



Final NIH Policy for Data Management and Sharing

Briefing Sheet — Institutional Leadership

Executive Summary:

In October 2020, NIH issued 4 Notices to convey upcoming additional Data Management and Sharing requirements that are effective January 2023. The new requirements will require a data management and sharing plan for ALL NIH-funded projects, an expansion from the current requirement for projects over \$500K in annual direct costs. Proper data management and sharing are critical research practices to accelerate scientific advancement and support scientific integrity. These requirements may vary between NIH Institutes, Centers, and Offices. Institutions will need to 1) foster a significant cultural shift for researchers at the lab level to re-think how data is collected and shared for broader use, 2) plan for how numerous new compliance requirements may be met, 3) engage data management experts to help researchers meet the new requirements and resolve new data management issues that arise as a result of these new requirements, and 4) support new data sharing and management costs that may not be borne by NIH or other sponsors.

Section 1. Regulations:

Applicable Policies (Released October 2020 // **Effective Date: January 25, 2023**)

1. [NIH-OD-21-013](#)—Final NIH Policy for Data Management and Sharing
2. [NOT-OD-21-014](#)—Supplemental Information to the NIH Policy for Data Management and Sharing: Elements of an NIH Data Management and Sharing Plan
3. [NOT-OD-21-015](#)—Supplemental Information to the NIH Policy for Data Management and Sharing: Allowable Costs for Data Management and Sharing
4. [NOT-OD-21-016](#)—Supplemental Information to the NIH Policy for Data Management and Sharing: Selecting a Repository for Data Resulting from NIH-Supported Research

POLICY OBJECTIVE: Maximize research outcomes (taxpayer dollars) while supporting rigor & reproducibility through leading a “cultural shift that makes data sharing the norm.” It also emphasizes the importance of good data management practices and establishes the expectation for maximizing the appropriate sharing of scientific data generated from NIH-funded or conducted research, with justified limitations or exceptions. This Policy applies to research funded or conducted by NIH that results in the generation of scientific data.

BACKGROUND:

- [2003 Policy](#) on Data Sharing (in effect until January 2023)
 - Applies to grants > \$500k and requires a plan for sharing and “timely release and sharing” of data
- [2008 NIH Public Access Policy](#): Requires all NIH-funded researchers to submit or have submitted to the National Library of Medicine’s [PubMed Central](#) an electronic version of their final, peer-reviewed manuscript, to be made publicly available no later than 12 months after the official date of publication
- [2013 OSTP Memo](#): “Increasing Access to the Results of Federally Funded Scientific Research.” Each Federal agency with over \$100 million in R&D expenditures must develop a plan to support increased public access to results of funded research inclusive of peer-reviewed manuscripts and articles and research data.
 - As of November 2021, all 20 federal departments and agencies subject to the Memo are in compliance. Several agencies with R&D below \$100 million have also adopted these principles.
- [2015 NIH Genomic Data Sharing](#) (applies to large scale human or human genomic data):
 - Establishes expectations for protection of human data and informed consent
 - Suggests repositories (e.g., dbGaP)

NEW POLICIES:

- **Effective January 25, 2023** (ICO policies may implement effective dates prior to January 2023)
- **Applies to all research that generates scientific data** (scientific data defined in the policy)
- NIH policy [NIH-OD-21-013](#) sets out a minimum standard for Data Management and Sharing (DMS) Plans at NIH. NIH Institutes, Centers, and Offices (**ICOs**) **are expected to issue more specific supplemental requirements for DMS plans**, for example, new standards for the interoperability of data sets.
- Requirements: DMS Plan **required at the time of proposal**
- DMS Plan Definition: A DMS Plan should reflect the proposed approach to data management and sharing at the time it is prepared and be updated during the award/support period to reflect any changes in the management and sharing of scientific data (e.g., new scientific direction, new repository option, timeline revision). NIH encourages data management and sharing practices to be consistent with the [FAIR \(Findable, Accessible, Interoperable, and Reusable\)](#) data principles and reflective of practices within specific research communities. NIH recommends addressing all elements described below.
- A DMS Plan outlines how scientific data will be shared, including metadata, and identifies potential restrictions / limitations). Recommended elements include:
 - Description of the plan
 - Related tools and software
 - Standards

- Data preservation
- Access/reuse considerations
- Oversight of plan (see [NOT-OD-21-014](#))

ON THE HORIZON:

- NIH ICOs with existing data management and sharing plans may modify their requirements to harmonize policies.
 - For example, NIH closed an [RFI on proposed changes](#) to the 2015 Genomic Data Sharing Policy on February 28, 2022 (see [COGR's 2/28/22](#) and [ARL's](#) response).
- NIH may develop more granular data management and sharing policies based on data types, participant type, and data sensitivity.
- NIH [issued an RFI](#) on January 25 to develop supplemental information—Policy for Data Management and Sharing: Responsible Management and Sharing of American Indian/Alaska Native Participant Data (see [COGR's 3/28/22 response](#)).
- NIH and ICO policies (as they become available) can be found at COGR's website here: <https://www.cogr.edu/nih-data-management-and-sharing>.

