National Institutes of Health (nih.gov): NIH Data Management and Sharing Plan (2026 Pilot DMS Plan Format)

Data Management and Sharing Plan

Will there be maximum appropriate sharing of scientific data underlying peer-reviewed publications and other findings resulting from the work supported by this award (including preprints, refereed papers reported at conferences, and other findings)?

- Yes
- No

Guidance:

Researchers are expected to maximize the appropriate sharing of scientific data, which is defined as data commonly accepted in the scientific community as being of sufficient quality to validate and replicate the research findings. NIH expects that researchers will take steps to maximize scientific data sharing, but may acknowledge in Plans that certain factors (i.e., ethical, legal, or technical) may necessitate limiting sharing to some extent. Foreseeable limitations should be described in DMS Plans - this occurs in Element 4.

Relevant NIH FAQs/links:

What are some examples of data the DMS Policy does not expect researchers to share?
What are justifiable reasons for limiting sharing of data?
If researchers are reusing existing, shared data to generate new datasets, are they expected to reshare the primary data they incorporated into their new analysis?
Additional policies of specific NIH Institutes and Centers

Will the scientific data underlying peer-reviewed publications be shared by the time of publication, or for other findings, by the end of the period of performance, which includes no-cost extensions?

- Yes
- No

Guidance:

Scientific data should be made accessible as soon as possible. More specifically, the DMS Policy expects scientific data to be shared by the earlier of these two timepoints:

The time of an associated publication: Scientific data underlying peer-reviewed journal articles should be made accessible no later than the date on which the article is first made available in print or electronic format.
The end of the performance period: Scientific data underlying findings not disseminated through peer-reviewed journal articles should be shared by the end of the performance period unless the grant enters into a no-cost extension. If a no cost extension is permitted, then the recipient should share the data by the end of the extended performance period.
Relevant NIH FAQs/links:

Do SBIR/STTR projects have to share scientific data under the DMS Policy?
Do scientific data underlying an invention that is the subject of a patent application need to be shared? If so, when?

Will shared scientific data be made available for at least as long as required by applicable data repository policies and/or journal policies?

- Yes
- No

- Not Applicable

Guidance:

Recipient institutions are required to keep the data for 3 years following closeout of a grant or contract agreement. Please note that the recipient institution may have additional policies and procedures regarding the custody, distribution, and required retention period for data produced under research awards.

Researchers are encouraged to consider relevant requirements and expectations (e.g., data repository policies, award record retention requirements, journal policies) as guidance for the minimum time frame that scientific data should be made available, which researchers may extend.

DMP Tool note:

Repository selection is addressed in guidance for Element 6. Repository documentation may include retention and preservation timeline information that impacts responses here. Journals may have further data retention policies relevant to this question (See the Data Availability Policies Index)

If you answered "no" to elements 1, 2, or 3, or if you anticipate that sharing will be limited in some other way, please describe these limitations and the ethical, legal, or technical factors for them. Your response should specify a particular reason(s) for limiting sharing.

Example Answer:

The proposed research will involve a small sample (less than 20 participants) recruited from clinical facilities in the New York City area with Williams syndrome. This rare craniofacial disorder is associated with distinguishing facial features. Even with the removal of all identifiers, we believe that it would be difficult if not impossible to protect the identities of subjects given the physical characteristics of subjects, the type of clinical data (including imaging) that we will be collecting, and the relatively restricted area from which we are recruiting subjects. Therefore, we are not planning to share the data.

Guidance:

Examples of justifiable factors for limiting scientific data sharing include:

informed consent will not permit or will limit the scope or extent of sharing and future research use
existing consent (e.g., for previously collected biospecimens) prohibits sharing or limits the scope or extent of sharing and future research use
privacy or safety of research participants would be compromised or place them at greater risk of re-identification or suffering harm, and protective measures such as de-identification and Certificates of Confidentiality would be insufficient
explicit federal, state, local, or Tribal law, regulation, or policy prohibits disclosure
restrictions imposed by existing or anticipated agreements (e.g., with third party funders, with partners, with repositories, with Health Insurance Portability and Accountability Act (HIPAA) covered entities that provide Protected Health Information under a data use agreement, through licensing limitations attached to materials needed to conduct the research)
datasets cannot practically be digitized with reasonable efforts
Examples of reasons that would generally not be justifiable factors limiting scientific data sharing include:

data are considered to be too small
data that researchers anticipate will not be widely used
data are not thought to have a suitable repository
Relevant NIH FAQs/links:

If researchers are reusing existing, shared data to generate new datasets, are they expected to reshare the primary data they incorporated into their new analysis?
Additional considerations around American Indian/Alaska Native data

If scientific data derived from human research participants will be shared, will privacy, rights, and confidentiality of participants be protected as outlined in NOT-OD-22-213?

