SOP: Data Transfers (DTA)

NUMBER	DATE	AUTHOR	APPROVED BY	PAGE
PRDP-020	07/01/2020	M. M. A. Potter	L. M. Lee	1 of 5

1 PURPOSE

1.1.1 This policy establishes the administrative review procedures for the approval and execution of Data Transfer Agreements regardless of funding when Virginia Tech is either the Provider or Recipient, disclosure and disposition of personally identifiable information (PII) for research by the privacy and research data protection program. PII refers to any data or information about an individual that might reveal the identity or personal information or that could allow someone to indirectly identify a participant.

1.1.2 The transfer of data between organizations is a common need in the research community. When data are confidential, proprietary, and/or otherwise considered sensitive, the organization providing the data (“Provider”) requires the organization receiving the data (“Recipient”) to enter into a written contract to outline the terms and conditions of the data transfer.

1.1.3 For the purpose of this guidance, such a contract is referred to as a Data Transfer Agreement; however, this type of contract is also referred to as a License Agreement, Data Use Agreement (DUA), Confidentiality Agreement, Non-Disclosure Agreement, Memorandum of Understanding, Memorandum of Agreement, or other names if these agreements include data sharing or data transfer requirements.

1.1.4 Any agreement for confidential or proprietary data exchange should be legally structured as a contract between Virginia Tech and the Provider or Recipient and be reviewed and signed by the Office for Sponsored Programs (OSP). DTAs may not be signed by University faculty or staff members in the absence of institutional approval from OSP.

2 REVISIONS FROM PREVIOUS VERSION

2.1 None

3 POLICY

3.1 Transfers of data between Virginia Tech and other institutions or entities must be reviewed and supported by an agreement.

4 RESPONSIBILITIES

4.1 Principle Investigator of a research project (study, investigation) is responsible for the data appropriate transfer of data into and out of Virginia Tech.

4.1.1 <u>Responsible Faculty Member or Principal Investigator</u>

4.1.1.1 Responsible for overall compliance with information protection and use requirements, including the data security level determination in consultation with the Scholarly Integrity and Research Compliance (SIRC)/Privacy and Research Data Protection Program (PRDP)

4.1.1.2 Approves final language and agrees to requirements within the DTA and ensures that the protection requirement can be met

4.1.1.3 Ensures that all study team members are aware of their responsibilities under the DTA and received appropriate training on the DTA requirements and relevant policies and procedures related to data security and access

4.1.1.4 Promptly notifies SIRC and departmental technical support who manages access to the data of any additions to the study team, to ensure that any new team members are appropriately trained and authorized to access project data. If the DTA lists team members with access to the data, the PI must notify OSP of any changes to the team within 3-5 business days.

4.1.1.5 Ensures that departing study team members are reported to SIRC and that access to study materials is removed promptly. Departing researchers may not retain study data in their personal possession or transfer data from Virginia Tech without an appropriate agreement in place.

4.1.1.6 Works with the appropriate IT support team to ensure an appropriately secured transfer-method and storage location is available to receive and maintain the data described in the DTA

4.1.1.7 Ensures that data are retained for the required period and disposed of according to the requirements of the DTA or Virginia Tech policy

4.1.2 Research Team

4.1.2.1 Responsible for understanding and complying with Virginia Tech policy, DTA security and access requirements, and completing any required training

4.1.2.2 Promptly notifies the Virginia Tech IT Security Office (ITSO) and SIRC/PRDP if they become aware of any breaches of security or unauthorized access to research data

4.1.3 Department Chair of Leaving Faculty

4.1.3.1 Approves data transfer in the event a departing faculty member wants to transfer Virginia Tech data to another institution. OSP will send the Department Chair an email with appropriate information for their affirmation of approval.

4.1.3.2 Responsible for appointing a data custodian to provide oversight of data being retained by the university

4.1.4 Office of Sponsored Projects

4.1.4.1 Responsible for negotiation of the DTA and is the institutional signatory for all DTAs

4.1.4.2 Renegotiates and signs amendments to previously executed DTAs

4.1.4.3 Confirms the appropriate data security level according to the High-Risk Digital Data Protection standard and processes outlined 7010, Policy for Securing Technology Resources and Services

4.1.4.4 Verifies the study team's ability to meet the protection requirements with the department IT Support team

4.1.4.5 Confirms that the PI has completed the appropriate reviews and obtained the necessary approvals, including provisioning and PRDP review, and manages timing of DTA execution accordingly

4.1.5 Scholarly Integrity and Research Compliance / Privacy and Research Data Protection

4.1.5.1 Responsible for review and approval of research protocols involving the participation of human subjects, and Not Human Subjects Research determinations as needed. SIRC identifies the data security classification level as part of their review.