Section 2. Faculty and Institutional Implications:

FACULTY

- **Culture change:** data and associated management will not be a by-product of research, but an inherent part of good scientific practices.
- **All NIH-funded principal investigators** will need to become proficient in developing DMS Plans and/or utilizing institution support to properly manage data.
- **Costing Challenges: the magnitude will vary by institution.** The move towards requiring that resulting research data, software, and coding be in a form and format to be shared broadly outside of the research group will require planning and staff work to ensure the data is clean and usable. Therefore, data management and sharing experts (typically in libraries and/or research computing services) will be critical to helping principal investigators develop sound strategies before a project begins. For those principal investigators who can make use of NIH-supported repositories, data sharing costs will be insignificant while for others, sharing requirements may be very significant. NIH-funded data repositories are not expected to charge additional fees and use of them should limit new storage costs.
- DMS Plan management and compliance **monitoring will be required** and possibly audited/monitored externally.
- **Training and educational offerings will be necessary** (potentially leveraging Responsible Conduct of Research training) and should include elements such as: data ethics, sensitive data, data de-identification and/or anonymization, curating data for re-use.

INSTITUTION

- **Increased cost** (capital and labor) to support faculty in the development, management, monitoring, and compliance oversight of DMSs
- **Increased storage costs**, particularly after the end of the project, particularly for large data sets, sensitive data, or where an external data repository does not exist
- **Increased discipline** related to data management under [FAIR](#) principles

INSTITUTIONAL SOLUTIONS NEEDED TO SUPPORT AND PROMOTE THE POLICY (CONCEPTUALLY IN FOUR LIFECYCLE COMPONENTS)

1. Identify need for Data Management and Sharing
 - DMS Plan Development
 - DMS Monitoring & Compliance over life of award through closeout
 - DMS Monitoring & Compliance—post closeout
 - Data Ingest
2. Data Storage
 - During life of project
 - Post-closeout for publication
 - Post-closeout for DMS Compliance
 - Post-closeout / last resort
3. Data Management & Publishing
 - Curating data according to [FAIR](#) and/or ethical data sharing principles (such as [CARE](#))
 - Data publication fees (often based on size, sensitivity, and duration of data)
4. Data Security
 - Security for sensitive data (PHI, HIPAA, Export Controls, FISMA, student data and IP, DUA compliance)

The breadth of culture change, business process impact, faculty burden, and cost will vary significantly by institution and faculty discipline & experience. The examples below illustrate the breadth on implications.

Faculty member conducting non-data-intensive work

- Data Profile:
 - Security classification: Low—Unauthorized access, use, disclosure, or loss is likely to have low or no risk to individuals, groups, or the institution.
 - Data types: tabular, publicly available data, etc.
 - Volume: less than 1 terabyte
- Implications:
 - Needs assistance in creating DMS, monitoring; needs assistance with data ingest/curation/metadata management, etc.

- Does not need assistance in data storage/sharing because needs are low and likely data at end of the project will go to a generalist (institutional, [Dryad](#), [Figshare](#), etc.) repository

Faculty member doing low-mid data-intensive work

- Data Profile:
 - Security classification: Moderate—Unauthorized access, use, disclosure, or loss is likely to have adverse effects for individuals, groups, or the institution, but will not have a significant impact on the institution. These adverse effects could include but are not limited to social, psychological, reputational, financial, or legal harm.
 - Data type: tabular, scientific images, etc.
 - Volume: between 1 and 10 terabytes
- Implications:
 - Needs some assistance in creating DMS, assistance of monitoring and compliance with DMS as it is likely to change throughout the life of the award
 - May need some assistance in data storage/sharing because it is likely data at end of the project will go to a disciplinary, institutional, or generalist provided data repository

Faculty member doing data-intensive work

- Data Profile:
 - Security classification: High (not restricted)—Unauthorized access, use, disclosure, or loss is likely to have significant and severe adverse effects for individuals, groups, or the university. These adverse effects could include, but are not limited to, social, psychological, reputational, financial, or legal harm. Data may include PII or HIPAA information.
 - Data type: tabular—genomic, scientific images, sensor data, etc.
 - Volume: greater than 10 terabytes
- Implications (discipline-dependent):
 - Needs some assistance in creating DMS, significant assistance of monitoring and compliance with DMS as it is likely to change throughout the life of the award
 - Needs assistance in data storage/sharing
 - Needs to consider post-award data management and storage

Section 3. Resources

[COGR's Webpage on NIH Data Management and Sharing](#)

[NIH Scientific Data Sharing Website](#)

[ARL Research Data](#)

INSTITUTIONAL GUIDES AND RECOMMENDATIONS:

AAU/APLU [Guide to Accelerate Public Access to Research Data](#)

[National Academies of Sciences, Engineering, and Medicine \(NASEM\) Changing the Culture of Data Management and Sharing: A Workshop](#)

FEDERAL AGENCY POLICY REFERENCES AND REPORTS:

[NIH Data Sharing Policy](#)

[NIH Data Management and Sharing Activities Related to Public Access and Open Science](#)

[Selecting a Repository for Data Resulting from NIH-Supported Research](#)

[2021 OSTP Public Access Congressional Report](#)

This document is a joint release from COGR and the Association of Research Libraries (ARL). If you have any questions regarding this document, please contact David Kennedy at dkennedy@cogr.edu or Toni Russo at trusso@cogr.edu.

About COGR & the Association of Research Libraries:

COGR is an association of almost 200 research universities and affiliated academic medical centers and research institutes. COGR concerns itself with the impact of federal regulations, policies, and practices on the performance of research conducted at its member institutions. COGR is on the web at cogr.edu.

The Association of Research Libraries (ARL) is a nonprofit organization of 126 research libraries in Canada and the US whose mission is to advance research, learning, and scholarly communication. The Association fosters the open exchange of ideas and expertise; advances diversity, equity, and inclusion; and pursues advocacy and public policy efforts that reflect the values of the library, scholarly, and higher education communities. ARL forges partnerships and catalyzes the collective efforts of research libraries to enable knowledge creation and to achieve enduring and barrier-free access to information. ARL is on the web at ARL.org.