to Comply	1. Contact the applicable research protection program office: • For intramural NIH CADRs, contact Office for Human Subjects Research Protections (OHSRP) to receive determination. Information on how to submit for a determination that an activity is not human subjects research can be found here. • For all other NIH CADRs, contact your Human Research Protection Program (HRPP) 2. Email ICO ISSO with evidence. 3. Based on determination, take appropriate implementation action(s).
Acceptable Evidence	Correspondence with relevant parties containing documentation (e.g., HRPP correspondence, IRB letter of approval, if applicable)
Additional Guidance	45 CFR 46 | HHS.gov

3. Standard Data Access Processes

Effective Date: November 1, 2025

1. Standardized Terms of Access for NIH CADR Access Agreements

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operation's agreements (e.g., Data Transfer Agreements (DTAs), Data Use Agreements

(DUAs), Data Use Certifications (DUCs), etc.) should include standard terms of access (see Appendix C). For model agreements whose terms may be subject to negotiation or for those NIH CADRs with existing agreements with specific NIH CADR terminology, any changes must be consistent with standard terms of access in Appendix C. The institution or corporation, through the Institutional Signing Official, and the Data Access Requester, are each signatories to the agreement and agree to adhere to terms of access. NIH CADRs may incorporate additional terms as required by other NIH policies or ICO priorities. See below for information on how this standard intersects with the NIH Genomic Data Sharing (GDS) Policy.

- Compliance with GDS Policy:
    - If sharing data from studies subject to the GDS Policy, intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations should use the NIH Data Use Certification Agreement or ensure that their agreement is consistent with this NIH DUC when sharing said data.
- If sharing data from studies **not** subject to the GDS Policy, intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations should incorporate into their agreements the standard minimum terms of access outlined in Appendix C. Terminology underlined in Appendix C may be updated, and different defined terms can be used, as long as the terms in the final agreement are defined in a way that aligns with standard terms of access definitions in Appendix C.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Determine if repository shares data from studies subject to the GDS Policy. See here for guidance in making that determination. • If so, NIH CADRs should use the NIH Data Use Certification Agreement or ensure that agreements are consistent with the NIH Data Use Certification Agreement. To ensure consistency, please contact OSP at sciencepolicy@nih.gov. When step 1 is completed, proceed to step 3. • If not, proceed to step 2. 2. If sharing data from studies **not** subject to the GDS Policy, incorporate into agreements (e.g., DTAs, DUAs) standard terms of access outlined in Appendix C. 3. If the agreement is an OMB-approved form or requires OMB clearance, email the Project Clearing Branch (ProjectClearanceBranch@mail.nih.gov) or, if applicable, the ICO project clearance when updating or developing a new agreement.

	4. Email ICO ISSO with evidence. 5. Implement updated agreement on February 25, 2026, to comply with the standard that institutions or corporations and Data Access Requesters will secure data according to the NIH Security Best Practices for Users of Controlled-Access Data.
Acceptable Evidence	Copy of agreement with relevant sections highlighted.
Additional Guidance	Does the Genomic Data Sharing Policy Apply to My Research? | Data Sharing

3.2. Access Request Standards

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must use standardized processes for authorizing data access. For specific expectations see subsections 3.2.1-3.2.3.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Review Standards for Data Access, subsections 3.2.1-3.2.3. 2. If additional guidance is required, contact ICO ISSO. OCIO is available for additional guidance at securenihdatasciencesupportservicesteam@mail.nih.gov. 3. If you have already established a data request process, cross-check standards with current process to identify missing standards. 4. Incorporate missing standards in process. 5. If any component of the request process has an OMB-approved form (e.g., portal, form) or if there are questions about the applicability, email the Project Clearing Branch (ProjectClearanceBranch@mail.nih.gov) or, if applicable, the ICO project clearance branch when updating or developing access request processes. 6. Email ICO ISSO with evidence.
Acceptable Evidence	Screenshots of adopted processes
Additional Guidance	N/A

3.2.1. Credentials and Email Standards

a. Required Credentials to Submit a Request for Access
Requests must be submitted by a Data Access Requester (e.g., Recipient) who meets all the following criteria:

1. Is a permanent employee of their institution at a level equivalent to, but not limited to, that of an academic professor (e.g., assistant, associate, or non-tenure or tenure-track professor) or senior researcher. This does **not** include lab technicians or trainees, e.g., post-docs or graduate students.
2. Uses an email address affiliated with their self-identified institution or corporation.
    i. Any request submitted by Data Access Requesters with email addresses unaffiliated with their institution or corporation (e.g., Gmail) must be rejected.
    ii. Requests from any individual with one of the following email addresses: "dnu@nih.gov" and dnu@od.nih.gov must be automatically rejected.
    iii. For further guidance on how to identify email addresses unaffiliated with institutions or corporations, please visit National Institute of Health Controlled Access Data Repository (NIH CADR) - NIH Usage and Security Overview - NIH InfoSec Wiki. Note only NIH staff can access wiki.
3. Has direct oversight of laboratory staff and trainees.
4. Is accountable for ensuring that the terms of access (through agreements such as DUA, DUC agreement, DTA, etc.) and the Data Access Requester's institutional policy(ies) are followed.
5. Only occupies one role at a time. Requests in which the Data Access Requester, or any other Key Personnel, occupy more than one role (e.g., Institutional Signing Official or IT Director) are not allowed.

b. Required Credentials for Institutional Signing Official (SO)
Requests must be certified by the institution as represented by an Institutional Signing Official (SO) who meets all the following criteria:

1. Is affiliated with the Data Access Requester's institution or corporation.
2. Has institutional authority to legally bind the institution or corporation in administrative matters.
3. Uses an email affiliated with the Data Access Requester's institution or corporation.
    i. Email addresses unaffiliated with institutions or corporations (e.g., Gmail) must be rejected.
    ii. Requests from any individual with one of the following email addresses: "dnu@nih.gov" and dnu@od.nih.gov must be automatically rejected.
    iii. For further guidance on how to identify email addresses unaffiliated with institutions or corporations, please visit National Institute of Health Controlled Access Data Repository (NIH CADR) - NIH Usage and

Security Overview - NIH InfoSec Wiki. Note only NIH staff can access wiki.

