DATA SHARING AND TRANSFER GUIDANCE

TOPICS COVERED BY THIS GUIDANCE

PURPOSE

This guidance outlines procedures for sharing both outgoing and incoming data at WashU, including the use of Data Transfer and Use Agreements (DTUAs).

“Outgoing data” refers to an investigator sharing locally-created data with an outside party. "Incoming data” refers to an investigator receiving data from an outside party. Both directions of sharing will typically involve use of a DTUA.

WHAT IS A DATA TRANSFER AND USE AGREEMENT?

A DTUA is a formal contract that defines the unique data set being shared and governs how the data can be used. They may be referred to as Data Use Agreements, Data License Agreements, Access Agreements, or other similar terms. All will generally define the terms and conditions of the transfer, such as limitations on use of the data, obligations to safeguard the data, time period for use, liability for harm arising from the use of the data, publication, and privacy rights. A DTUA protects the party providing the data by ensuring the data will not be misused. It also prevents misunderstandings between the provider and recipient of the data regarding permitted uses, such as the ability to further share the data or use the data for a commercial purpose.

There are also other types of agreements may cover the necessary provisions for data sharing. For example, a clinical trial agreement with an outside entity will establish the terms and conditions for conducting the clinical trial as well as the terms and conditions for sharing the trial data. The specific type of agreement needed varies based on several factors: the relationship of the parties, the goals of the transaction, and the nature of the data. (See also, Special Considerations for Human Subjects Research Data for discussion on specific types of agreements relevant for sharing human subjects data.)

PROCESS

The Joint Research Office for Contracts (JROC) is responsible for drafting, negotiating, and signing DTUAs. For incoming data (other than data being submitted to a registry ran by WashU), the party that is sending the data to WashU will usually provide a draft agreement, which you should submit to JROC for review. For outgoing data, where WashU is the data provider, we would generally use the WashU template agreement for transferring data to an outside party. Submit requests for a DTUA to researchcontracts@wusm.wustl.edu. Also, include a DTUA intake form to facilitate the development of an appropriate DTUA by JROC.

WHEN IS A DATA TRANSFER AND USE AGREEMENT REQUIRED?

In general, DTUAs are used for the transfer of data that are not public or that cannot be made publicly available without restriction. For example, a DTUA is required to transfer the following types of data:

- Individual identifiable health information or protected health information (PHI) as defined by HIPAA
- De-identified health information as defined by HIPAA
- Data on individuals originating in the European Union or the United Kingdom that is subject to the General Data Protection Regulation (GDPR)
- Student information derived from education records that are subject to Family Educational Rights and Privacy Act (FERPA)
- Export controlled data or Controlled Unclassified Information
- Data controlled by laws or regulations other than those listed above
- Data obtained from another organization or individual under obligations of confidentiality or restricted use
- Data collected at WashU that is subject to contractual confidentiality obligations
- Individual level data proposed to be shared under the scope of WashU's Policy Governing Disclosure of Human Data to Third Parties for Product Development
- Data proposed to be transferred in association with an investigator leaving WashU in compliance with WashU's Research Data & Materials Policy
- Data that is considered confidential or protected under WashU's Information Classification Policy

Per the Research Data & Materials Policy, research data are owned by Washington University. WashU must ensure that data are shared in ways consistent with the best interests of the organization and in compliance with regulatory obligations, funding agency or other sponsor requirements.

Only authorized signatories (e.g., authorized individuals in JROC) have the authority to sign DTUAs on behalf of WashU. Individual faculty are not authorized to sign DTUAs.

DOES HIPAA APPLY TO THE DATA?

It is important to determine if HIPAA applies to the data you are proposing to share. HIPAA applies to data that includes individually identifiable health information. When HIPAA applies, it is also important to determine if the data is considered de-identified, a limited data set (LDS), or protected health information (PHI) exceeding a LDS.

- Deidentified Data: data is considered deidentified if the information does not identify an individual and there is no reasonable basis to believe it can be used to identify an individual. HIPAA allows information to be deidentified through the "Safe Harbor" method or the "Expert Determination" method. Data may be deemed deidentified under the Safe Harbor method by removing all 18 identifiers under HIPAA (e.g., all elements of dates (except year) related to an individual, including date of birth, admission date, discharge date, date of death, etc.).
- Limited Data Set: A limited data set (LDS) may include certain "limited identifiers" such as dates and geographic information at the level of town or city, state, and zip code. Under HIPAA, a "Data Use Agreement" is recognized as a particular type of agreement required by HIPAA prior to disclosing a LDS for research. It is important to understand that a LDS is a subset of Protected Health Information. It is not considered deidentified.
- PHI exceeding a LDS: If the data includes identifiers in excess of those allowed in a LDS, it is considered PHI exceeding a LDS. This may be disclosed for research purposes with an individual's authorization or pursuant to a waiver of HIPAA authorization.

