FDP DATA TRANSFER AND USE AGREEMENT (DTUA) TEMPLATE
FREQUENTLY ASKED QUESTIONS

Introduction
These FAQs, created by the DTUA Working Group under the direction of the FDP Data Stewardship and Contracts Subcommittees, pertain to the FDP Data Transfer and Use Agreement (DTUA) Template and its applicable attachments.

Categories of Questions (click hyperlink below):

Questions regarding this FAQ document can be directed to the DTUA Working Group Co-Chairs, Melissa Korf at Melissa_Korf@hms.harvard.edu or Martha Davis at mrdavis@brandeis.edu.

General Questions

1. For what data types/sharing scenarios has the template been created?

The DTUA template currently developed is intended to facilitate the transfer/sharing of research data from a provider institution to a recipient institution for use in a specific research project to be conducted at the recipient institution. The DTUA template is designed to be flexible enough for use in sharing multiple different types of data which may be subject to differing requirements under law and/or regulation. Currently, the FDP has finalized and published the following template components for sharing various types of data on the Data Stewardship and Contracts subcommittee website pages:

- DTUA Face Page with Attachments 1 and 3
- DTUA Attachment 2: De-identified Data about Human Subjects
- DTUA Attachment 2: Limited Data Set
- DTUA Attachment 2: Other (See Question 9 for more information on when use of this attachment might be appropriate)

- DTUA Attachment 2: Personally Identifiable Information – Common Rule Only
- DTUA Attachment 2: Personally Identifiable Information – HIPAA
- DTUA Attachment 2: Personally Identifiable Information - FERPA

The currently published template is not designed to accommodate a bidirectional flow of information nor to facilitate collaborative research project(s) between the Provider and Recipient; however, these use cases are scheduled for future work. The current template may be modified to reflect a bidirectional flow of information; however, if you modify the standard template language for such a use case, please remove the FDP moniker so that it is clear the FDP standard template language was altered.

The DTUA template is also not intended for use in transferring materials. The FDP DTUA Guidance Chart provides further guidance on when the DTUA template may be needed and/or when data terms may be incorporated into another agreement, such as a Material Transfer Agreement when both data and materials are being shared. Your institution may use other standard template agreements for material transfers, such as the Uniform Biological Material Transfer Agreement (UBMTA). The UBMTA could be incorporated into the DTUA by reference in Attachment 1 or as a separate attachment to the DTUA.

The FDP DTUA template is also not designed for use when sharing data from a repository or where third party rights inconsistent with the template terms are likely to attach to the data.

2. Our legal counsel would like to make changes to the FDP DTUA terms and conditions. May we do this?

The FDP DTUA terms and conditions should not be modified except in the case of the editable parameters built into the templates (i.e., the form fields in Attachment 1) when issuing DTUAs to another domestic nonprofit entity. The FDP DTUA template is a collaborative document developed by an FDP working group that included broad representation of the membership. It was distributed for review and vetting by the full membership prior to publication. This collaboration has resulted in a template that reflects a widely accepted set of standard terms and conditions for the most commonly shared data types. The overarching goal of this template project, reducing the administrative burden associated with sharing data that cannot be made publicly available, cannot be realized if member institutions alter the terms and conditions of the template.

If using the DTUA for a circumstance that the FDP template is not intended to cover, such as sharing data with a foreign recipient, you may modify the standard template language for such a case; however, please remove the FDP moniker so that it is clear the FDP standard template language was altered.

3. Could my institution choose to edit the FDP DTUA Template so that it may be used for a circumstance not covered by the published template?

The FDP DTUA Working Group recognizes that the published DTUA does not cover all data transfer and use scenarios. In those limited cases not covered by the published DTUA, institutions can choose at their own risk to make edits to the FDP DTUA template and issue their own form of agreement. However, they must remove references to FDP anywhere it appears within the template, and the agreement should look distinct. This is necessary to facilitate review and make clear to the other party that the commonly accepted FDP DTUA language has been changed and that the version is not that which has been published on the FDP website. This permission does not extend to instances for which the template has been designed.