3.2.2. Institutional Signing Official and Data Access Request Standards

a. Institutional Signing Official (SO) Attestation of Data Access Requester Affiliation
Requests must include an attestation by the SO that all listed Data Access Requesters fulfill the criteria below:

1. Are affiliated with their listed institution or corporation.
2. Meet the minimum criteria to qualify as a Data Access Requester (see 3.2.1 a. 1-5)

The SO's attestation that all listed Data Access Requesters meet the specified criteria can be incorporated into agreements, included in the request process, or verified by the SO via email.

b. Tracking datasets accessed by Data Access Requester

1. Requests should specify the datasets that the Data Access Requester is authorized to access. Repositories can adopt variable methods to specify what datasets the Data Access Requester is authorized to access. Regardless of method used, the NIH CADR should be able to identify what datasets have been approved/accessed by the Data Access Requester. For tracking ease, it is strongly recommended that NIH CADRs, and their access management systems include this information within its metadata for monitoring and reporting purposes.

c. Collaboration Standards

Requests must incorporate the following expectations for collaborators:

1. Internal collaborators, i.e., Data Access Requesters within the Data Access Requester's same institution or corporation, must be listed on the request. No separate request will be expected from the internal collaborators.
2. External collaborators, i.e., Data Access Requesters outside of the Data Access Requester's institution or corporation, must submit a separate request with the exact title and research use wording as the Data Access Requester. This standard may also be satisfied by having the SO, Data Access Requester, external SO, and external Data Access Requester sign the same access request.

d. Research Use Statements
All Data Access Requests must include a Research Use Statement detailing at least the following:

1. Research objectives.
2. Study design.
3. Analysis plan.
4. Research use alignment with any data use limitations.

3.2.3. Renewal and Closeout Standards

a. All requests must be approved for a duration not to exceed 12 months.

b. All requests must be re-approved through an annual renewal process that re-authenticates the Data Access Requester and the Institutional Signing Official (SO) through a process that meets the standards, requirements, and identity proofing outlined in 3.2.1, 3.2.2., and 5.4.

c. Reporting standards are expected for request renewals and request close-outs (i.e., the dataset will no longer be used).

d. Renewals must include at least the following:

1. Options to update collaborators, key personnel, and datasets.
2. A report of any publications or presentations using the data.
3. A report of any research progress within the last year even if progress is unchanged.
4. Report of any violations of the terms of access (e.g., data misuse, breaches, security incidents) and the implemented remediation.
5. Report of information on any downstream intellectual property generated from the data.

e. Close-outs must include at least the following:

1. Report of publications or presentations using the data.
2. Report of research progress within the last year even if progress is unchanged.
3. Report of any violations of the terms of access (e.g., data misuse, breaches, security incidents) and the implemented remediation.
4. Report of information on any downstream intellectual property generated from the data.
5. The institution or corporation, through SO, and the Data Access Requester, are each signatories to the agreement and ensure that all copies and versions of the dataset(s) have been destroyed from local hardware and third-party Information Technology (IT) systems according to the NIH Security Best Practices for Users of Controlled-Access Data.

3.3. Standardized Body to Review Research Use: NIH Data Access Committees (DACs)

Standard: Intramural repository staff or NIH-funded entities and contractors' staff responsible for NIH CADR operations must use NIH DACs that adhere to standardized DAC materials to review and approve or disapprove requests for controlled-access data.

For NIH CADRs that do not have an NIH DAC that adheres to these standards, NIH will work with the NIH CADR to establish an NIH DAC(s) or, where feasible, incorporate an existing NIH DAC into their review process.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. If not using an NIH DAC: • Partner with an existing NIH DAC, or • Establish an NIH DAC (this may be done by reconfiguring existing bodies reviewing requests). 2. Ensure any new or existing NIH DAC(s) used by the NIH CADRs is adhering to standardized NIH DAC materials. Contact OSP at sciencepolicy@nih.gov for standardized NIH DAC materials. 3. Email ICO ISSO with evidence.
Acceptable Evidence	See 3.4
Additional Guidance	N/A

3.4. Registration of NIH Data Access Committees

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for overseeing an NIH CADR must register their DAC(s) internally at NIH. Registration must include charter, roster, and point of contact.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Contact OSP at sciencepolicy@nih.gov for guidance on NIH DAC registration. 2. Collect standardized NIH DAC materials from OSP. 3. Email ICO ISSO with evidence.
Acceptable Evidence	Screenshot of NIH DAC registration or email confirming registration
Additional Guidance	N/A

4. Standard Data Submission Processes

Effective Date: February 25, 2026

4.1 Standardized Provisions for NIH CADR Submission Forms or Certifications

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations should ensure that all data submission forms or certifications include standard submission provisions. Refer to Appendix D for these provisions. Additionally, the institution or corporation and the Submitting Investigator should assure to NIH that the data are appropriate to share as signatories to the data submission form or certification. NIH CADRs may incorporate additional terms as required by other NIH policies or ICO priorities.

a. Compliance with GDS Policy:
    1. For NIH CADRs receiving data from studies subject to the GDS Policy, intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations should use the Institutional Certification or ensure that their submission form or certification is consistent with that form.

b. If receiving data from studies **not** subject to the GDS Policy, intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations should incorporate into their submission form or certification the standard submission provisions outlined in Appendix D. Terminology may be updated to fit NIH CADR definitions so long as the edits remain consistent with the standard submission provisions.