Contact the Privacy Office or HRPO for questions involving PHI.

The DTUA (or other appropriate agreement addressing data sharing) must be executed prior to transfer of any data set subject to HIPAA or any individual level human data.

HOW DO I KNOW IF I CAN SHARE DATA COLLECTED AS PART OF HUMAN SUBJECTS RESEARCH AND/OR DATA SUBJECT TO HIPAA?

Requirements for HIPAA data: Described below are different HIPAA pathways for sharing protected health information. Such data sharing should occur in conjunction with an appropriate agreement:

- Signed informed consent forms along with a HIPAA-compliant authorization approved by the IRB
- Waivers of informed consent and waivers of HIPAA authorization in conjunction with IRB oversight for the data recipient
- Data-sharing agreements

- Data Use Agreements – used for sharing a Limited Data Set for research purposes
- Business Associate Agreements – used for sharing PHI with a Business Associate in conjunction with a service agreement

Requirements for all data collected as part of human subjects research (whether deidentified or PHI): In order to share human subjects research data, the IRB-approved application/protocol and corresponding consent and/or authorization form (or waivers thereof), must allow for the sharing of the data. The intended sharing must align with the description of how data will be shared in the protocol, the consent form, and/or the HIPAA authorization form (such authorization may already be included within the research informed consent). If the data is housed in a repository or collected under a banking protocol, it is important to review all consents applicable to that data. For example, if the data was collected from a subject in 2012, the consent form used with that subject in 2012 must be reviewed before sharing the data collected under the 2012 consent. If you are uncertain whether the intended sharing is permitted, please consult with HRPO. For sharing of identifiable data (more than a LDS) that was collected under a consent to any external party, HRPO will review and approve to ensure consistency with the consent.

When drafting research materials, e.g., protocols, consent forms and data sharing plans, it is important to consider future uses of data and to draft them with sharing in mind and with language that allows for flexibility. The HRPO template informed consent form includes data sharing consent language.

ARE THERE CONTRACTUAL RESTRICTIONS ON SHARING THE DATA?

If the data you are proposing to share originated outside of WashU or in connection with sponsored research, including clinical trials, there may be contractual limitations on your ability to share that data. For example, data collected under an industry sponsored clinical trial likely includes contractual restrictions on further sharing or use. It is important to review any contracts covering the acquisition of the data to determine if further sharing is permitted. JROC will assist you with this review at the time a DTUA is requested.

If data sharing is not permitted under the applicable contracts, you will need to seek written approval from the other party to the contract.

SPECIAL WASHU CONSIDERATIONS FOR SHARING HUMAN DATA

Sharing human data for commercial product development:

Any individual level human data being shared with a for-profit entity for purposes of commercial product development is required to be reviewed by the Human Data Review Committee (HDRC) in accordance with WashU's Policy Governing Disclosure of Human Data to Third Parties for Product Development. (email: hdrc@wustl.edu)

Direct access to the electronic medical records: Some organizations may propose a method of accessing WashU clinical data through a direct link to Epic, WashU's electronic medical records (EMR), as a more efficient mechanism for accessing and extracting clinical data. Any direct access to the EMR requires review by WashU leadership, including approval from the WashU/BJC Epic1 Research Steering

Committee, the HIPAA Privacy Officer, the Chief Research Information Officer (CRIO), the Chief Clinical Informatics Officer, and potentially from the Human Data Review Committee (HDRC) per the Policy Governing Disclosure of Human Data to Third Parties for Product Development.