4. Where can I add my special terms and conditions?

The DTUA was created to encourage consistency among Data Providers and Recipients and reduce the administrative burden and delay caused by the use of special terms and conditions that may not be necessary or applicable to agreements between FDP members. That being said, the DTUA does allow for certain categories of terms and conditions to be incorporated, if such language is required due to the nature of the Data and Project.

Attachment 1 of the DTUA allows for the inclusion of project-specific terms. Paragraph 3 provides for inclusion of any requirements pertaining to the transfer of the Data, such as instructions for transmitting or accessing the Data. Paragraph 4 provides for inclusion of terms concerning payment, such as the amount the Recipient is paying for the Data and relevant payment deadlines. Paragraph 5 provides for inclusion of any disposition requirements that may apply to the Recipient upon termination or expiration of the Agreement, such as a date by which the Data must be returned or destroyed, a method of destruction, or any required documentation of the Data's disposal.

5. My institution wants to add specific information security requirements. Where can I add those?

The purpose of the DTUA template program is to minimize the addition of institution-specific terms, conditions, and controls. The template has been carefully developed for use in many of the most common data transfer and use transactions encountered. As such, the template includes references to those laws and regulations of the United States which are commonly applicable to the transfer and use of data and contains reasonable and acceptable requirements in Attachment 2 for the protection of the types of data for which use of the template is deemed appropriate.

However, the template should not be considered appropriate for use in every data transfer and use scenario. For situations involving the transfer of highly controlled or sensitive information, such as classified data, export controlled data (other than data designated as EAR99), or data subject to foreign laws and/or regulations (such as the European Union's General Data Protection Regulations (GDPR)), the DTUA template should not be used. For those situations involving data for which the use of the template is appropriate, the inclusion of additional terms and conditions generally adds additional administrative burden without enhancing the protections for the Data or Provider.

If a Provider believes the Recipient to be at high-risk for data loss or inappropriate data exposure, or that the Recipient will otherwise be unable to adhere to the applicable laws and regulations, either the Data should not be shared or the template should not be used for that specific data transfer. In such circumstances, the development of a project-specific DTUA, which includes additional specific controls, requirements, or remedies in the event of data loss or inappropriate data exposure, would be more appropriate.

6. The template doesn't include any references to cloud storage. Does this mean that the Recipient is permitted to store the Data in the cloud? Or is this prohibited since it isn't mentioned?

The DTUA template is designed to be a living document that can accommodate rapidly changing technology and therefore is intentionally silent regarding the type of storage used to house the data once transferred. Instead, we have focused the template language on the protections required for housing that data under applicable laws and regulations, irrespective of the type of storage used (e.g., cloud server vs. local server).

7. Can I use the DTUA to share any kind of controlled information?

The DTUA template should not be considered appropriate for use in every data transfer and use scenario. For situations involving the transfer of highly controlled or sensitive information, such as classified data, export controlled data (other than data designated as EAR99), or data subject to foreign laws and/or regulations (such as the European Union's General Data Protection Regulations (GDPR)), the DTUA template should not be used.

8. What if I need to share data with an entity not contemplated by the DTUA?

The terms and conditions of the DTUA are designed to cover the risks encountered by non-profit, federal, and educational institutions when they share data under typical research conditions; these terms and conditions are not entirely appropriate for data centers or registries, or when sharing data with a for-profit or foreign entity. However, the FDP recognizes that the language contained within the

template can be a useful starting point when creating DTUAs for these other situations. Therefore, you may copy the terms into a customized template, so long as your custom template does not reference the FDP.

9. When would it be appropriate to create a customized Attachment 2?

If a published version of Attachment 2 exists for the type of data being shared, using the published Attachment 2 will help reduce the administrative burden on both parties to the DTUA. However, in the event that you are sharing a unique data set that requires protections other than those found in the existing versions of Attachment 2, you may use "Attachment 2 - Other" to incorporate the required protections for your data set. Please keep in mind that this is not intended to be used to incorporate terms and conditions in excess of or in conflict with what has been agreed to by the FDP membership.

