National Institutes of Health
Office of Science Policy

OHSRP Education Series

April 30, 2026

NIH Controlled-Access Data Repository Security and Operational Standards

Cheryl Jacobs, Ph.D.
Assistant Director of Genomics and Data Access, Scientific Data Sharing Policy Division
Office of Science Policy

AGENDA

- Background & Gaps — The regulatory landscape and why NIH needed to act
- Defining NIH CADRs — Establishing a framework for controlled-access data repositories
- NIH CADR Requirements — Standards developed to harmonize security, access, and transparency
- Compliance & Implementation — Pathways to compliance and the rollout timeline
- For Investigators — What researchers need to know

NIH DATA REPOSITORY LANDSCAPE

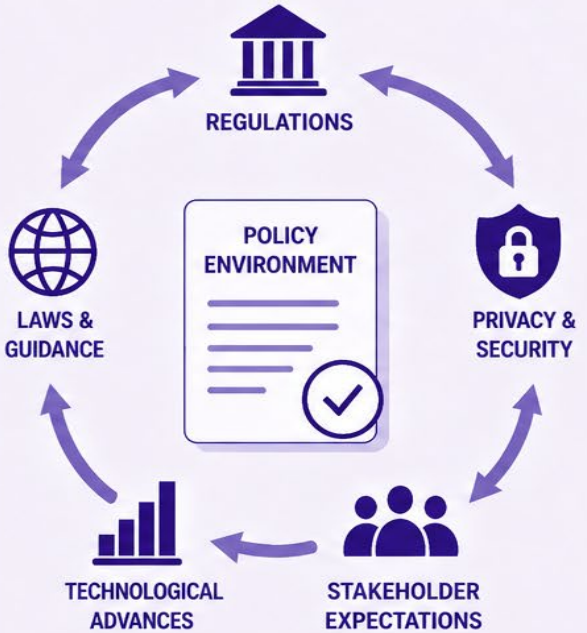
NIH provides substantial capacity to the research community for storing and managing controlled access

SECURE. SCALABLE. RELIABLE.

Repository controls vary across NIH and risk further divergence as new infrastructure is developed

NIH INSTITUTE A	NIH INSTITUTE B	NIH INSTITUTE C	NIH INSTITUTE D
CONTROLLED ACCESS	CONTROLLED ACCESS	CONTROLLED ACCESS	CONTROLLED ACCESS
ACCESS CONTROLS • Role-based access • Encryption at rest • Data use agreements	ACCESS CONTROLS • Role-based access • Multi-factor authentication • Audit logging • Data use agreements	ACCESS CONTROLS • Role-based access • Encryption at rest and in transit • Audit logging	ACCESS CONTROLS • Role-based access • Data enclaves • No download • Data use agreements • Audit logging

The policy environment for controlled-access repositories continues to evolve rapidly



CONTINUOUS CHANGE. ONGOING ADAPTATION.

EXTERNAL POLICY AND OVERSIGHT DRIVERS IMPACTING NIH CONTROLLED-ACCESS DATA MANAGEMENT

National Institutes of Health
Office of Science Policy

DOJ Final Rule for E.O. 14117:

Restricts bulk sensitive personal data transactions with countries of concern, including genomic, transcriptomic, epigenomic, and proteomic data from more than 1,000 U.S. persons

Consolidated Appropriations Act, 2023 (H.R. 2617):

Mandates HHS/NIH to update genomic data sharing policies for national security risk and develop a framework for managing risks related to human genomic data

HHS Controlled Unclassified Information (CUI) Policy (under development)

could impact how NIH manages and provides data that qualifies as CUI, including controlled-access data

Ongoing oversight:

Multiple Congressional reports and inquiries from GAO and OIG related to controlled access operations

IDENTIFIED GAPS IN NIH REPOSITORY OVERSIGHT

National Institutes of Health
Office of Science Policy

- The Scientific Data Council-Data Science Policy Council Controlled Data Access Coordination WG Finding (2021) that NIH lacked the foundational elements needed for consistent, secure data governance
  - No unified framework — Missing common policy and implementation standards for data deposition and sharing
  - Inconsistent risk management — No standardized approach to identifying and managing risks across repositories
  - Siloed oversight — Limited communication across NIH repository oversight bodies and Data Access Committees (DACs)
- These gaps challenged the ability of NIH to respond effectively and consistently across the repositories

DEFINING NIH CONTROLLED-ACCESS DATA REPOSITORIES (CADRS)

- OSP catalogued repositories and identified 40+ that were supported by NIH, used an NIH oversight body to review and approve requests, and provided long-term storage
- OSP presented this analysis to NIH Leadership for a decision on what categories should be determined as controlled

NIH Leadership Definition — To be an NIH CADR, repository must meet the following criteria:

- 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;
- Control access to data by prospective review of data access requests or partner with access systems that control access via prospective review of requests; and
- Use federal employees to conduct reviews and authorize access, or partner with access systems that use federal employees for those purposes.