Applicability	Repository
Steps to Comply	1. Develop or update submission form or certification to incorporate standard submission provisions outlined in Appendix D. 2. If any component of the request process is OMB-approved, email the Project Clearing Branch (ProjectClearanceBranch@mail.nih.gov) or, if applicable, the ICO project clearance branch to understand responsibilities under the Paperwork Reduction Act (PRA) when updating or developing a new submission form. 3. For NIH CADRs sharing data from studies subject to the GDS Policy, use the Institutional Certification for data submissions, or ensure the submission form or certification is consistent with the Institutional Certification. To ensure consistency, contact OSP at sciencepolicy@nih.gov

	4. Email ICO ISSO with evidence.
Acceptable Evidence	Copy of data submission form or certification with relevant sections highlighted
Additional Guidance	For provision refer to Appendix D

5. Security Standards and Practices

Effective Date: February 25, 2026

5.1 Adherence to NIH Security Best Practices

Standard for NIH CADRs:

a. Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must adhere to the cybersecurity standards established in the NIH Security Best Practices for Controlled-Access Data Repositories.

Standard for Data Access Requesters

b. Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must require that Data Access Requesters and their institution or corporation secure data according to the NIH Security Best Practices for Users of Controlled-Access Data.

Applicability:	Both repositories and access management systems
Steps to Comply	**Adherence to NIH Security Best Practices for Controlled-Access Data Repositories:** 1. Contact ICO ISSO as soon as possible to begin NIH CADR security control assessment aligned to the NIH Security Best Practices for Controlled-Access Data Repositories. OCIO is available to assist as needed with supplemental guidance at securenihdatasciencesupportservicesteam@mail.nih.gov. **Adherence to NIH Security Best Practices for Users of Controlled-Access Data:** 1. Communicate to Data Access Requesters and their institution or corporation that effective February 25, 2026, Data Access Requesters and their institution or corporation will have to attest to securing controlled-

	access data accessed from an NIH CADR according to the security standards described in the NIH Security Best Practices for Users of Controlled-Access Data. 2. Include an attestation in updated agreements or the access process that the Data Access Requester and their institution or corporation attest, as signatories, that the data are secured according to the NIH Security Best Practices for Users of Controlled-Access Data. 3. Implement updated agreement on February 25, 2026, to comply with the standard that Data Access Requesters and their institution or corporation will secure data according to the NIH Security Best Practices for Users of Controlled-Access Data. 4. Email ICO ISSO with evidence.
Acceptable Evidence	**Standards for NIH CADRs** OCIO and the ICO ISSO will provide what evidence is required to demonstrate adherence to the "NIH Security Best Practices for Controlled-Access Data Repositories". **NIH CADR Standards for Data Access Requesters and Institutions** Evidence for NIH CADRs implementing the "NIH Security Best Practices for Users of Controlled-Access Data" can be a copy of the template agreement with relevant sections highlighted.
Additional Guidance	• NIH Security Best Practices for Controlled-Access Data • NIH Security Best Practices for Users of Controlled-Access Data • GDS Frequently Asked Questions| NIH Security Best Practices

5.2 Review of Compliance with NIH Security Best Practices for NIH CADRs

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must:

a. Obtain independent review of compliance with the NIH Security Best Practices for Controlled-Access Data Repositories and future iterations.

b. Maintain documentation of compliance with NIH Security Best Practices for Controlled-Access Data Repositories.

c. Provide the federal government with an Assurance Package (non-federal) or Authorization to Operate (Federal) with evidence to third-party implementation and continuous monitoring aligned to NIH Security Standards.

Applicability	Both repositories and access management systems
Steps to Comply	Contact ICO ISSO. OCIO is available to provide supplemental guidance at securenihdatasciencesupportservicesteam@mail.nih.gov for guidance.
Acceptable Evidence	ICO ISSO & OCIO will communicate what evidence is required
Additional Guidance	N/A

5.3 Minimum Standard Operating Procedures for Developer Oversight

Standard: The ICO Senior Official responsible for NIH CADR operations must ensure that developers working on the NIH CADR adhere to the Minimum Standard Operating Procedures for Developer Oversight described in this Notice, NOT-OD-24-157. This standard applies to all NIH CADRs.

Applicability	Both repositories and access management systems
Steps to Comply	1. Review NOT-OD-24-157 to understand all expectations under the Minimum Standard Operating Procedures for Developer Oversight. 2. The ICO Senior Official should ensure that the developer terms of access (NOT-OD-25-021) are incorporated into the Notice of Award, contract, or other funding agreements (e.g., Other Transactions) for newly funded activities involving developer work. • For existing awards, the ICO Senior Official should ensure that the developer terms of access are incorporated into the Notice of Award, contract, or other funding agreement at the next budget period. 3. The ICO Senior Official should coordinate with the intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations to review all developer repository work involving the NIH CADR and ensure that all Lead Developers have submitted a Developer Use Statement (DUS) to the NIH Developer DAC (DeveloperAccessDAC@od.nih.gov). 4. Once approved, every two years, the NIH CADR must submit a renewal or close-out request to the Developer DAC (DeveloperAccessDAC@od.nih.gov).

	5. Email ICO ISSO with evidence.
Acceptable Evidence	Evidence can include: • A copy of the executed agreement (e.g., terms of access incorporated in the Notice of Funding Opportunity or Notice of Award, contract, or other funding agreement); or • A copy of the approved DU; or • Email correspondence from the NIH Developer DAC decision indicating approval.
Additional Guidance	• Minimum Standard Operating Procedures for Developer Oversight in NOT-OD-24-157 • Standard Language for Developer Terms of Access in the Terms and Conditions of Award NOT-OD-25-021

5.4 Secure Access with RAS and Identity Proofing

Standard:

Target Measure to be eventually adopted

a. Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must integrate with NIH Researcher Auth Service (RAS) to enforce user:
   - Authentication (AuthN) at NIST Authenticator Assurance Level 2 (AAL2) and
   - Identity-proofing to Identity Assurance Level 2 (IAL2).
   - Authorization (AuthZ) is granted via the consumption of GA4GH Passport and Visas.

b. If RAS integration is not yet implemented, please use the Interim Measure below.

