



## INTRODUCTION

A Data Use Agreement (DUA) is a binding contract governing access to and treatment of nonpublic or sensitive data provided by one party (a “Provider”) to another party (a “Recipient”). DUAs are often required by external parties before they permit data to be received by Harvard and may also be necessary for Harvard data to be disclosed to another organization. DUA terms and conditions vary depending on the laws and regulations governing the specific type of data to be shared, as well as the policies and/or requirements of the Provider and Recipient. Formal agreements in these cases help to avoid misunderstandings and disputes over the use and storage of data, appropriate access and security measures, and other important matters, including publication rights and ownership of results.

## POLICY STATEMENT AND EXEMPTIONS

All DUAs shall be considered research-related agreements and must be reviewed and signed by one of the Negotiating Offices<sup>1</sup>, in accordance with the [Delegation of Signing Authority with Regard to Grants and Research Contracts](#). The signature of an institutional official certifies that commitments made in such agreements can and will be honored, and ensures that all DUAs conform to relevant laws, regulations, agency guidelines, and University policies and processes. Researchers and staff other than those designated in the Delegation of Signing Authority may not sign DUAs.

All DUAs or requests for DUAs shall be submitted through the University-wide [Agreements Application](#) for review, negotiation, and endorsement by the appropriate Negotiating Office. For further information, including details regarding procedures, roles, and responsibilities of all involved parties, as well as defined terminology, please see the attached Data Use Agreement (DUA) Guidance.

All questions pertaining to the interpretation of this Policy, or requests for an exception to one of the requirements, should be referred to the [Office of the Vice Provost for Research](#) and the [Office for Sponsored Programs](#).

## RELATED RESOURCES, DOCUMENTS AND POLICIES

### Negotiating Offices Contacts:

- Harvard T.H. Chan School of Public Health: [Office of Research Administration](#) (ORA) [dua@hsph.harvard.edu](mailto:dua@hsph.harvard.edu)
- Harvard Medical and Dental Schools: [Office of Research Administration](#) (ORA) [SPAContracts@hms.harvard.edu](mailto:SPAContracts@hms.harvard.edu)
- University Area, all other Harvard schools: [Office for Sponsored Programs](#) (OSP) [dua@harvard.edu](mailto:dua@harvard.edu)

### Resources:

- [Agreements System Guidance](#)
- [Research Support Website](#)

**Data Policies:** <https://researchdatamanagement.harvard.edu/policies>

---

<sup>1</sup> The Office for Sponsored Programs, the HSPH Office for Research Administration, and HMS Office for Research Administration



## PURPOSE

The purpose of this Guidance is to set forth the administrative review procedures for the approval and execution of DUAs at Harvard when Harvard is either the Provider or Recipient.

The transfer of data between organizations is common in the research community. When the data is confidential, proprietary, or otherwise considered sensitive, the Provider will often require that the Recipient enter into a written contract to outline the terms and conditions of the data transfer. For the purpose of this Guidance, such a contract is referred to as a DUA, however, Providers may refer to such contracts as a License Agreement, Confidentiality Agreement, Non-Disclosure Agreement, Memorandum of Understanding, Memorandum of Agreement, etc. Any agreement for confidential or proprietary data is considered a legally binding contract between Harvard and the Provider or Recipient, and must be reviewed and signed by an authorized Harvard signatory in one of the Negotiating Offices. DUAs may not be signed by University faculty, students or staff members in the absence of institutional approval from the appropriate Negotiating Office.

## OVERVIEW

Harvard has established processes and supporting systems for reviewing and approving DUAs and other related components of research projects. The University's [Compliance System](#) is comprised of applications (e.g. ESTR-IRB, Agreements-DUA, Research Data Safety-IT Security) that facilitate compliance with internal policies, as well as external regulations and requirements, such as those included in a DUA. As described in greater detail throughout this Guidance, researchers are required to utilize the [Agreements Application](#) to request DUA review and signature by the cognizant Negotiating Office. Due to the responsibilities and security obligations that can result from a DUA, researchers are also required to link<sup>2</sup> the Agreements Application review to a corresponding [Research Data Safety](#)<sup>3</sup> submission, to allow for information security reviewers to assess the DUA's security language and ensure data is appropriately protected.

## DEFINITIONS

**Agreements Application (Agreements Application):** University-wide system of record used by the Harvard faculty, students, and staff to prepare, submit, review, and manage DUAs and DUA updates.