WHY THIS DEFINITION MATTERS

The Impact:

- With this framework in place, NIH could move forward with policy development to address:
  - Heterogeneous controls and access processes across CADRs
  - Inconsistent security systems
  - Outstanding legal, regulatory, and policy requirements

DEVELOPING THE NIH CADR REQUIREMENTS

OSP, OCIO, ODSS and OER, with input from a Trans-NIH Working Group of subject matter experts (SMEs) developed:

- "Required Security and Operational Standards for NIH Controlled-Access Data Repositories" (NOT-OD-25-159)
  - Strengthens protections for the privacy and autonomy of research participants
  - Harmonizes submission and access processes across NIH CADRs
  - Establishes clear security requirements for repositories and users
  - Sets standards for public transparency
  - Facilitates implementation of forthcoming mandates

National Institutes of Health
Office of Science Policy

NIH CADR REQUIREMENTS – FOUR CATEGORIES

CATEGORY	DESCRIPTION
Laws and Policies	Documentation of adherence to relevant laws and policies
Data Access	Standard processes for reviewing and granting access to controlled data
Data Submission	Standard processes for submitting data to NIH CADRs
Security and Transparency	Security standards for NIH CADRs and users of NIH CADR data; public transparency requirements

Detailed requirements are described in the NIH CADR Guidebook

National Institutes of Health
Office of Science Policy

COMPLIANCE OPTIONS FOR NIH CADRS

- Adopt Requirements Directly: Implement required standards or partner with a system that has already met them
- Pause Access: Disable all controlled-access data access and halt new requests until standards are met
- Migrate Data: Move controlled-access data to another NIH CADR that has already met all standards
- Decontrol Data: Recommend specific datasets to OCIO for decontrolling

National Institutes of Health
Office of Science Policy

NIH CADR REQUIREMENTS IN MORE DETAIL

Documentation of Adherence to Relevant Laws & Policies

- Certificates of Confidentiality: Determine applicability; develop SOP to prevent compelled disclosure
- FOIA: Determine applicability; develop SOP to route FOIA requests appropriately
- Privacy Act: Determine applicability; maintain a Privacy Impact Assessment (PIA) and System of Records Notices (SORNs)
- Common Rule: Determine whether the CADR constitutes human subjects research requiring IRB review

Standard Data Access Processes

- Use Data Use Agreements (DUAs) containing minimum required terms of access
- Follow a standard access review process
- Use NIH Data Access Committees (DACs) for all request reviews

National Institutes of Health
Office of Science Policy

NIH CADR REQUIREMENTS IN MORE DETAIL CONT.

Standard Data Submission Processes

- Use data submission forms containing minimum required terms

Security Standards and Practices

- NIH CADRs must adopt controls per NIH Security Best Practices for Controlled-Access Data Repositories
- Data users of NIH CADR data must comply with NIH Security Best Practices for Users of Controlled-Access Data
- Developers supporting NIH CADR infrastructure or developing tools agree to terms of access and oversight
- NIH CADRs implement Research Authentication Services (RAS) and standard identity proofing

Transparency & Utility Standards

- Collect and publicly share metadata to enable discovery, reuse, and citation of datasets
- Make information on research uses publicly available — both individually and in aggregate
- Maintain documentation of Certificate of Confidentiality status for all datasets

IMPLEMENTATION TIMELINE & REVIEW

Phased Implementation

- Phase 1: January 27, 2026
  - Documentation of adherence to relevant laws and policies
  - Data Access Processes
- Phase 2: April 1, 2026
  - Standard Data Submission Processes
  - Security Standards and Practices
- Phase 3: Fall 2026
  - Transparency and Utility Standards

- OCIO, with support from the Secure Data Science (SDS) Team and OSP, reviews submitted evidence
- Evidence is assessed as Complete, Needs Revision, or Ongoing

National Institutes of Health
Office of Science Policy

WHAT TO KNOW

- Investigator data sharing is not necessarily within scope of the NIH CADR Requirements
  - Reach out to the Science Policy mailbox (sciencepolicy@od.nih.gov) for questions about if the NIH CADR requirements may apply

Thinking of Standing Up a New NIH CADR?

- Consider sharing through an existing NIH CADR first
- Reach out to the SDS Team: SecureNIHDataScienceSupportServicesTeam@mail.nih.gov

Questions About How Users Secure NIH CADR Data ?

- Review Resources (at the bottom of the webpage) on the NIH CADR Requirements webpage
  - 2026 Community Days covers user responsibilities and how to meet compliance
  - FAQs about NIH Security Best Practices

Any Questions About What Was Covered Today?

- Reach out to the Science Policy mailbox (sciencepolicy@od.nih.gov)