See the FAQs in the Guidance on Selecting Versions of Attachment 2 section below for further information on selecting the appropriate version of Attachment 2 in various data sharing scenarios.

An example of when Attachment 2-Other might be appropriate: Your university is based in California. You have a faculty member in the computer science division doing research in collaboration with a law professor at another California university. Your faculty member is collecting data on the efficacy of the Student Online Personal Information Protection Act (SOPIPA), which requires websites to remove student information upon request by the school district. The data being gathered for the collaboration does not include identifiable information on the students but focuses on the school districts. While you are pretty sure that the SOPIPA provisions do not apply to the research, your office would like to ensure that the SOPIPA provisions are flowed down, for the avoidance of any doubt.

An example of when use of Attachment 2-Other would not be appropriate is when human subjects data has been obtained from a State or Federal Agency, such as the Veterans Health Administration, and you would need to flow-through a publication term or indemnification which would conflict with the same terms included in the DTUA. In such a case, you may choose to use the FDP DTUA template as a starting point as long as the FDP moniker is removed.

10. Section 2 of the Agreement and Section 4 of Attachment 1 provide the option for the Provider to request reimbursement for any costs associated with the assembly, preparation, compilation, and transfer of the Data to the Recipient. What are some examples of costs that a Provider could include under this section?

The intent of the DTUA is not as a funding agreement, per se, but if assembly of the Data requires incidental costs that need to be reimbursed, the Provider may request reimbursement. Examples include purchase and shipment of a standalone server for transfer of the

Data or labor involved in extracting a dataset from a larger database. The DTUA should not be used for revenue-generating sale or licensing of data, nor should it be a substitute for a funding agreement. The intention of this section is to facilitate reimbursement to the Provider for its actual costs incurred in sharing the Data with the Recipient.

11. When should a DTUA be used with a funded subaward agreement?

The FDP Subaward Template now provides the parties the opportunity to incorporate terms and conditions that may otherwise be included in a separate DTUA within the subaward to alleviate the need for the parties to execute a separate agreement, with the understanding that many institutions may still require a separate DTUA due to their institutional policies, procedures and/or structure. This section of the Subaward Template is intended to prompt the parties to consider whether a DTUA or incorporation of special language in the subaward is needed at the time that the initial subaward is issued, as this could help alleviate delays in the transfer of human subjects data needed to perform the project.

The DTUA Working Group and Subawards Subcommittee formed a collaborative working group in January 2019 with the goal of:

1. Creating subaward template language that PTEs and/or Subrecipients may use to incorporate DTUA terms;
2. Providing recommendations to the Subaward Template Working Group on the best technical solutions for inclusion of such terms; and
3. Creating FAQs or guidance specific to the inclusion of DTUA terms in a subaward (including when it might be best to have a separate DTUA, considerations for each institution in determining whether (or not) to develop a process to include DTUA language in the subaward, and considerations for working with institutions that have made a different decision on this topic).

Further guidance will be released on this topic as developed by this new working group. For more information, please feel free to contact the DTUA Working Group and Subawards Subcommittee co-chairs via Melissa_Korf@hms.harvard.edu, mrdavis@brandeis.edu, and/or subawards@thefdp.org.

12. My institution would like to require a list of each individual who will access the data on behalf of the Recipient. Where should I incorporate the list into the Agreement? Can I require that a formal amendment is processed each time there are changes to this list?

The face page carefully defines authorized persons as, “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").” Given this, there should be no need for the Provider to contractually permit each individual user by name to access the data. If the Provider requires information on the individuals who have access to the data, the low burden method to achieve this is to require a report of these individuals from the Recipient. This reporting requirement, instructions for individual users to access the data via VPN, or other special instructions on qualifications of individuals who access the data could be incorporated into Section 3 of Attachment 1 or the definition of Collaborator Personnel in Attachment 3, whichever is most appropriate. To avoid the introduction of unnecessary administrative burden through execution of amendments to change personnel lists, the personnel list should not be a part of the contract. Please keep in mind that Recipient individual users of the Data would be tracked by IRB protocol and approvals; therefore, the list of Recipient personnel accessing the Data would be tracked there as well.