Interim Measure to be adopted as NIH CADR works toward IAL2 integration

a. Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations may implement identity proofing at Identity Assurance Level 1 (IAL1) with acceptable compensating controls to ensure proper authentication of the Data Access Requester and the SO's identity.

Compensating controls must include **one** of the identity assurance validations below:

b. Authenticating identity and organizational affiliation by:

   1. Validating that the SO is using the email domain associated with the institution or corporation submitting the request.

   2. Validating that the Data Access Requester is using the email domain associated with the SO's institution or corporation (example@umd.edu, @researchinnovat.org, etc.)

c. Requiring a digitally signed pdf with valid certificates from the Institutional Signing Official's institutions or corporate certificate authority. Examples include:

   1. Validating digital signatures, Adobe Acrobat https://helpx.adobe.com/acrobat/using/validating-digital-signatures.html)

2. Electronic Signature for Online Documents | Google Workspace
3. Obtain a digital certificate and create a digital signature - Microsoft Support

d. Additional compensating controls can include a blend of automated and manual review processes designed to validate the authenticity of Data Access Requesters, institutions or corporation, and their SOs.

1. Applying system web search methods for organizational and identity validation such as searching for published manuscripts within PubMed can be employed.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Contact ICO ISSO. OCIO is available to provide supplemental guidance at securenihdatasciencesupportservicesteam@mail.nih.gov for a briefing on the security control implementation process for identify proofing. 2. Provide OCIO with standardized identity proofing artifacts for a risk assessment. 3. OCIO will provide a recommendation for Identity Proofing Integration Plans and assist the NIH CADR in submitting a formal RAS integration request with the RAS integration team to become IAL2 compliant. 4. If not in compliance with IAL2, adopt IAL1 with compensating controls as an interim approach while RAS integration moves forward.
Acceptable Evidence	ICO ISSO and OCIO will communicate what is required as evidence
Additional Guidance	NIST SP 800-63 Identity Proofing Requirements

5.5 NIH CADR Logging Standards

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must be able to provide accessible records of data downloads and Data Access Requester access when requested by NIH for investigating a data management incident (DMI). To that end, NIH CADRs should meet the following logging expectations:

a. Mandatory Logging:
   1. Authentication and authorization events (e.g. single sign on logins, automated lock outs and logouts, failed and timed attempts).
   2. Data Access Request (DAR) submissions, approvals, modifications, and rejections processed established.
   3. Data downloads, uploads, and deletion/archival/destruction processes established.

b. Log Data Fields: For each logged entry (where applicable), the following fields should be included:
    1. _time: Timestamp of the event
    2. src_ip: Source IP address of the connection
    3. dest_ip: Destination IP address of the connection
    4. dest_port: Destination port of the connection
    5. user_name: Identifies the users first name and last name associated with the event
    6. user_id: user identification name from NIH, Login.gov, or other linked credentials with unique identifiers.
    7. user_id_provider: NIH, Login.gov, RAS or other providers
    8. session_id: Unique session identifier
    9. url: The requested URL
    10. app: The application or service accessed
    11. http_user_agent: Browser or client application making the request
    12. status: Outcome of the action (e.g., HTTP status code)
    13. http_content_type: Content type of the HTTP response
    14. bytes: Number of bytes transferred
    15. duration: Duration of the connection
    16. nih_ico: for example, NCI
    17. cadr_name: for example, CDS (Cancer Data Service)
    18. user_country_name: from the user DAR
    19. user_org: Name of the user's institution affiliation
    20. user_email: User's Email address
    21. associated_study: for example, psh000xxx
    22. eRA_commons_id: if applicable
    23. user_permission_group: for example, dbGap
    24. event_type: Authentication, data request, download, etc.
c. Retention:
    1. M-21-31 require federal agencies to store logs in "active" storage for 12 months and then move them to "cold" storage for an additional 18 months, resulting in a total retention period of 30 months.

Applicability	Repositories
Steps to Comply	1. Determine if repository meets NIH CADR Logging Standard. 2. If not, develop a mechanism that meets logging standards. 3. Email ICO ISSO with evidence.
Acceptable Evidence	ICO ISSO and OCIO will communicate what is required as evidence
Additional Guidance	N/A

6. Transparency and Utility Standards

Effective Date: February 25, 2026

6.1 Metadata

Standard: To the extent possible, Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must collect and make publicly available metadata to enable discovery, reuse, and citation of datasets, using schema that are appropriate to, and ideally widely used across, the community(ies) the repository serves.

Applicability	Repositories
Steps to Comply	1. Identify metadata schema that are appropriate to, and ideally widely used across, the community(ies) the repository serves. 2. Ensure that relevant metadata is exposed to enable discovery, reuse, and citation of datasets. 3. Email ICO ISSO with evidence.
Acceptable Evidence	Screenshots of adopted metadata schema
Additional Guidance	N/A

6.2 Information on Use and Research products

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must provide publicly available information on research uses, individually and in aggregate, including data use statements/summaries with project dates, and user and institution names.

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Publicly provide the following information for approved requests: • Data use statements/summaries • Project dates • User and institution names 2. Tabulate aggregate number of approved requests. 3. Publicly provide aggregate number of approved requests. 4. If publications resulting from secondary research use are collected and compiled, publicly provide a list of these publications.

	5. For federal information systems, ensure compliance with the Privacy Act, E-Government Act of 2002 (see 2.4) for collecting and providing information on users and institutions. 6. If the agreement or other collection instrument is an OMB-approved form or requires OMB clearance, email the Project Clearing Branch (ProjectClearanceBranch@mail.nih.gov) or, if applicable, the ICO project clearance branch to understand responsibilities under the Paperwork Reduction Act (PRA). 7. Email ICO ISSO with evidence.
Acceptable Evidence	Screenshots of examples of publicly provided information on approved research uses and aggregate data on approved requests.
Additional Guidance	N/A

6.3 Tracking of Certificate of Confidentiality Status

Standard: Intramural repository staff or NIH-funded entities and contractors responsible for NIH CADR operations must collect and maintain documentation for each dataset or maintain documentation verifying their ability to track whether datasets submitted to the repository are covered by a Certificate of Confidentiality (e.g., through metadata, statements in agreements).