- Yes
- No
- Not Applicable

Guidance:

NOT-OD-22-213 outlines 6 operational principles and 3 best practices to consider (more details at notice link):

Operational Principles for Protecting Participant Privacy When Sharing Scientific Data:

Proactive assessment of protections.
Clear communication of data sharing and use in consent forms.
Consideration of justifiable limitations to sharing data.
Institutional review of the conditions for data sharing.
Protections for all data used in research.
Remaining vigilant regarding data misuse.

Best Practices for Protecting Participant Privacy When Sharing Scientific Data:

Apply Appropriate De-identification.
Establish Scientific Data Sharing and Use Agreements.
Understand and Communicate Legal Protections Against Disclosure and Misuse.
Relevant NIH FAQs/links:

Considerations for Scientific Data Derived from Human Participants

Data Outputs Table

Expected Data Outputs Table

Example Answer:

Expected Data Type	Established Repository or Example
Mouse scRNA-seq	Gene Expression Omnibus (GEO)
Mouse functional magnetic resonance imaging data	OpenNeuro
Mouse tissue histology staining images	Zenodo
Human genomic data	Database for Genotypes and Phenotypes (dbGaP)
Human survey and interview data	Inter-university Consortium for Political and Social Research (ICPSR)

DMP Tool Note: These are example repositories for these data types. There may be other appropriate options to choose from as well. Make sure to keep your total table under 100 words.

Guidance:

For data generated from research involving programs and types of data where NIH policy(ies) and/or funding opportunities identify particular data repositories, researchers should use the designated data repository. For genomic data, consider this table of frequently used human genomic data repositories.

For data generated from research for which no data repository is specified by NIH, consideration should be given to data repositories that are discipline or data-type specific and conform to the NIH's list of desirable characteristics. For a list of NIH-supported repositories, visit Repositories for Sharing Scientific Data.

If no appropriate discipline or data-type specific repository is available, consider other potentially suitable data sharing options:

Accompanying articles submitted to PubMed Central
Data repositories, includingGeneralist repositories (more information and resources on generalist repositories is available);
Institutional repositories that make data available to the larger research community, institutions, or the broader public
Large datasets may benefit from cloud-based data repositories
Reasonable, allowable costs may be included in NIH budget requests when associated with curating data and developing supporting documentation, local data management considerations, and preserving and sharing data through established repositories.

Genomic Data Sharing Policy (GDS)

a. Will you share all large-scale human genomic and associated data in a NIH-designated repository according to the accelerated timelines expected in the GDS Policy? If "No," address in Element 4 in the first section.

- Yes
- No
- Not Applicable

Guidance:

NIH expects the broad and responsible sharing of human as well as non-human genomic data resulting from NIH-funded research because the timely sharing of research results can accelerate discoveries that improve our ability to diagnose, treat, and prevent disease.

To comply with the NIH Genomic Data Sharing Policy, NIH expects that investigators and institutions:

Provide an Institutional Certification form at Just-in-Time, if working with human data
Submit genomic data in a timely manner to an appropriate repository
Responsibly use controlled-access data
Appropriately cite controlled-access data in publications and presentations
A separate GDS Plan is not required.

Relevant NIH FAQs/links

Additional genomic data sharing expectations by NIH Institute & Center
Genomic Data Sharing Policy Notice with links to updates
Request for Information on Draft NIH Controlled-Access Data Policy and Proposed Revisions to NIH Genomic Data Sharing Policy
Requirements for NIH Controlled-Access Data Repositories and Users

7b. Do you anticipate that when sharing you will be able to meet the expectations of the Institutional Certification in the GDS Policy? If "No," address in Element 4 in the first section.

- Yes
- No
- Not Applicable

Guidance:

The responsible Institutional Signing Official of the submitting institution should provide an Institutional Certification to the funding IC prior to award consistent with the genomic data sharing plan submitted with the request for funding. For obligations that Institutional Certifications must address, see section 5, Institutional Certification, of the GDS Policy. Investigators are responsible for working with the Institutional Signing Official for this certification, which must be done prior to award.

By signing an Institutional Certification, an institution and its IRB, privacy board, or similar body assure NIH that:

The study submission is consistent with relevant (e.g., local, state, federal, Tribal, and/or institutional) laws and policies
The certification states the data use limitations, if any, on secondary research performed with the data
The participants' identities will not be disclosed to NIH-designated data repositories
An IRB or equivalent body has reviewed the proposal and assures NIH that:The data collection protocol appropriately protects the research participants
The submission and sharing of the data are consistent with the informed consent of the study's participants; and
The risks associated with genomic data sharing have been considered.
See the Institutional Certification form for a complete list of all assurances.

Exceptions may be requested when the Institutional Certification criteria cannot be met, and the investigator should provide a justification for the exception in the application in Element 4