SOP for Managing Data Retention Requirements in Core Facilities

The **Vanderbilt University Medical Center Policy on Sharing, Retention and Ownership of Research Data** details the institutional and investigator responsibilities related to ownership, sharing and storage of primary research data, regardless of the technology used to create, preserve or record it. **The Principal Investigator (PI) has primary responsibility for archiving and maintaining data as required by the Policy.**

The purpose of this **SOP for Managing Data Retention Requirements in Core Facilities** is to ensure consistent best practices for Cores, which may provide data management and storage services to PIs. Cores are not required to provide data management and storage services, and PIs may also "opt-out" of such services that are provided by a Core facility. In these cases, the PI should take possession, or provide instructions for transfer, of data at the end of the minimum operational data retention period (see item 1, below).

Note: Unless otherwise qualified, the term data refers to original, primary research data as defined in the institutional Policy on Ownership of Research Data.

1. Each Core should define what constitutes original, primary research data and additional valuable derivatives that may be stored by the Core, as appropriate to its technology platforms, applicable regulatory requirements and in consultation with institutional advisory structures (for example ISROC, faculty advisory committees, or other etc.). This definition may vary by Core and by service type.

2. Cores should establish and consistently adhere to a minimum operational data retention period. This is defined as the timeframe immediately following collection of data necessary for processing and releasing results to the PI. This minimum period may vary by Core and by service type.

3. Cores should create a written **Data Management SOP**, which should be readily available to PIs by website or other means, especially at the initiation of a project. The Core SOP should include as applicable:
   a. The Core-specific minimum data storage period, including schedule or timetable.
   b. Other data storage options provided by the Core.
   c. Cost of storage options.
   d. Any restrictions on types of data that can be stored by the Core (e.g. personal protected information; encryption; formats).
   e. Information about alternative storage options if available, e.g. public repositories – these may vary by Core and by service type.
   f. Additional considerations may include export compliance, confidentiality or non-disclosure agreements, patent protection and IP standards as applicable to Core and/or service type.

   Note: *Each Core's Data Management SOP should be reviewed and approved by the Office of Research. It is expected that each SOP will apply to any ad hoc or "legacy" data storage going forward.*

4. Cores may opt to offer data storage and management services for all, part or none of the required data retention time frame – provided this is clear to the PI at the initiation of work. Cores may contract with internally or externally managed data storage services, or may provide other appropriately managed environments for storage.

5. If Cores offer data storage and management services the following guidelines apply:
   a. Cores should establish the minimum operational data retention, which by definition ends at the point when data are finally transferred to the PI or other storage facility as directed by the PI.
   b. Cores should use best practices to ensure that data is managed in an appropriate, safe and accessible environment. Criteria for data safety include (1) regularly verifying data integrity and (2) avoiding single points of failure (e.g., storage device, computer, or server room).
   c. The costs associated with data storage services may be charged back to the PI. Costs for commonly used storage solutions such as the central storage repository (e.g. cost per terabyte in BlueArc) should be consistent across all Cores. As for all other Core services fees, data storage fees are subject to review and approval by the Office of Research.
   d. Cores should establish a notification process that includes a brief reminder to investigator of his/her responsibilities (reference Policy).
   e. Cores should send timely reminders to PIs regarding deadlines for discarding data. Before any data is destroyed, the Core should document the PI's acknowledgement of the planned data destruction. If the PI is not available (e.g., is not responsive or has left Vanderbilt), the Core should work with the Office of Research to contact the PI's department chair for guidance before any action is taken.
   f. Cores should maintain a log to document all communications and actions related to data storage, including:
      - PI request for data storage services
      - PI "opt-out" from Core-based data storage services
      - PI or departmental requests to destroy data
      - Actions taken by Core

For additional guidance, contact Susan Meyn in the Office of Research: s.meyn@vumc.org

Reference:

Vanderbilt University Medical Center Policy on Sharing, Retention and Ownership of Research Data