Special Considerations When WashU is Receiving Data from Multiple Parties and/or Hosting a Database/Registry

When working with multiple entities in a collaborative nature (e.g., multisite study, consortium, network), the PI should work closely with JROC to establish the appropriate data sharing agreement structure. In some cases, JROC may recommend that data sharing be addressed in the underlying collaboration agreement, if possible, rather than through separate data sharing agreements. The types of things addressed in these agreements may include:

- Conditions regarding the transfer of the incoming data to WashU
- Governance associated with future use of the data, including joint decision-making regarding access, secondary use, publication policies, etc.
- Conditions regarding the transfer of data out of the registry to the registry participants or other entities
- Security measures that apply to the management of the data

For registries where WashU is hosting data from other institutions, researchers should consult with Information Security Office to ensure the hosted registry meets appropriate security protocols.

What needs to be in a Data Transfer and Use Agreement?

The amount of detail required in a DTUA should be commensurate with the nature of the data to be shared, the likelihood of a privacy breach, and the possible magnitude of harm which may occur to the institution or to participants if their privacy rights were violated.

Below are topics typically included in DTUAs:

- Intended use of the data: there should be a clear and specific description as to how the data will be used.
- Restrictions on use and retransfer of the data: restrictions on how the data can be used should be described. Can the recipient share or disseminate the data set and, if so, with whom and for what purpose? Who can access the data at the recipient institution?
- Data security & transfer method: describe any methods the recipient should use to maintain data security (e.g., password protections, locked cabinets for hard copies, etc.). Describe how the data will be transferred to the recipient (e.g., via shared Box folder, encrypted transfer, etc.).
- Financial costs: if there are expenses related to sharing the data, clarify who will cover the costs.
- Disposition of data: include special disposition instructions once the reason for sharing has ended (e.g., return or destroy).
- Liability: allocation of responsibility in the event of breach or unauthorized disclosures

- Compliance: assurances regarding compliance with laws applicable to the data or other regulatory obligations

PROCEDURES FOR ACCESSING OR SUBMITTING DATA TO/FROM A GOVERNMENT REPOSITORY

Many federal agencies that host data repositories often require a data access or data submission agreement or other certifications regarding the data.

- NIH has established certain NIH-designated data repositories, such as the Database of Genotypes and Phenotypes (dbGaP), for securely storing and sharing controlled-access human research data submitted to NIH under the NIH Genomic Data Sharing Policy. In these instances, the institution must certify that the data submitted to the repository was collected under the appropriate approvals and informed consent was obtained. This certification process is managed by HRPO. The Office of Sponsored Research Services (OSRS) is the authorized signing official for dbGaP requests.
- For other access or submissions agreements with government repositories (other than dbGaP), JROC will review and consult with HRPO, as needed.
- Most federal agencies also support deposit into an institutionally run repository that follows the guidelines described in the Desirable Characteristics of Data Repositories for Federally Funded Research report. WashU provides an institutional data repository. Resources and support are provided by Becker Library and University Libraries.

EXTERNALLY HOSTED DATA ACCESSED ELECTRONICALLY

In some cases, data may be accessed through acceptance of an electronic DUA, frequently appearing as terms and conditions displayed on the researcher's computer screen for the researcher to click "I accept" (or similar) button. A WashU PI may electronically accept terms and conditions associated with access to externally hosted data. JROC does not need to review the terms and conditions associated with electronic access to data. If you are uncertain whether you should accept the terms and conditions, you may contact JROC for review and advice. If there is a separate, standalone DUA requiring authorized institutional signature associated with access to the data, the standalone DUA must be sent to JROC for review and signature.

Any individual who electronically accepts terms and conditions is responsible for reading the terms and conditions, saving them electronically, and distributing them to every individual who will have access to the data. Any individual who has access to the externally hosted data is bound by the accepted terms and conditions.

DATA-SHARING PLANS

Many sponsors, including most federal agencies, require data sharing plans to be included in proposals. Development of an appropriate data-sharing plan is the responsibility of the PI. When developing your

data-sharing plan, it is important to ensure that the plan aligns with the study protocol, applicable informed consent forms, contractual responsibilities associated with the project or data, regulatory requirements, and anticipated future use of the data. Resources and support for development of a data-sharing plan are provided by Becker Library and University Library.

Related Offices, Policies, and Helpful Contacts

- Joint Research Office for Contracts
- Human Research Protection Office
- HIPAA Privacy Office
- Office of Sponsored Research Services
- Resources and tools regarding research data on the OVCR website
- Data Services in University Library and Becker Library can support researchers in data management, including the development of data sharing plans.
- Secure storage and communication services from the Office of Information Security
- Research Infrastructure Services
- Research Data & Materials Policy
- Policy Governing Disclosure of Human Data to Third Parties for Product Development