SECTION: Research **Number: 08.03.01**
AREA: Research Integrity and Oversight

SUBJECT: Data Management and Sharing

I. PURPOSE AND SCOPE

Data Management is the process of controlling and appropriately handling the information generated during a research project, including the storage, access and preservation of data throughout the research life cycle and beyond. In accordance with SAM 07.A.08, Data Classification and Protection, research data includes mission-critical information (Level 1) and requires consistency in the handling and maintenance of the data. Mission-critical information includes all research data necessary to substantiate research results or to satisfy grant funding requirements, regardless of whether such data was developed by the U~~u~~niversity of Houston or obtained from third parties. All research projects involve some level of data management; the outcome of the research depends in part on how well this data is managed. Data sharing is at times required by, or at a minimum, encouraged by, governmental and other funding agencies to reinforce open scientific inquiry, encourage diversity of analysis and opinion, and to permit the creation of new data sets when data from multiple sources are combined.

The purpose of this policy is to:

- Ensure consistency in the appropriate handling, storage, and dissemination of research data; and
- Protect the U~~u~~niversity and research teams by meeting the requirements of funding agencies; and
- Provide adequate oversight by the Division of Research to monitor the protection of research data and investigate related concerns.

II. DEFINITIONS

Research Data: Recorded factual material commonly accepted in the scientific or scholarly community as necessary to validate research findings, excluding preliminary analyses, drafts of scholarly or scientific work, plans for future research, peer reviews, communications with colleagues and physical objects (e.g., laboratory samples).

III. POLICY

A. Data Management Roles and Responsibilities

1. University of Houston (UH): the primary owner of data generated by awards, gifts, or contracts/subcontracts to faculty and staff, as well as intellectual property (IP) generated at UH, whether or not the research is externally funded.

   NOTE: This may also apply to students who generate data as part of their employment by UH and/or whose data collection is supported by an external award. Data related to human subjects research must be retained by UH in accordance with federal and IRB requirements.

The University also has the right to refuse data coming into the institution, or leaving the institution, on a project-by-project basis.

2. Principal Investigator (PI): The primary steward of the data.

   The PI is responsible for:

   - Identifying an individual as information custodian as defined in SAM 07.A.08, Data Classification and Protection to provide operational support during the project;
   - Identifying the individual from the college/division/U~~u~~niversity serving as the Information Security Officer for the research project with responsibilities for data protection and compliance;
   - Developing a written data management plan that adheres to U~~u~~niversity requirements and any applicable contracts. For example, in the case of funded research, the plan should include procedures for retaining and sharing data according to sponsor requirements;
   - Reviewing the data management plan at least annually to ensure it remains current;
   - Enacting processes necessary to confirm compliance with the plan, including data security per sponsor and regulatory requirements;
   - Working closely with the College, the Division of Research, and collaborating institutions upon leaving UH to ensure the appropriate transfer and ownership of data and IP; and
   - Producing the plan and associated documentation upon request by the UH Division of Research and/or applicable funding agencies.

3. Colleges/Departments/Centers

   The College/Department/Center is responsible for:

   - Providing the necessary resources for data management, addressing related information security issues and ensuring investigator compliance with data management requirements and U~~u~~niversity policy, such as SAM 07.A.08, Data Classification and Protection and MAPP 10.03.06, College/Division Responsibilities for Information Technology Resources;
   - Working with the PI upon their~~his/her~~ leaving UH to ensure appropriate transfer and ownership of research data.

4. Division of Research (DOR)

   DOR is responsible for:

   - The development of a campus-wide policy for data management and review of compliance concerns related to data management, particularly with regard to compliance with federal grant requirements for sponsored project agreements, and data use agreements relating to data received from third parties;

- Maintaining the right to refuse an award if the University is unable to meet data requirements;
- Sequestering/taking custody of data as necessary for investigations of noncompliance and/or research misconduct;
- Upon request, working with the College upon a PI leaving UH to ensure appropriate transfer and ownership of research data.

