**MGM Investigator Offboarding Expectations and Checklist**

It is crucial for research institutions such as Duke to have the ability to locate data upon request. Too often, when an investigator leaves Duke, there is not a clear list of expectations conveyed at offboarding for documenting the disposition, location of and access to research data, including transfer of data access to the university. Without this information, other investigators, including collaborators, may not be able to easily locate data when needed to continue current research projects or support inquiries into historic data. This checklist/process should gather information for projects with data used in some way in the last **6 years**(per the Duke policy for retention).

**Off-boarding Checklist**

If you are Duke University personnel (faculty, staff); have engaged in research; and are planning to leave or disengage with Duke, ensure that the items in this checklist are complete. Keep in mind the time commitment to appropriately prepare data for your departure. Some items may not be applicable. If you have questions, contact myresearchnavigators@duke.edu.

*Note: The original versions of data sets that lead to disseminable research must remain at Duke. The personnel leaving may request copies of the data to take with them as permitted by regulatory or contractual obligations associated with the data.*

1. **Create or update a knowledge transfer file (i.e.,** [**README**](https://data.research.cornell.edu/content/readme)**) for project(s) to ensure long-term accessibility and facilitate reuse of your data and methods.** Verify that the items below are included in the knowledge transfer file as applicable.

[ ]  Contact information for original person or personnel related to the project, datasets, and methods

[ ]  Metadata including file naming conventions, formats, software tools employed, permissions, and versioning

[ ]  Location of data files

[ ]  Location of documentation associated with the research data, including relevant agreements

[ ]  If applicable, how the data relates to associated funding sources (including grant # and fund codes) and manuscripts

[ ]  Ensure that this Knowledge Transfer file is shared with the new data steward at Duke, and with appropriate personnel within your organization unit or, (if applicable) research team

1. **Identify a steward for the data.** It is important to ensure that prior to you leaving Duke, a responsible steward is selected to ensure proper data upkeep. The data steward can be a new Duke PI, the department chair, or research leadership within your organizational unit. Please ensure the following items are completed as part of selecting that person/entity.

[ ]  Obtain written approval from department chair or research leadership to transfer data to another PI or the department/organizational unit

[ ]  Provide documentation of transfer of stewardship to the department chair or research leadership of your organizational unit. For clinical research projects, it must be stored with the regulatory file.

[ ]  Ensure that the new data steward is given access to the original, or a copy of, all relevant storage resources used for your data. Move data from any personal storage spaces (personal hard drives, personal Box folder, etc.) as the steward would not have access to this once you leave.

[ ]  For studies that will remain at Duke, ensure the new data steward will maintain continued project access to collaborators as appropriate or per relevant agreements

1. **Ensure compliance with data retention or deletion requirements.** The new data steward will need to be aware of any contractual or regulatory requirements associated with the data. As applicable, use the following items to guide your actions.

[ ]  Ensure data steward is aware of any regulatory requirements or policies around the data. For studies involving IACUC/OAWA, review and follow their relevant [policies](https://myresearchpath.duke.edu/topics/animal-welfare-iacucoawa) and notify them if there is a change in PI. For human subjects research, review and follow the [DUHS](https://irb.duhs.duke.edu/policies-and-regulations) or [Campus](https://campusirb.duke.edu/irb-policies) IRB policies as appropriate. For clinical research studies operating within a Clinical Research Unit, engage your Research Practice Manager in the process. Ensure data steward is aware of any regulatory requirements or policies around the data.

[ ]  For studies with contractual agreements, review and follow required retention and deletion agreements. If contracts need to be updated to the new data steward, work with your contracting office (ORS/ORC) to ensure proper updates to the contract are done prior to leaving.

1. **Review storage of and organize data.** Use of proper data storage will ensure that data are properly secured and can be efficiently accessed by future users

[ ]  Review [existing policies and guidance](https://myresearchpath.duke.edu/topics/archive-data-and-documents#pg-f3bc4c4d-9efd-47ec-ab15-0cd3553bd6c0) associated with data storage and ensure that your projects are appropriately stored with the new Duke steward.

[ ]  Ensure that data are organized in meaningful ways, and document this in the Knowledge Transfer File

[ ]  For studies active with the DUHS IRB, update the Research Data Storage Plan (RDSP) for review by the CRU.

[ ]  If applicable, ensure that field or laboratory notebooks are stored in alignment with internal procedures or data management plan and if applicable, the Scholarly/Science Culture and Accountability Plan of your organizational unit. Be sure to review notebook for any restricted or sensitive data (ex. 3rd party data or PHI/PII).

1. **Transfer permissions if you intend ongoing use of data:** If you plan to transfer or take a copy of the data to another institution, take the following steps:

[ ]  If your data was: 1) collected from research that was externally sponsored, 2) classified as sensitive or you are not sure of your data classification, work with the research contracting office (ORS/ORC) to put a Data Use or Data Transfer Agreement in place.

[ ]  Ensure that regulatory documentation (e.g., IRB protocols, Data Management Plans, Data Protection Plans) appropriately update your new affiliations and document the Duke data steward’s involvement as appropriate

[ ]  If you are transferring public, sensitive, restricted, protected or controlled information (such as PHI), contact your future institution for information about their procedures

[ ]  If available, use local IT support to help assist with the technical aspects of the data transfer. If not available or for more complicated technical support with data transfer, reach out to OIT or DHTS as appropriate.

1. **Identify and prepare data for deposit or long-term storage.** Ensuring proper preparation of the data prior to leaving will increase the chances that long-term storage services like repositories will be able to accept your data and curate it for the long term

[ ]  Contact your Department/Center/Institute/CRU for local guidance and/or reach out to Information Technology Security Office (DHTS or OIT), as well as the Duke Libraries to determine appropriate locations for deposit or long-term storage of your data

* OIT IT security
* DHTS Storage team is accessed in Service Now
* Duke libraries

[ ]  Ensure that appropriate and allowable backups are prepared and stored

[ ]  If applicable, ensure that any associated costs are understood and accounted for by the new data steward

[ ]  Document long-term storage or deposit information in the Knowledge Transfer File

[ ]  Review policies and guidance associated with data sharing and [Intellectual Property](https://policies.duke.edu/intellectual-property)

[ ]  If applicable, identify publisher requirements for data sharing

[ ]  If applicable, review funder requirements for data sharing

[ ]  Review relevant regulatory or contractual documentation (e.g., Consent forms, DUAs, etc.) to ensure adherence to any obligations

[ ]  Review any project Data Management Plan to ensure follow-through with planned data sharing activities