

DATA USE AGREEMENTS

DEFINITIONS

- Data- As used in relation to research agreements, Data may include confidential, protected, research project results, or restricted use information. Examples include records from governmental agencies or corporations, student records information, and human research subjects' data including PHI (Protected Health Information) and PII (Personally Identifiable Information)

DEFINITIONS

PHI stands for Protected Health Information. It refers to any individually identifiable health information that is created, received, maintained, or transmitted by a "covered entity" under the Health Insurance Portability and Accountability Act (HIPAA).

DEFINITIONS

PHI includes:

Medical records

Health insurance information

Demographic data (e.g., name, address, birth date)

Genetic information

Payment information related to healthcare

HIPAA protects PHI by establishing standards for its use and disclosure. It ensures that individuals have control over their medical information and that it is handled confidentially.

DEFINITIONS

PII, or Personally Identifiable Information, is any data that can be used to identify a specific individual, either on its own or when combined with other information. Examples of PII include names, addresses, Social Security numbers, driver's license numbers, and biometric data like fingerprints or facial images. This information must be protected to prevent harm, embarrassment, or unfairness to individuals.

DEFINITIONS

What Constitutes PII

Direct Identifiers:

Information that directly identifies an individual, such as a full name, Social Security number, or passport number.

Indirect or Quasi-Identifiers:

Information that, on its own, might not identify someone but can be linked with other data to trace an individual's identity. Examples include:

Date of birth

Place of birth

Race

Geographic indicators

Employment information

PURPOSE OF AGREEMENTS

There are two primary reasons for utilizing a Data Use/Transfer Agreement

- **Data Use** – Creating an agreement between “Data User” (person or organization utilizing data) and the “Data Owner/Provider (the person or organization providing the data) that will include the provisions associated with the sharing of defined Data.
- **Data Transfer** – Creating an agreement to transfer data from “Data Owner” (person/organization that owns data) to another organization. The data is transferred in its entirety, including ownership, to the Data User as opposed to the allowance of access to the data set.
- **Data Purchases** – please note that there are instances where data and data use may be purchased under a data purchase agreement. In these cases, the agreement may require review as a procurement.

PURPOSE OF AGREEMENTS

- DTUAs address important issues such as limitations on use of the data, liability for harm arising from the use of the data, publication, and privacy rights that are associated with transfers of confidential or protected data. The DTUA also assures that Data Users are using the data in accordance with applicable law (e.g. [HIPAA](#), [FERPA](#)) and prevents the inappropriate use of protected or confidential data that could cause harm to the investigator, the University, or individuals whose data is part of the data set.
- When is a DTUA required – A Data Use Agreement is required when any data is exchanged which is not de-identified. This may include Protected Health Information or Personally Identifiable Information.

INFORMATION REQUESTED FOR AND INCLUDED IN DATA TRANSFER OR USE AGREEMENTS:

- What data will be released or shared
- Who has ownership of the data
- What, if any, identifiers will be included
- The purposes for which the data may be used
- With whom, if anyone, the data may be shared
- Data security and safeguards
- To whom violations of the agreement should be reported
- The term of the agreement
- The disposition of the data at the end of the agreement

COMPLIANCE OFFICE ENGAGEMENT

- **Institutional Review Board** – engaged when the data includes human subjects' data.
- **Privacy** – engaged when the data includes restricted data, such as Protected Health Information (PHI) and some Personally Identifiable Information (PII).
- **Information Technology (IT)** – IT may be asked for review and provide assistance when certain software, hardware, encryption, dissemination, or storage requirements are identified in the agreement.

FEDERAL DEMONSTRATION PARTNERSHIP

TAMU utilizes the FDP (Federal Demonstration Partnership) Data Transfer and Use Agreement for sending data to outside organizations. The FDP Template can be used for different types of data transfer. Once you select the type of data to be transferred the requirements are automatically entered into the form.

Agreement ID:

FDP Data Transfer and Use Agreement (“Agreement”)	
Provider:	Recipient:
Provider Scientist	Recipient Scientist
Name:	Name:
Email:	Email:
Agreement Term	Project Title:
Start Date: Date of last signature below	
End Date: Three (3) Years after the Start Date	Attachment 2 Type: Select Data Type
Terms and Conditions 1) Provider shall provide the data set described in Attachment 1 (the “Data”) to Recipient for the research purpose set forth in Attachment 1 (the “Project”). Provider shall retain ownership of any rights it may have in the Data, and Recipient does not obtain any rights in the Data other than as set forth herein. 2) If applicable, reimbursement of any costs associated with the preparation, compilation, and transfer of the Data to the Recipient will be addressed in Attachment 1. 3) Recipient shall not use the Data except as authorized under this Agreement. The Data will be used solely to conduct the Project and solely by Recipient Scientist and Recipient’s faculty, employees, fellows, students, and agents (“Recipient Personnel”) and Collaborator Personnel (as defined in Attachment 3) that have a need to use, or provide a service in respect of, the Data in connection with the Project and whose obligations of use are consistent with the terms of this Agreement (collectively, “Authorized Persons”). 4) Except as authorized under this Agreement or otherwise required by law, Recipient agrees to retain control over the Data and shall not disclose, release, sell, rent, lease, loan, or otherwise grant access to the Data to any third party, except Authorized Persons, without the prior written consent of Provider. Recipient agrees to establish appropriate administrative, technical, and physical safeguards to prevent unauthorized use of or access to the Data and comply with any other special requirements relating to safeguarding of the Data as may be set forth in Attachment 2. 5) Recipient agrees to use the Data in compliance with all applicable laws, rules, and regulations, as well as all professional standards applicable to such research. 6) Recipient is encouraged to make publicly available the results of the Project. Before Recipient submits a paper or abstract for publication or otherwise intends to publicly disclose information about the results of the Project, the Provider will have thirty (30) days from receipt to review proposed manuscripts and ten (10) days from receipt to review proposed abstracts to ensure that the Data is appropriately protected. Provider may request in writing that the proposed publication or other disclosure be delayed for up to thirty (30) additional days as necessary to protect proprietary information.	

Data Use Agreement

Any Data Transfer/Use Agreements received by outside organizations should be reviewed and approved by Sponsored Research Services Unfunded Negotiations Team or TAMU Contract Administration if data is being purchased.

CONTACT INFORMATION

Send Data Use Agreements for review
and approval to
negotiations@tamu.edu

For any questions contact Heather
Maass
hmaass@tamu.edu