Guidance on Data Use Agreements involving University of Miami investigators

Why share data?

Data sharing can speed translation of research results into meaningful knowledge and products. It increases the ability of researchers and other stakeholders to collaborate and discourages duplication of effort in data collection. Further, researchers can use data collected by others to answer questions not considered by the initial investigators. Sharing data also encourages accountability and transparency, enabling researchers to validate one another’s findings. Finally, data from multiple sources can often be combined to allow for comparisons that cross disciplines as well as geographic boundaries.

The National Institutes of Health (NIH) published its Final NIH Statement on Sharing Research Data in the NIH Guide on February 26, 2003. This statement extends NIH policy on sharing research resources, and reaffirms NIH support for the concept of data sharing.

What is a Data Use Agreement and why is it necessary?

An agreement to share data (often called a Data Use Agreement, or DUA) is a formal contract that clearly sets out what data are being shared and how the data can be used. DUAs serve two purposes. First, they protect the agency or institution providing the data by ensuring that the data will not be misused. Second, they minimize miscommunications by ensuring that questions about data use and protection are discussed before data are shared. Optimally the provider and receiver of the data should discuss data sharing and data use issues and come to a mutual understanding that is then documented in the DUA. It is important to recognize that the processes for setting up DUAs vary with respect to the type of data that are being shared as well as the countries and agencies or institutions involved.

What should be addressed in a DUA?

Below is a list of items/topics that are usually found in a DUA. This list is intended to cover basic components commonly found in DUAs. Additional concerns may be relevant to specific data sets, countries, agencies or institutions:

**Period of agreement**

Define when the provider will give the data to the received and how long the receiver will be able to use the data.

Once the receiver no longer has the right to use the data, define what happens next. Are the data returned? Destroyed (deleted from drives, servers, shredded, etc.)?
Intended use

Clearly state how the receiver will use the data. Include specifics such as what studies will be performed, what questions will be asked and what the expected outcomes are.

Be sure to define whether the receiver can use the data to explore additional research questions without the consent or approval of the provider.

Restrictions or constraints on use of the data

Any restrictions or limitations on how the data, analysis or data findings can be used should be clearly articulated.

Items to consider include: is the receiver required to document how the data are used? Can the receiver share, publish or disseminate data findings, analyses, or reports without the approval or pre-review of the provider? If the receiver generates a report or analysis of the data, who “owns” that report or analysis? This issue is important to consider if there is any chance that intellectual property may be generated using the data. Can the receiver share, sell, or distribute data findings, analyses or any part of the data set to another agency or institution?

Data Confidentiality

The agreement should describe how the receiver will ensure confidentiality of the data. Because some data may contain information that can be linked to individuals, it is important to put safeguards in place to ensure that sensitive information (e.g., exam results, protected health information) remain private. Personal data should remain confidential and should not be disclosed verbally or in writing to an unauthorized third party, by accident or otherwise. In general, only the minimum necessary data elements needed for the intended use should be shared.

Questions related to Protected Health Information (PHI) should be directed to the Office of HIPAA Privacy and Security (http://privacyoffice.med.miami.edu/).

Questions related to student data should be directed to the Student Consumer Information office (http://www.miami.edu/index.php/about_us/hea_student_consumer_information/).

Items to consider include: will the receiver report information that identifies individuals? What safeguards are in place to prevent sensitive information from becoming public?

Data Security

The methods that the receiver must use to maintain data security should be clearly described. Hard copies of data should be kept in secure areas and electronic copies should be password protected or kept in a secure format (encrypted device, etc.).

Questions related to and best practices for information security should be directed to Information Technology (IT) Security (http://www.miami.edu/index.php/information_technology_security).
Items to consider include: Will there be a plan for role-based access? If not, who at the receiver agency will have access to the data? What kind of passwords or encryption will be put in place? Who will have access to physical data, including servers and paper files? What will happen when the data-sharing period ends? What are the standards for data archiving? Destruction?

Methods of data sharing

The manner in which the data will be transferred should be clearly described.

Items to consider include: How will the data be transferred – physically, electronically, both? If the data are to be sent electronically, how will the secure connection be guaranteed? What type of encryption is required? When will the data be encrypted? Who is responsible for assuring that encryption occurred?

Financial costs of data sharing

It is important to consider and clearly state what the costs are related to sharing of the data as well as who will be responsible for covering the costs.

Items to consider include: Are there expenses related to sharing the data? Will the provider or receiver share the costs or will one agency be responsible for all the data-sharing expenses?

Data sharing templates from federal agencies

Agencies such as the NCBI have large data sets to be shared with investigators (e.g., the Database of Genotypes and Phenotypes, or dbGaP). In this case the data sharing agreement is a pre-determined template that constitutes an online application. Access to the dbGaP is requested by investigators but must be certified by the UM administration. Contact the Office of Research Administration (Stewart MacIntyre) for further information.

Who at UM can help me with a DUA?

- The Vice Provost for Research signs DUAs on behalf of the University. Contact the Office of the Vice Provost for Research for general information on data sharing in research.
- Special precautions must be in place and approved for DUAs involving PHI. The Human Subjects Research Office maintains a template DUA that serves as a starting point for DUAs that involve PHI. This template DUA is available at: (http://hsro.med.miami.edu/documents/UM_Template_Data_Use_Agreement_for_Disclosure_of_a_LDS_for_Research_%2812-2-13%29.pdf). See also the HIPAA/Privacy Office, above.
- The Office of IT Security has information concerning the secure handling of data. Contact Tim Ramsay, Associate Vice President and Chief Information Security Officer if you have questions.

(Portions adapted from the University of Chicago http://researchadmin.uchicago.edu/clinical_trials/DSA.shtml)