Applicability	Access management systems and repositories with integrated access management systems
Steps to Comply	1. Track whether submitted datasets are covered by a Certificate of Confidentiality through the data submission form (see Appendix D for provisions) 2. Develop approach to track covered datasets submitted to an NIH CADR. 3. Email ICO ISSO with evidence.
Acceptable Evidence	Documentation of ability to track covered status of datasets submitted to the repository (e.g., through fields in data submission forms and agreements and/or metadata)
Additional Guidance	NIH Certificate of Confidentiality Policy

Appendix A

SOP for Maintaining and Modifying the NIH CADR List

Version	Implementation Date	Summary of Changes	Sections Updated	Changes Approved By
1.0	9.22.2025	Initial release	All	OCIO, OSP

The following SOP will be used for maintaining and modifying the list of NIH CADRs.

1. NIH ICO or OD staff should notify OSP (sciencepolicy@nih.gov) to add or remove an NIH CADR from the NIH CADR list.
2. To determine whether the access management system or repository is an NIH CADR, OSP will do the following:
    a. Review available information to assess against the criteria for NIH CADRs (see criteria at the end of this SOP). OSP may request additional information from the NIH CADR ICO Senior Official, system administrators, and/or other NIH staff to aid in the determination.
    b. Document the evidence to support the determination for each criterion, e.g., identifying specific supporting text and providing a link to the website, collecting the document, or collecting the email correspondence in which the supporting information is provided.
    c. For new NIH CADRs to be added to the list, OSP will also determine whether the NIH CADR has data from studies subject to the GDS Policy and include this in the documentation.
3. To remove the NIH CADR from the list, OSP will review to determine that removal is consistent with the "Guidance on Options to Implement Security and Operational Standards for NIH Controlled-Access Data Repositories" (see options below).
4. If OSP determines that a change is required to the NIH CADR list, OSP will notify relevant NIH offices and the NIH CADR ICO Senior Official. OCIO will maintain the NIH CADR list and notify relevant NIH offices when the list is updated.

Appendix B

Guidance on Options to Implement Security and Operational Standards for NIH Controlled-Access Data Repositories

Version	Implementation Date	Summary of Changes	Sections Updated	Changes Approved By
1.0	9.22.2025	Initial release	All	OCIO, OSP

In coordination with relevant intramural approval or approval of the relevant contracting officer or program officer, as applicable, NIH CADRs have the following options for implementing the Security and Operational Standards:

1. NIH CADRs can implement all updates by the effective date(s) and continue functioning as normal. Direct adoption requires the following confirmations:
    a. A signed attestation by the ICO Senior Official affirming compliance with all requirements. This attestation (see page 9) must be sent to OCIO at securenihdatasciencesupportservicesteam@mail.nih.gov.
    b. All evidence, including information security artifacts, sent to the ICO Information System Security Officer (ICO ISSO). Intramural CADR staff can find their ICO ISSO here. External CADR staff who do not know their ICO ISSO can inquire by emailing OCIO with NIH CADR details at securenihdatasciencesupportservicesteam@mail.nih.gov.

2. NIH CADRs intending to implement the updates but unable to meet the required timelines must disable all access to controlled-access data and cease processing new data access requests until the updates can be implemented.

3. NIH CADRs can withdraw controlled-access data from public availability permanently or temporarily until compliance can be achieved, including download capabilities for previously approved projects.

    a. NIH CADRs implementing this option will still be considered an NIH CADR as they maintain data that warranted controls but will only need to comply with requirements for maintaining data, not for providing access to data (e.g., ensuring oversight of access by a DAC) until a decision is made to restore public access.

    b. NIH CADRs will provide plans for withdrawal of data availability to OCIO.

5. NIH CADRs can migrate controlled-access data to another NIH CADR that has implemented the updates.

a. Under extenuating circumstances, NIH CADRs may be permitted to migrate controlled-access data to a non-NIH CADR with equivalent controls. NIH will consider such exceptions on a case-by-case basis.

b. NIH CADRs that successfully migrate their data will no longer be considered NIH CADRs and will not have to comply with any requirements for NIH CADRs.

c. NIH CADRs will provide plans for migration of data to OCIO for approval prior to migrating data and being removed from the list of NIH CADRs.

d. Once migration is complete, OSP will make a determination for modification of the list of NIH CADRs using the SOP for Maintaining and Modifying the NIH CADR List (see above).

6. NIH CADRs can recommend specific controlled-access data to OCIO for de-controlling (i.e., NIH CADRs can cease requiring prospective review of data access requests).

    a. NIH CADRs will need to provide all of the following to OCIO prior to de-controlling any data:

        i. The specific datasets recommended for de-controlling;

        ii. The measures, if any, that will still be employed to protect the data;

        iii. The justification for why the specific datasets were controlled previously but should not be controlled now;

        iv. Documentation regarding whether explicit informed consent for sharing without controls has been obtained from participants represented in the dataset;

        v. Documentation regarding whether institutional review was conducted to determine that providing the data without controls poses very low risk when shared and used, including risks posed by the presence of information that can allow inferences to be made about a participant's identity when combined with other information; and

        vi. A determination that de-controlling the data would not violate the terms of participants' informed consent, data transfer agreements, data use limitations, data use agreements, data submission agreements, institutional certifications, Certificates of Confidentiality, the Privacy Act, funding agreements or contracts, and any other applicable laws, regulations, or NIH policies.

    b. The following data types will not be considered for de-controlling at this time:

        i. Human genomic data, human transcriptomic data, human epigenomic data, human proteomic data, and any other data expected to be controlled by law or regulation.

    c. Once documentation is received, OSP will review and make a recommendation to OCIO on whether to approve, deny, or request additional information. The OCIO will notify NIH CADRs of the determination.

    d. If all controlled-access data in the NIH CADR are de-controlled, the CADR will no longer be considered an NIH CADR and will not have to comply with any requirements for NIH CADRs.

e. Once all data in the NIH CADR are successfully de-controlled, OSP will make a determination for modification of the list of NIH CADRs using the SOP for Maintaining and Modifying the NIH CADR List (Appendix A).