5. University Information Technology (UIT)

UIT is responsible for:

- The oversight of enterprise level software and systems related to data management;
- Providing guidance and assisting faculty and staff with completion of a data management plan and grant required documentation related to security requirements~~Ensuring that designated Information Security Officers (ISO's) are appropriately trained~~.

B. Data Management Plan

1. To ensure the appropriate identification and protection for information research, all U~~u~~niversity research projects should have~~require~~ a formalized, written data management plan, regardless of whether the sponsor requires such a plan.

a. The PI should determine if the funding agency for a particular research project has specific requirements for a data management plan, and ensure a plan meeting those requirements is submitted to the funding agency as applicable.

b. If there are no formal requirements, a data management plan including, at a minimum, the following information must be documented and shared with all key personnel involved with the project:

- Type of data being collected and stored (e.g., medical, financial, educational). This should include designation of any data with specific compliance requirements, such as Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA), Federal Information Security Management Act (FISMA), or any project requiring compliance with National Institute of Standards and Technology (NIST) standards;
- Description of the appropriate platform for data storage, including security components;
- Responsibility for the data from an ownership perspective;
- Responsibility for the data from an IT support perspective;
- Responsibility for the data from an information security perspective, including the identification of the ISO for the College/Center;

- Location where the data will be stored (e.g., standalone computer, department share). All data should be stored in accordance with SAM 07.A.08;
- How and by whom logical access to the data will be controlled;
- How physical access to the system containing the data will be controlled;
- Type of anti-virus controls the system containing the data will have;
- Process for digital data backups for recovery purposes, including the media that will be used for backups, how often the backups will occur and how often backups will be restored for testing; and
- Process for securely storing non-digital data (e.g. lab books, consent/data collection forms).

C. Data Storage and Archiving

1. Data must be archived in a controlled, secure environment in a way that safeguards the data (primary, secondary and metadata), observations, or recordings in accordance with SAM 07.A.08.

2. The archive must be accessible by scholars analyzing the data, and available to collaborators or others who have rights of access as allowed or required by the sponsor.

3. Research data must~~should~~ be stored securely for sufficient time following publication, analysis, or termination of the project. Research data includes not only the primary information produced through the conduct of the research, but also the corresponding metadata. Research data must be retained in accordance with all applicable sponsor and federal regulatory data retention requirements and profession-specific ethical guidelines/timelines.

4. If sponsor requirements indicate that data must be destroyed at a given time ~~point~~, the PI is responsible for ensuring destruction per these requirements and notifying DOR in writing once completed.

D. Data Sharing

1. Investigators are expected to share with other researchers data created or gathered in the course of funded research within a reasonable time frame. These requirements may vary, based on funding agency, but in general require that research data be made available to the scientific community for subsequent analysis. In most cases, the PI has the right to first analysis, unless other requirements are in place to warrant immediate release. It is the PI's responsibility to ensure that data sharing plans are developed and provided to the granting agency as required, and to ensure that the plan is executed.

2. Methods of sharing data may include, but are not limited to, publications, placing data in public archives, and sharing directly with other researchers.

3. PI's are responsible for working with the University Office of Tech Transfer and Innovation (OTTI) to ensure that the intellectual property of the University is protected throughout any data sharing arrangement.

4. Any data shared must meet all requirements for compliance including privacy and data protection. It is the PI's responsibility to ensure that all compliance requirements for the data are properly identified and satisfied through any data sharing arrangement. This includes requirements identified through IRB and other compliance processes.

IV. REVIEW AND RESPONSIBILITIES:

Responsible Party: Executive Director, Office of Research Integrity and Oversight

Review: Every five years ~~on or before September 1~~

VI. APPROVAL

~~*/Amr Elnashai/*~~
~~Vice Chancellor/~~Vice President for Research ~~and Technology Transfer~~

~~*/Renu Khator/*~~
President

Date of President's Approval: ~~May 15, 2019~~