Policy Title: Research Data Management and Security
Category: Research
Sponsor: Executive Vice President for Research
Effective Date: November 15, 2023

INTRODUCTION AND PURPOSE.

The University's commitment to research excellence is dependent on maintaining a rigorous data management and security practice. The purpose of this policy is to outline the obligations and responsibilities of the University, the Principal Investigator (PI), and any other researchers regarding the acquisition, storage, management, and security of primary Research Data and Materials.

SCOPE AND APPLICABILITY.

This policy is applicable to all RFUMS faculty, staff, students, visiting scholars, postdoctoral fellows, and any other persons affiliated with RFUMS who participate in the creation, acquisition, access, use, management, sharing, retention, and disposal of Research Data and Research Materials, either on behalf of or at RFUMS. This policy applies to all research activities, regardless of funding status or funding source, except where specific sponsor requirements take precedence.

POLICY STATEMENTS.

Responsibilities

The responsibilities of RFUMS include, but are not limited to: 1) complying with the terms of sponsored project agreements; 2) ensuring the appropriate use of project resources, e.g., animals, human participants, recombinant DNA, biological agents, radioactive materials, etc.; 3) protecting the rights of researchers, including, but not limited to, their rights to access data from research in which they participated; 4) securing intellectual property rights; 5) facilitating the investigation of charges, such as research misconduct or conflict of interest; 6) maintaining confidentiality of research data, where appropriate, and 7) complying with applicable state, federal, or international laws and regulations.

The responsibilities of the PI include, but are not limited to: 1) ensuring proper management of research data in accordance with this Policy; 2) establishing and maintaining appropriate procedures for the protection of research data and other essential records, particularly for long-term research projects; 3) ensuring compliance with program requirements; 4) maintaining confidentiality of research data, where appropriate, and 5) complying with applicable state and federal laws and regulations.

Data Collection and Archiving.

PIs are expected to comply with any RFUMS policies related to the collection and archiving of electronic data. Where appropriate, PIs must also comply with all predetermined data archiving agreements, or data management plans, as defined in contracts, grants, or other agreements.

For policy related to data ownership and sharing, data retention, data destruction, and data transfer, please refer to the university's Research Data Retention Policy.

Personal Electronic Devices

PIs must ensure that any personal devices used to access RFUMS information systems or collect research data are used in a secure, authorized, and responsible manner, and that any research data collected or produced is transferred to an RFUMS device or administered location. Under no circumstances should research data be stored exclusively on any personal devices such as laptops, hard drives, external hard disk drives, USB drives, or any other electronic storage device or service not administered by RFUMS.

Data Security

PIs must ensure that research data are securely protected. The PI should work with the university's Security Officer to develop a security plan that ensures the protection of sensitive research data and proprietary information. Such a plan is required if necessary to maintain compliance with applicable RFUMS policies, other contracts, grants or agreements, or state and federal laws and regulations.

DEFINITIONS.

Research Data: Information that is created or collected in the process of performing research regardless of how it is recorded or stored. This includes both tangible data (original electronic data files; recorded notes; Personal Identifiable Information; films, instrument printouts, digital storage devices, etc.) and intangible data (analyses, statistics, etc.), as well as any other materials or documentation that can be used to reconstruct published research findings.

Research Materials: Includes, but are not limited to, new, modified or unmodified biological specimens, animal models or chemical compounds, computer software.

POINTS OF CONTACT.

The Executive Vice President for Research, RFUMS has authority for compliance with this Policy and is responsible for its implementation. The Research Data Management Coordinator serves as the subject matter expert and contact for questions about interpretation and implementation of this Policy. The university's Security Officer should be consulted on matters related to the security, storage, and sharing of electronic research data or materials.

REFERENCES AND RELATED POLICIES.

Manual on Responding to Allegations or Evidence of Possible Research Misconduct

RFUMS Guidelines for the New NIH Data Sharing Policy

RESOURCES

NOT-OD-21-013 (NIH Policy for Data Management and Sharing).

POLICY HISTORY.

Policy issue date: November 15, 2023

Policy updates: N/A