For the avoidance of doubt, this would not apply to changes to the Recipient Scientist, changes to which would require some action to be taken with the Agreement.

Guidance on Selecting Versions of Attachment 2

13. Is the Provider or Recipient ultimately responsible for determining which version of Attachment 2 is used in the DTUA?

It is the purview of the Provider to determine what type of Data will be shared and, correspondingly, what requirements must be incorporated into the DTUA and which version of Attachment 2 is appropriate. The intent of the DTUA is for the Provider to ensure their obligations are met and not necessarily to cover all obligations that would apply to the Recipient (for example, state laws that would apply to the Recipient but not the Provider may not be incorporated into the DTUA but would still apply to the Recipient).

This determination is different from the process that would be followed in a subaward agreement. In a subaward, the required flow-down terms may depend upon specific characteristics of the subrecipient. Under a DTUA, the Provider owns the data and expects the Recipient to protect the data as necessary for the Provider to make sure that the Provider is able to meet its obligations under law/regulation. The Recipient’s obligation is to review the DTUA to ensure that they can meet the stated data protection obligations. In this sense, a DTUA is a simpler transaction and does not need to take into account the entity type of the Recipient.

14. My institution is not a covered entity. Can my institution receive Protected Health Information (PHI) (including a Limited Data Set) from a Covered Entity?

Yes; a HIPAA Covered Entity may disclose patient PHI for research pursuant to either an individual’s Authorization, an IRB or Privacy Board Waiver of Authorization, or as a Limited Data Set. Covered Entities may also provide data that has been de-identified in

accordance with HIPAA, in which case it is no longer PHI under HIPAA (and would also no longer be considered identifiable under the Common Rule).

15. When would a non-covered entity/component disclose a HIPAA Limited Data Set?

It would not. "Limited Data Set," as used in these Attachments, is a HIPAA term that is only applicable to a HIPAA Covered Entity. The Attachment 2 for a Limited Data Set assumes that the Provider is a HIPAA Covered Entity (see Number 4 in that Attachment). The Covered Entity/Component status of the Recipient does not impact this selection by the Covered Entity Provider.

16. When should one of the versions of Attachment 2 that incorporates HIPAA be used?

If the Data are being disclosed from the Provider's Covered Entity Component or if the Provider is a Covered Entity and the data have not been de-identified to the HIPAA standard, then the Data are governed by HIPAA and the PII-HIPAA or Limited Data Set attachments should be used. Next look to the list of HIPAA identifiers to determine if the Data are fully identifiable or a Limited Data Set (further information available in the FDP Tool for Classifying Human Subjects Data) and pick the appropriate Attachment 2 based on that analysis.

If the Provider is not a Covered Entity or Covered Entity Component, then HIPAA does not apply, and the Attachment 2 for a Limited Data Set or PII - HIPAA should not be used. There is no equivalent to a Limited Data Set under the Common Rule; the Data are either identifiable or de-identified. Please consult your institution's privacy officer to learn how your institution implements these rules.

The Attachment 2 for de-identified data can be used for data generated under either HIPAA or the Common Rule, so long as no identifiers are shared.

17. Which attachment would an entity that is considered a Hybrid under HIPAA use?

See the FDP DTUA Project Glossary for more information on the definitions of Hybrid and Covered Entity. Hybrid entities under HIPAA contain both HIPAA-Covered Components and non-covered components. The Hybrid's Covered Components are subject to HIPAA in the same way as a HIPAA Covered Entity, and should use the version a Covered Entity would choose in the same circumstances. The Hybrid's non-covered components are not subject to HIPAA and would make the same choice as an entity that is not subject to HIPAA in the same circumstances.

18. As the Provider, what information do I need to gather and consider in order to make a determination on which version of Attachment 2 I should use?

