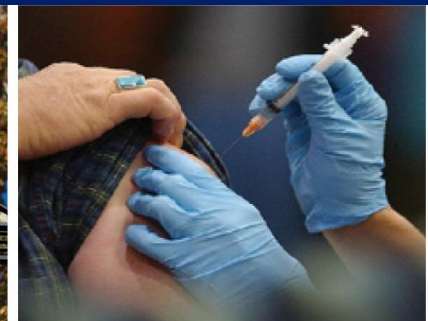


Ask RCRA

January 19, 2023

NSPM –33 Update



NSPM-33 @ Emory



Disclosure Requirements and Standardization

Consequences for Violation of Disclosure Requirements



Digital Persistent Identifiers (DPIs)

ORCID



Research Security Programs

- Information Sharing
- Cybersecurity
- Foreign Travel Security
- Trainings



Disclosure Compliance

- eDisclose implemented
- Annual Certifications – in progress
- Disclosure & Management Plan Monitoring
- New streamlined processes with IRB, IACUC
- School accountability & collaboration - CBOs, ADRs



Policies

Visiting Scholar

Export Controls

Foreign Travel Security

Research Data Protection

- Data Sharing Standards - in accordance with NIH Policy requirements

COC – Faculty & Research Staff

COI Research



ORCiDs

Emory Libraries - Jody Bailey & Team

OIT worked to integrate ORCID iDs into Emory Shared Data and other Emory IT systems

This team collaborated with [ORCID US Community](#) Specialist at Lyris (host organization for ORCID US Community) on the technical aspects of the integration.

Number of Emory researchers whose ORCID iD is now connected to Emory: 652 (11/28/2022)



RSP - Foreign Travel Security



- Led by Foreign Travel Subcommittee – GSI, Travel, OGC, Compliance, GHI, Risk Management
- International Travel Policy
 - Currently under review
 - Approval -summer 2023
- Travel Briefings - GSI
 - Faculty, Staff
 - Dept Level Briefings
- Travel Registry
 - RFP
 - Timeline - Fall 2023
- Loaner Laptop Program

RSP - Loaner Laptop Program

Provide laptops to faculty and staff who:

- Travel to high-risk destinations
- Data that may be deemed sensitive or restrictive

Laptop Use Criteria

- Countries – OFAC, China, Dept of State Level 4
- Research Data Risk Prioritization – High, Medium, Low - benchmark with Stanford's established program



RSP - Research Data Protection

Partnering
with OIT,
Information
Security

- New Policy draft
- Outlines responsibilities of the enterprise, the schools, and the investigator
- Data sharing standards



RSP - Cybersecurity

NSPM-33 has 14
cybersecurity elements
defined

In alignment with other
information
security standards that
we are actively pursuing
(NIST 800-171)



RSP - TRAININGS

- Cybersecurity
 - Staff – currently provided as part of onboarding
 - Students & Faculty – to be added
 - Content refresh – depending on agency guidance
- Research Security
 - TBD – frequency, content, learner population
- Export Controls
 - In progress as part of FY 23 Work plan activities



Compliance Plan & Monitoring

- NSPM-33 Compliance Plan – in progress
- Monitoring
 - COI/COC
 - Data Sharing – NIH policy, new research project consults
 - Foreign Travel – Research Security & Export Control screenings
 - Training completion compliance



DMS Policy Overview

Applicability

All research, funded or conducted in whole or in part by NIH, that results in the generation of "**scientific data**".

The recorded factual material commonly accepted in the scientific community as of sufficient quality to validate and replicate research findings, regardless of whether the data are used to support scholarly publications.

Requirements

- ✓ **Submission of DMS Plan** with all applications for funding
- ✓ **Compliance with the DMS Plan** approved by the funding NIH Institute, Center, or Office



Activities Subject to the DMS Policy

APPLIES TO...