4.1.5.2 Ensures that the data storage location and method are compliant with the assigned data security level and the terms set forth in the DTA

4.1.5.3 Evaluates data privacy protections and data custodian arrangement

4.1.5.4 Confers with ITSO if they are unable to determine the appropriate data classification level for research data

4.1.5.5 Promptly notifies the research team, OSP, and appropriate parties if they become aware of any data security breaches

4.1.5.6 Reports any confirmed security breaches or unauthorized access to the Provider promptly in accordance with the terms of the DTA and the Virginia Tech IT Security office.

4.1.6 Virginia Tech IT Security Office

4.1.6.1 Works with other responsible parties to resolve any uncertainties related to security controls set forth in the DTA relevant to the computers or systems that will be used to access and maintain the data

4.1.7 Virginia Tech Departmental IT

4.1.7.1 Provides attestation of OSP and PRDP that the stated controls are in place

4.1.8 Office of the Vice President for Research and Innovation (OVPRI)

4.1.8.1 Responsible for regulatory and policy compliance related to Virginia Tech research activities

4.1.8.2 Ensures that the Virginia Tech policies are implemented for research projects

4.1.9 University Legal Counsel

4.1.9.1 Provides necessary support to OSP to negotiate problematic terms of the DTA, including if the other party is a foreign government

4.1.10 Virginia Tech Intellectual Properties (VTIP)

4.1.10.1 Provides necessary support to OSP if the other party requests non-standard rights regarding Virginia Tech intellectual property

5 PROCEDURE

5.1 Types of Data Requiring a Data Transfer Agreement

5.1.1 The need for a DTA depends on the applicable laws and regulations governing the particular type of data to be exchanged, the policies and/or requirements of the Provider and/or Requester, and Virginia Tech Policy on Ownership and Control of Research Results.

5.1.2 A DTA is required to transfer the following data types:

5.1.2.1 Student information derived from education records that are subject to the Family Educational Rights and Privacy Act (FERPA)

5.1.2.2 Individually identifiable health information or protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA) privacy requirements

5.1.2.3 Deidentified data may require a DTA under certain circumstances if requested by the Provider. The need for a DTA will be determined during the evaluation.

5.1.2.4 Data controlled by laws or regulations other than or in addition to those listed above

5.1.2.5 Data obtained from another individual or organization under obligations of confidentiality

5.1.2.6 Data requiring storage, use, and transfer controls for other reasons (e.g., data that will be shared with anyone outside of Virginia Tech, or proprietary concerns)

5.1.3 When Virginia Tech is the Recipient, a DTA may be required for any of the reasons listed above or as otherwise required by the Provider

5.1.4 If it is unclear whether a DTA is needed OSP will make the determination in consultation with University Legal Counsel.

5.2 Data Request, Transfer, and Disposition

5.2.1 When Virginia Tech is the Provider of the data to another organization or institution, the following steps must be taken:

5.2.1.1 An external or transitioning investigator (Data Requester) submits a data request to the Virginia Tech Principal Investigator (PI) of the study from which the data were generated

5.2.1.2 The PI or Data Requester submits a data intake form for a DTA evaluation request to OSP

5.2.1.3 If the PI is transitioning to another university the PI must notify their Department Chair of data transfer request and OSP will obtain approval from the Department Chair before proceeding

5.2.1.4 If human subject data is to be exchanged, OSP consults with PRDP, as representative of the IRB, to ensure that the proposed use/transfer of the data is consistent with consent form(s) signed by the subjects and has the appropriate protections in place for the data security level assigned to the data

5.2.1.5 If the data to be transferred will be de-identified, PRDP, as a representative of the IRB, will review and attest to that data meets the regulatory requirements for de-identification and document this in the IRB Protocol Management system and OSP Agreement Tracking system with a copy of the associated informed consent for the project.