Step 1: Determine what type of entity you are sending the data from. See the FDP DTUA Project Glossary for definitions of the different entity types for assistance in making this determination

Step 2: Classify the data you are sharing. See the FDP Tool for Classifying Human Subjects Data for guidance on how you can distinguish between the different categories of data.

Step 3: Confirm that you have the authority to share the data for the purpose being described in the DTUA under the laws/regulations that apply to you

Example 1: I am a Non-Covered Entity/Component under HIPAA, and I will provide a dataset containing date of birth (MM/DD/YYYY) to a Covered Entity/Component.
Resolution 1: Because the Provider is not part of a Covered Entity/Component, neither the Limited Data Set nor HIPAA Attachment 2s would be appropriate. Many institutions would consider this identifiable data under the Common Rule, but check with your privacy officer to confirm your institution's practice. Once the Data are accepted, the Recipient can apply whatever additional protections beyond the DTUA that they deem appropriate.

Example 2: I am a Covered Entity/Component under HIPAA, and I will share a Limited Data Set with a Non-Covered Entity/Component.
Resolution 2: The Limited Data Set Attachment 2 is appropriate.

19. How does the HIPAA status of the Provider and Recipient affect the choice of Attachment 2?

There will be some situations where the determination is more complex, but the FDP DTUA Provider Guidance Chart is a good guide. Organizations should also remember to check with their legal counsel regarding the guidance provided in the chart as different institutions may classify these data and their status differently.

20. Are there instances in which a DTUA could include two Attachments 2s?

How this is handled will depend on the study design. If the data sets are being combined into a single database, the entire database must be used and secured in accordance with the most restrictive regulations/requirements applicable to any of the data types. Accordingly, the version of Attachment 2 that reflects the requirements of the most restrictive regulation would be used. In the event that the data sets will be maintained separately, we recommend issuing separate agreements so that all parties are clear which restrictions apply to which data sets. Therefore, it would be highly unusual that more than one Attachment 2 would be needed.

Guidance for Transferring Personally Identifiable Information

21. What is Personally Identifiable Information (PII)?

Please refer to the FDP DTUA Project Glossary for definitions. PII is a broad term that encompasses PHI, as well as other personally identifiable information. While PII is not a defined term under the Common Rule, the Common Rule includes the term "...individually identifiable information..." in its definition of human subject research and does incorporate the concept of PII.

22. Why are there three versions of Attachment 2 for PII?

The original intent of the DTUA Template Working Group was to create a single Attachment 2 to the DTUA to cover PII. However, based on the collective experiences of the Working Group members, which included representatives from both public and private institutions as well as government agencies, we determined that the most effective course would be to create three versions tailored to the specific regulations governing the data. Working Group members have found that incorporating references to regulations that don't apply to the particular data being shared could be inappropriate, concerning, and confusing.

23. What categories of PII are covered by the DTUA template components?

There are three versions of Attachment 2 that work for PII; they include:

- PII - FERPA: The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. More information on FERPA privacy regulations may be found at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

- PII - HIPAA: The regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR Part 160 and Part 164) includes mandated standards for the secure electronic storage and transmission of healthcare information. To comply with these standards, the Department of Health and Human Services issued two regulations, administered and enforced by the Office for Civil Rights: the Privacy Rule and Security Rule. More information on HIPAA privacy regulations may be found at https://www.hhs.gov/hipaa/index.html. HIPAA applies only to Protected Health Information, which is information about the health of an individual created or received by a HIPAA Covered Entity, and which has not been de-identified in accordance with HIPAA's requirements. Please note that a separate version of Attachment 2 has been developed for use in sharing Limited Data Sets; therefore, this version of Attachment 2 should only be used when the data set includes more identifiers than would qualify it as a Limited Data Set.