All research generating scientific data, including but not limited to:

- Research Projects
- Certain Career Development Awards (Ks)
- Small Business SBIR/STTR
- Research Centers

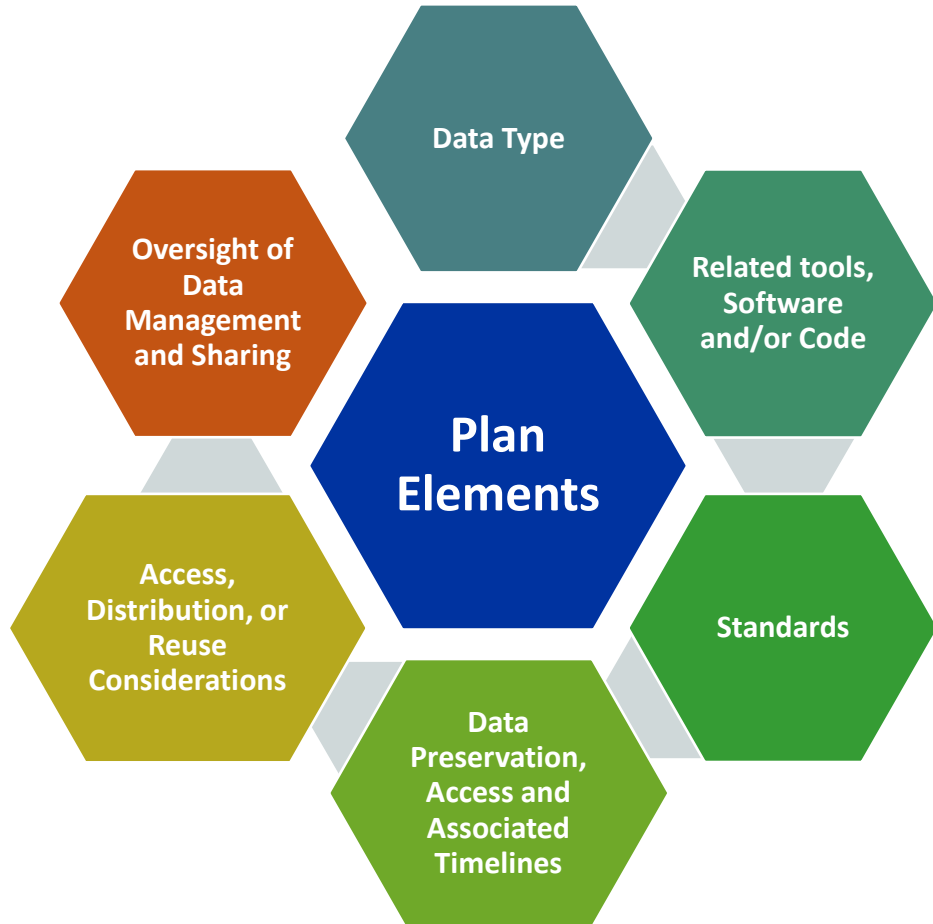
DOES NOT APPLY TO...

research projects not generating scientific data or non-research projects, including but not limited to:

- Training (Ts)
- Fellowships (Fs)
- Construction (C06)
- Conference Grants (R13)
- Resources (Gs)
- Research-Related Infrastructure Programs (e.g., S06)



Elements of a DMS Plan



- ✓ Plans should be no more than 2-3 pages in length
- ✓ No hyperlinks or URLs
- ✓ Optional format page will be available from NIH forms, or use template from DMPTool (dmptool.org)



Emory Dataverse

sco.library.emory.edu/dataverse

- **Dataverse** is Emory's open data repository, offered through a partnership between Emory and UNC's Odum Institute.
- Data deposited with the Emory Dataverse is made available through a web-accessible repository at no cost to depositors or users.
- **Provides persistent access to your data.** Each dataset in Dataverse is assigned a Digital Object Identifier (DOI) for reliable citation and linking.



Compliance/Enforcement

- Extramural Awards: The Plan will become a Term and Condition of the Notice of Award. Failure to comply with the Terms and Conditions may result in an enforcement action, including additional special terms and conditions or termination of the award, and may affect future funding decisions.
- Questions will be added to Research Performance Progress Report (RPPR) to help determine compliance with Plan



Resources

- NIH Data Sharing FAQs: <https://sharing.nih.gov/faq>
- National Institute for Mental Health (NIMH) Example Data Sharing Plans:
 - <https://www.nimh.nih.gov/funding/managing-your-grant/nimh-data-sharing-for-applicants-and-awardees#4>
- DMPTool NIH Contest award winner:
 - [https://dmptool.org/plans/74502/export.pdf?export\[question_headings\]=true](https://dmptool.org/plans/74502/export.pdf?export[question_headings]=true)

Contact: dataplan@emory.edu

More information: <https://researchdata.emory.edu/plan/nih-dmsp.html>