Altering CADR operations to fall out of scope of the criteria (e.g., removing federal employees from the prospective review process) is **not** considered an acceptable implementation strategy.

Appendix C

Standard Provisions for Data Use/Data Transfer Agreements

Version	Implementation Date	Summary of Changes	Sections Updated	Changes Approved By
1.0	9.22.2025	Initial release	All	OCIO, OSP

Note: For model data use/data transfer agreements whose terms may be subject to negotiation or for those NIH CADRs with existing data use/data transfer agreements with specific NIH CADR terminology, any changes must be consistent with standard terms of access in Appendix C. This includes changes to the underlined terms that are described in Terms and Definitions. The institution or corporation, through the Institutional Signing Official (SO), and the Data Access Requester, are each signatories to the data use/data transfer agreement and agree to adhere to terms of access.

NIH CADRs will need to determine if the repository is covered by a Certificate of Confidentiality per 2.1 above prior to including the Certificate of Confidentiality term. **The language of the Certificate of Confidentiality term cannot be edited, except for the underlined definition used for Data Access Requester(s) and Institutional Requester.**

DUCs, DTAs, and/or DUAs should have these standard terms of access:

Non-identification

Data Access Requesters agree not to use controlled-access data sets obtained through the Data Access Request, either alone or in concert with any other information, to identify or contact individual participants from whom data and/or samples were collected. These provisions do not apply to original Submitting Investigators operating with specific Institutional Review Board (IRB) or equivalent body approval, pursuant to 45 CFR 46, to contact individuals within datasets or to obtain and use identifying information under an IRB-approved research protocol. All Data Access Requester(s), conducting "human subjects research" within the scope of 45 CFR 46 must comply with the requirements contained therein.

Certificate of Confidentiality

Certificates of Confidentiality (Certificate) protect the privacy of research participants by prohibiting disclosure of protected information for non-research purposes to anyone not connected with the research except in specific situations. The data that are stored in and shared through the data repositories accessed under this agreement are protected by a Certificate. Therefore, the Institutional Requester and the Data Access Requester(s), whether or not funded by the NIH, who are approved to access a copy of information protected by a Certificate, are also subject to the requirements of the Certificate of Confidentiality and subsection 301(d) of the Public Health Service Act.

Under Section 301(d) of the Public Health Service Act and the *NIH Policy for Issuing Certificates of Confidentiality*, recipients of a Certificate of Confidentiality shall not:

> Disclose or provide, in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding, the name of such individual or any such information, document, or biospecimen that contains identifiable, sensitive information about the individual and that was created or compiled for purposes of the research, unless such disclosure or use is made with the consent of the individual whom the information, document, or biospecimen pertains; or
>
> Disclose or provide to any other person not connected with the research the name of such an individual or any information, document, or biospecimen that contains identifiable, sensitive information about such an individual and that was created or compiled for purposes of the research.
>
> Disclosure is permitted only when:
>
> 1. Required by Federal, State, or local laws (e.g., as required by the Federal Food, Drug, and Cosmetic Act, or state laws requiring the reporting of communicable diseases to State and local health departments), excluding instances of disclosure in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding.
> 2. Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual.
> 3. Made with the consent of the individual to whom the information, document, or biospecimen pertains; or
> 4. Made for the purposes of other scientific research that is following applicable Federal regulations governing the protection of human subjects in research.

For more information see: *Certificates of Confidentiality (CoC) | Grants & Funding*.

Non-Transferability

The Institutional Requester and Data Access Requester agree to retain control of NIH controlled-access datasets accessed through the request and further agree not to distribute controlled-access data to any entity or individual not identified in the submitted request. If the Data Access Requesters are provided access to controlled-access datasets for inter-institutional collaborative research described in the Research Use Statement of the Data Access Request, and all members of the collaboration are also Data Access Requesters through their home institution(s), data obtained through the Data Access Request may be securely transmitted within the collaborative group. Each Data Access Requester and their Institutional Requester will secure the data according to the NIH Security Best Practices for Users of Controlled-Access Data, the terms of this Agreement, and the Institutional Requester's IT security requirements and policies.

The Institutional Requester and Data Access Requester acknowledge responsibility for ensuring the review and agreement to the terms within this Agreement that apply to them and the appropriate research use of controlled-access data obtained through the Data Access Request, subject to applicable laws and regulations. Institutional Requester and Data Access Requester agree that

controlled-access data obtained through the Data Access Request, in whole or in part, may not be sold to any individual at any point in time for any purpose.

Institutional Requester must have policies and procedures to ensure that the Data Access Requester completes the Project Close-out process (See Termination and Data Destruction Provision) before moving to a new institution. If a Data Access Requester moves to a new institution without completing the Project Close-out process, the Institutional Requester must immediately notify the relevant NIH DAC(s) so that the project may be closed out and the data are destroyed according to NIH Security Best Practices for Users of Controlled-Access Data. A new Data Access Request, in which the new Institutional Requester agrees to the Data Use Agreement, must be approved by the relevant NIH DAC(s) before controlled-access data may be re-accessed by the Data Access Requester.

Data Security and Unauthorized Data Release

The Institutional Requester and Data Access Requester acknowledge NIH's expectation that they have reviewed and agree to manage the requested controlled-access data according to NIH's expectations set forth in the current NIH Security Best Practices for Users of Controlled-Access Data and the Institutional Requester's IT security requirements and policies.