- PII - Common Rule Only: The Common Rule Only version of Attachment 2 should only be used when neither FERPA nor HIPAA apply to the identifiable data being shared. The Federal Policy for the Protection of Human Subjects or the "Common Rule" was published in 1991 and codified in separate regulations by 15 Federal departments and agencies:
    1. Department of Agriculture: 7 CFR Part 1c
    2. Department of Energy: 10 CFR Part 745
    3. National Aeronautics and Space Administration: 14 CFR Part 1230
    4. Department of Commerce - National Institute of Standards and Technology: 15 CFR Part 27
    5. Consumer Product Safety Commission: 16 CFR Part 1028
    6. Agency for International Development (USAID): 22 CFR Part 225
    7. Department of Housing and Urban Development: 24 CFR Part 60
    8. Department of Justice - National Institute of Justice: 28 CFR Part 46
    9. Department of Defense: 32 CFR Part 219
    10. Department of Education: 34 CFR Part 97
    11. Department of Veterans Affairs - Office of Research Oversight - Office of Research and Development: 38 CFR Part 16
    12. Environmental Protection Agency - Research and Development: 40 CFR Part 26
    13. Department of Health and Human Services: 45 CFR Part 46
    14. National Science Foundation: 45 CFR Part 690
    15. Department of Transportation: 49 CFR Part 11

    The Central Intelligence Agency, the Department of Homeland Security, and the Social Security Administration also comply with all subparts of 45 CFR part 46.

More information on Common Rule privacy regulations may be found at https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html. The revised Common Rule went into effect January 21, 2019. We do not currently anticipate that the revisions to the Common Rule will impact the requirements included in the DTUA, but institutions using the DTUA are responsible for ensuring that their use of the template remains consistent with applicable laws and regulations as they may be updated or revised.

24. What if I am sending both PHI and Education Records?

The Department of Health and Human Services (DHHS) has published a helpful guidance on the difference between educational records and treatment records under FERPA, available here: https://www.hhs.gov/hipaa/for-professionals/faq/518/does-ferpa-or-hipaa-apply-to-records-on-students-at-health-clinics/index.html. If a single data set includes both educational and health records, please also see Question 20 for the DTUA Working Group's recommendation on how to handle these complex/combined data sets. You may also want to engage your institution's privacy officer to determine the best way to handle these complex determinations consistent with your institution's policies and procedures.

Guidance for Third Party Rights

25. What are some examples of third party rights that might mean that I can't use the FDP DTUA template?

Third party rights can attach to a data set in a broad array of circumstances. Examples include:

1) The entity that funded the study under which the data was obtained;
2) The data set was obtained from another party via a different Agreement;
3) Privacy of the persons from whom the data were collected; and
4) The country or jurisdiction in which the data were collected.

For instance, certain data collected in the European Union (EU) are subject to the General Data Protection Regulation (GDPR). The FDP DTUA template is not appropriate for data subject to the GDPR. The template likewise would not be appropriate for data collected in the course of research deemed to be export controlled or when a for-profit funding agency had applied special terms regarding commercialization restrictions. Consent form language may also pose additional concerns for sharing with third-parties: for instance, the IRB may need to review the original consent form to determine whether it allows for the data to be shared with the intended Recipient. Finally, data is often collected across multiple entities, such as when an academic institution collects data from affiliated hospitals, and agreements between these entities may inform how and/or with whom the data may be shared.

Any underlying agreements regarding the arrangement should be reviewed to ensure there is no disagreement with the terms of the template. If any underlying agreements require the addition or flow-down of terms, then use of the FDP DTUA template is not appropriate. The FDP does not recommend using the template to share data that any of the above-referenced agreements would not permit to be shared for the purpose.

26. What is the intended use of Attachment 3?

Attachment 3 was created to allow the Provider the option to authorize Collaborator Personnel (individuals who are employed by another organization and are not under direct control of the Recipient, and who, by nature of their participation in the Project, need to have access to the Data) to access the data via the Recipient. These individuals might include, for example, those affiliated with another entity that also has a DTUA with your organization for this project (multi-site project), a visiting professor working at the Recipient while on sabbatical, or individuals at an institution that might receive only a portion of the Data from the Recipient under conditions that would not require a separate DTUA.