5.2.1.6 As necessary OSP will consult with PRDP, University Legal Counsel, OVPRI, or VTIP on information security, regulatory, intellectual property, or other legal requirements that need to be included in the DTA.

5.2.1.7 When the negotiation and all applicable compliance reviews are complete, the DTA will be executed by OSP on behalf of Virginia Tech.

5.2.1.8 OSP notifies the Virginia Tech PI that the DTA is complete and provides a copy of the signed agreement.

5.2.1.9 Data are transmitted to the Data Requester in accordance with the DTA terms and conditions.

5.2.1.10 When the DTA expires or is terminated, the Data Requester destroys or returns the data in accordance with the DTA terms and conditions and provides an attestation of destruction (if requested). If an extension is desired, the Data Requester must submit an intake form for OSP to review the request.

5.2.2 When Virginia Tech is the Recipient of the data, the following steps must be taken:

5.2.2.1 A Virginia Tech Data Requester submits a data intake form for a DTA evaluation request to the Office of Sponsored Projects

5.2.2.2 On the intake form the Virginia Tech Data Requester provides the:

5.2.2.2.1 Protocol number (if study related)
5.2.2.2.2 Provider of the data being requested
5.2.2.2.3 Purpose of the study or project
5.2.2.2.4 Data being requested
5.2.2.2.5 Information on the data transfer process
5.2.2.2.6 Any other information and/or documentation required to evaluate the request

5.2.2.3 OSP reviews the information and documentation submitted by the Virginia Tech Data Requester, including any draft DTA received from Provider, and requests additional information as necessary to complete the review or drafting of the DTA

5.2.2.4 If applicable, OSP confirms that HRPP has reviewed the project and the appropriate approval is in place before the DTA can be finalized

5.2.2.5 The Virginia Tech Data Requester must provide a data management plan that includes storage requirements and access controls that are at least as stringent as those required in the Virginia Tech protection standard

5.2.2.6 PRDP reviews the data management plan and any explicit security requirements and confirm with the department IT support team and/or ITSO that the minimum protections can be met

5.2.2.7 OSP negotiates the DTA in compliance with Virginia Tech policies and in consultation with other offices and individuals as needed. If, after negotiation with the Provider, OSP determines that the DTA cannot be brought into compliance with an applicable policy, OSP will consult with the Virginia Tech Data Requester, Legal Counsel, OVPRI, and other offices as required to see if a compromise can facilitate an acceptable agreement.

5.2.2.8 When the negotiation and all applicable compliance reviews are complete, the DTA is executed by OSP on behalf of Virginia Tech

5.2.2.9 OSP notifies the Virginia Tech Data Requester that the DTA is complete and places a fully executed copy in the OSP Agreements Tracker

5.2.2.10 Data are transmitted to the Virginia Tech Data Requester in accordance with the DTA terms and conditions

5.2.2.11 The DTA might contain specific conditions regarding publication review and/or the final disposition of the data such as destruction, limited time archiving, etc. The Virginia Tech Data Requester is responsible for following such requirements.

5.2.2.12 Any requested updates to the DTA must be submitted by the Virginia Tech Data Requester to OSP for review and execution

5.2.2.13 When the DTA expires or is terminated, the Virginia Tech Data Requester ensures disposition of the data in accordance with the DTA terms and conditions and provides an attestation of destruction (if requested). If an extension is desired, the Recipient Data Requester must submit an intake form to OSP to review the request.

6 DEFINTIONS

6.1 **OSP Agreements Tracker**: University-wide system of record used by Virginia Tech faculty, students, and staff to prepare, submit, review, and manage DTAs and DTA updates

6.2 **Data Transfer Agreement (DTA):** A binding contract between organizations governing the transfer and use of data. DTA terms and conditions vary depending on the laws and regulations governing the type of data as well as the policies and/or requirements of the Provider. A DTA must be signed by an Institutional Signatory.

6.3 **Data Security Level:** A qualification applied to a data set considering the content and use. The determined data security level corresponds with required security controls (including data storage and management).

6.4 **Provider:** Individual or organization providing data to a recipient individual or organization

6.5 **Receiver/Recipient:** Individual or organization receiving data from a provider individual or organization

7 MATERIALS

7.1 Policy 13015 “Ownership and Control of Research Results”

7.2 Policy 13000 “Policy on Intellectual Property”

7.3 Data Intake form

8 REFERENCES

8.1 None