The Institutional Requester or Data Access Requester agree to notify the NIH Incident Response Team, NIH DAC(s) on the project request, and the NIH Data Management Incident Notification inbox of any unauthorized data sharing, breaches of data security, or inadvertent data release that may compromise data confidentiality within 24 hours of when the incident is identified. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357or TTY: (301) 496-8294 and can also be sent by email to NIHInfoSec@nih.gov or via the Report an Incident Link: https://irtportal.ocio.nih.gov/. For the NIH Data Management Incident Notification inbox, email DMI_OER@mail.nih.gov.

As permitted by law, notifications should include any known information regarding the incident and a general description of the activities or process in place to define and remediate the situation fully. Within 3 business days of the notification, the Institutional Requester or the Data Access Requester agree to submit to the NIH DAC(s) on the project request and the NIH Data Management Incident Notification inbox a detailed written report including the date and nature of the event, actions taken or to be taken to remediate the issue(s), and plans or processes developed to prevent future incidents, including specific information on timelines anticipated for action. The Institutional Requester and the Data Access Requester agree to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Institutional Requester and/or the Data Access Requester(s).

NIH, or another entity designated by NIH may, as permitted by law, also investigate any data security incident or policy violation. The Institutional Requester and Data Access Requesters and their associates agree to support such investigations and provide information, within the limits of applicable local, state, Tribal, and federal laws and regulations. In addition, the Institutional Requester and Data Access Requester agree to work with NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

Terms of Access Violations

The Institutional Requester and Data Access Requester acknowledge that NIH may terminate the Data Access Request, including this Agreement and immediately revoke or suspend the Institution's or the Data Access Requester's access to all controlled-access datasets at any time if the Institutional Requester and/or Data Access Requester is found to be no longer in compliance with the terms described in this Agreement, or the policies, principles, and procedures of NIH. NIH may apply for injunctive or other equitable relief before courts of competent jurisdiction as remedy for breach of the Agreement, in addition to all other remedies available at law or in equity.

The Institutional Requester or Data Access Requester(s) agree to notify the NIH DAC(s) indicated in the project request to this Agreement, and the NIH Data Management Incident Notification inbox of any terms of access violations, hereinafter referred to as data management incidents (DMIs), within 24 hours of when the incident is identified. For the NIH Data Management Incident Notification inbox, notifications can be sent to DMI_OER@mail.nih.gov. As permitted by law, notifications should include any known information regarding the incident and a general description of the activities or process in place to define and remediate the situation fully.

Within 3 business days of the notification(s), the Institutional Requester or the Data Access Requester agrees to submit to the NIH DAC(s) indicated on the project request and the NIH Data Management Incident Notification inbox a detailed written report including the date and nature of the event, actions taken or to be taken to remediate the issue(s), and plans or processes developed to prevent future incidents, including specific information on timelines anticipated for action. The Institutional Requester and the Data Access Requester agree to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Institutional Requester and/or the Data Access Requester.

As outlined in Term "Data Security and Unauthorized Data Release", all notifications of unauthorized data sharing, breaches of data security, or inadvertent data releases should also be sent to the NIH Incident Response Team. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357or TTY: (301) 496-8294 and can also be sent by email to NIHInfoSec@nih.gov or via the Report an Incident Link: https://irtportal.ocio.nih.gov/.

NIH, or another entity designated by NIH, may, as permitted by law, also investigate any DMI. The Institutional Requester and the Data Access Requester and their associates agree to support such investigations and provide information, within the limits of applicable local, state, Tribal, and federal laws and regulations. In addition, Institutional Requester and Data Access Requester agree to work with NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

Termination and Data Destruction

Upon Project Close-out, the Institutional Requester and Data Access Requester agree to destroy all copies and versions of the dataset(s) retrieved from NIH controlled-access data repositories

regardless of the storage medium or format in accord with the NIH Security Best Practices for Users of Controlled-Access Data. However, the Data Access Requester may retain these data as necessary to comply with law, regulation, and government policy. A Data Access Requester who retains data for any of these purposes, and their Institutional Requester, continue to be a steward of the data and is responsible for the management of the retained data in accordance with the NIH Security Best Practices for Users of Controlled-Access Data, and any institutional policies.

After termination of the approved research project, the data may not be used to answer any additional research questions, even if they are within the scope of the approved Data Access Request, unless the Data Access Requester submits a new Data Access Request and is approved by NIH to conduct the additional research. If a Data Access Requester retains data for any of these purposes, the Institutional Requester and the Data Access Requester are bound by the terms for Non-Identification, Certificate of Confidentiality, Non-transferability, Data Security and Unauthorized Data Release, Terms of Access Violations, and Termination and Data Destruction until the data is destroyed.

Non-Endorsement, Indemnification

The Institutional Requester and the Data Access Requester acknowledge that although all reasonable efforts have been taken to ensure the accuracy and reliability of controlled-access data accessed through the request, the NIH and Submitting Investigator(s) do not and cannot warrant the results that may be obtained by using any data included therein. NIH and all contributors to these datasets disclaim all warranties as to performance or fitness of the data for any particular purpose.

No indemnification for any loss, claim, damage, or liability is intended or provided by any party under this agreement. Each party shall be liable for any loss, claim, damage, or liability that said party incurs because of its activities under this agreement, except that NIH, as an agency of the United States, may be liable only to the extent provided under the Federal Tort Claims Act, 28 USC 2671 et seq.

Public Posting of Approved Users' Research Use Statements

The Institutional Requester and the Data Access Requester agree that information about themselves and the approved research use may be posted publicly on the repository website. The information may include the Data Access Requester's name and Institutional Requester, project name, and research use description. Citations of publications resulting from the use of controlled-access data obtained through the Data Access Request may also be posted on the repository website.

Terms and Definitions

Collaborator: An individual whose identity has been validated and who is a permanent employee of their institution at a level equivalent to, but not limited to, that of an academic professor (e.g., assistance, associate, or non-tenure or tenure-track professor) or senior researcher, who is not under the direct supervision of the Data Access Requester, who assists with the research project involving controlled-access data. This cannot be a lab technician or trainee, e.g., post-docs or graduate students. Internal collaborators are employees of the Institutional Requester and work at the same

institution as the Data Access Requester. External collaborators are not employees of the Institutional Requester and do not work at the same location as the Data Access Requester.

Data Access Request: A request submitted to an NIH Data Access Committee for a specific research use specifying the data to which access is sought, the planned research use, and the names of collaborators.

Data Access Requester: The individual who prepares and submits requests, Project Renewals, and Project close-outs. A Data Access Requester is a permanent employee of their institution at a level equivalent to, but not limited to, that of an academic professor (e.g., assistance, associate, or non-tenure or tenure-track professor) or senior researcher; has oversight responsibility for others named on the request who will be granted access to the data; and can be accountable for ensuring that all aspects of data usage align with the terms of the agreement. This cannot be a lab technician or trainee, e.g., post-docs or graduate students.

Data Use Agreement (DUA)/Data Use Certification (DUC)/ Data Transfer Agreement (DTA): Terms of access that include how the data accessed should be secured and used by the Data Access Requester, those they directly supervise, and any collaborators. The Institutional Requester, through the Institutional Signing Official (SO), and the Data Access Requester, are each signatories to the agreement and agree to adhere to terms of access.

Institutional Requester: The home institution or corporation of the Data Access Requester.

Institutional Signing Official: The label, "Institutional Signing Official" refers to the individual that has institutional authority to legally bind the institution in administrative matters. The individual fulfilling this role may have any number of titles in the institution but is typically located in its Office of Sponsored Research or equivalent

NIH Data Access Committee (DAC): NIH Data Access Committees (DACs) review and approve, or disapprove, requests from Data Access Requesters for proposed secondary research uses of controlled-access datasets.

Project Close-out: Termination of a research project that used controlled-access data from an NIH controlled-access data repository and confirmation of data destruction when the research is completed and/or discontinued.

Project Renewal: Renewal of a Data Access Requester's access to controlled-access datasets for a previously approved project with options to add or remove datasets, collaborators, or Key Personnel.

Progress Update: Information included with the Project Renewal or Project Close-out providing a summary of research progress and citing any presentations or publications with the approved controlled-access data.

Research Use Statement: A summary of research intent submitted by the Data Access Requester that includes information about at least the following: research objectives, study design, and analysis plan.

Submitting Investigator – The individual responsible for assuring to NIH that the data are appropriate to share as signatory to the data submission form or certification.

Submitting Institution: The home institution or corporation of the Submitting Investigator responsible for assuring to NIH that the data are appropriate to share as a signatory to the data submission form or certification.

Appendix D

Standard Provisions for Data Submission Form or Certifications

Version	Implementation Date	Summary of Changes	Sections Updated	Changes Approved By
1.0	9.22.2025	Initial release	All	OD

Note: For model submission forms or certifications whose terms may be subject to negotiation or for those NIH CADRs with existing forms with specific NIH CADR terminology, any changes must be consistent with standard submission provisions in Appendix D. The institution or corporation, through the Institutional Signing Official, and the Submitting Investigator, are each signatories to the form and agree the data are appropriate to share.

Submission forms or certifications should have these submission provisions:

- That the data was collected in a manner consistent with all applicable national, Tribal, and state laws and regulations as well as relevant institutional policies.
- That submission of the data is consistent with applicable national, Tribal, and state laws and regulations as well as relevant institutional policies.
- That expectations with explicit limitations on subsequent use, such as those imposed by laws, regulations, policies, informed consent, and agreements, as applicable, or as otherwise determined by the Submitting Institution, will be delineated at submission.
- That metadata and supporting information, materials, and documentation to adequately describe and facilitate interpretation will be submitted to NIH controlled-access data repositories at submission.
- That different offices or components of an institution with appropriate roles and expertise (such as an Institutional Review Board (IRB), Privacy Board, Human Research Protection Program (HRPP), or equivalent body) has reviewed the investigator's proposal for data submission and assures that:
    - Submission for subsequent sharing and use of the data for research purposes is consistent with explicit limitations on subsequent use, such as those imposed by laws, regulations, policies, informed consent, and agreements, or as otherwise determined by the Submitting Institution.
    - The submitted data has been de-identified to the extent required by the NIH controlled-access data repository, applicable laws, regulations, and NIH policies.
    - Consideration has been given to risks to individual participants and their families associated with data submitted to NIH controlled-access data repositories and subsequent sharing.

- Consideration has been given to risks to groups or populations associated with submitting datasets to NIH controlled-access data repositories and subsequent sharing.

Does the information to be submitted include **identifiable, sensitive information**?
□Yes □No

IMPORTANT: Research in which identifiable, sensitive information is collected or used includes research that:

- Meets the definition of human subjects' research as defined in the Federal Policy for the Protection of Human Subjects (45 CFR 46)), including exempt research in which participant information cannot be identified or their identity cannot readily be ascertained, directly or through identifiers;
- Is collecting or using human biospecimens that are identifiable or that have at least a very small risk of being used to deduce the identity of an individual;
- Involves the generation or use of individual level human genomic data from biospecimens, regardless of identifiability; or
- Involves any other information where there is at least a very small risk that a person could be identified.

Is the identifiable, sensitive information to be submitted covered by a CoC?
□Yes □No

IMPORTANT: Note that research subject to the NIH Certificates of Confidentiality Policy that involves the generation, collection, or use of identifiable, sensitive information that is funded in whole or in part by NIH is automatically deemed to be issued a Certificate of Confidentiality (CoC). For more information, see the NIH Certificates of Confidentiality webpage.