**Compliance System:** The Compliance System is made up of various applications (e.g. ESTR-IRB, Agreements-DUAs, Research Data Safety-Information Security) that support institutional compliance with internal policies as well as external laws and regulations. Reviews from each application should be linked using the [Manage Related Projects](#) function. Both researchers and administrators have access to the Compliance System, as it is intended to provide transparency and consistency to Harvard's research processes and procedures.

---

<sup>2</sup> [Guidance](#) on Managing Related Projects (i.e. "linking" reviews)

<sup>3</sup> [Data Safety Application](#) for Research Data Security Review



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

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

**Electronic Submission, Tracking & Reporting (ESTR) Application:** University-wide system of record for submission of IRB review requests, for studies involving human subjects research.

**Harvard Enterprise Information Security Policy (HEISP):** Policy which addresses the need to protect confidential and sensitive information. When indicated in this document, it is inclusive of the Harvard Research Data Security Policy.

**Harvard Research Data Security Policy (HRDSP):** Policy which outlines requirements for proper management of research data, including relevant reviews, training and submissions in the Compliance System.

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

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

**Related Offices:**

- Institutional Signatories
  - Harvard T.H. Chan School of Public Health: Office of Research Administration (ORA)
  - Harvard Medical and Dental Schools: Office of Research Administration (ORA)
  - University Area, all other Harvard schools: Office for Sponsored Programs (OSP)
- Institutional Review Boards (IRB)
  - Harvard T.H. Chan School of Public Health, and Harvard Medical and Dental Schools: Longwood Campus IRBs
  - University Area, all other Harvard schools: Committee on the Use of Human Subjects (CUHS)
- Information Security Policy and Consultation
  - Harvard Enterprise Information Security Policy: Harvard University Information Technology
  - Harvard Research Data Security Policy: Office of the Vice Provost for Research

**Research Data Safety Application (Safety Application):** University-wide system of record for submission of data security and management plans, security reviews of DUAs, and other researcher requests for Security Review by an Information Security Reviewer.



## ROLES AND RESPONSIBILITIES

The following describes the roles and responsibilities related to the DUA process for various individuals and offices at Harvard.

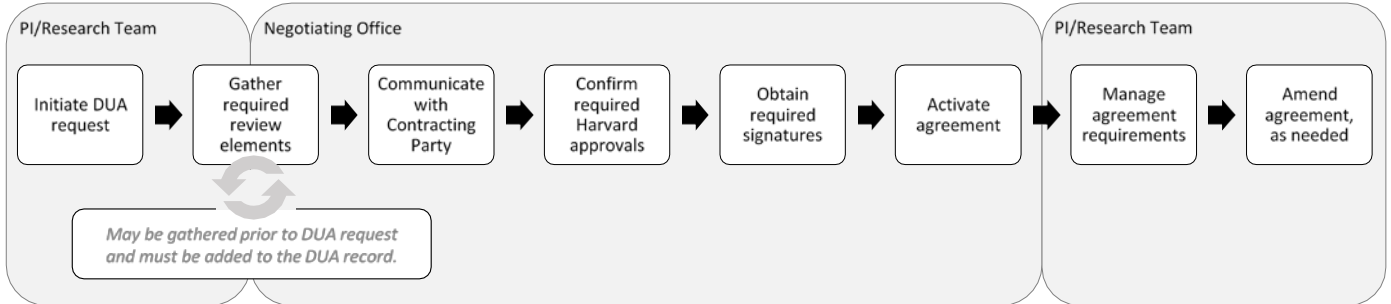
1. *Harvard Data Requestor (researcher submitting request in Agreements Application)*: Initiates the DUA review in the Agreements Application and communicates with the appropriate Negotiating Office to provide additional information, as needed, to facilitate review and negotiation of the DUA. Also initiates corresponding Security Review of project in the Safety Application, and Manages Related Projects.
2. *Responsible Faculty Member or Individual with Principal Investigator status (if different from Harvard Data Requestor)*:
  - Responsible for overall compliance with information protection and use requirements, including submission of review requests in the ESTR (as necessary), Agreements and Safety Applications.
  - Approves final language and agrees to the responsibility as indicated by the DUA, including, if required by the DUA, by way of signature.
  - Ensures that all study team members are aware of their responsibilities under the DUA and corresponding Data Security Plan.
  - Ensures that the protection requirements can be met and that all individuals who have access to the data have received appropriate training on the DUA requirements and relevant policies and procedures related to data security and access.
  - Promptly updates Data Security Plan in the Safety Application in the event of any changes to the composition of the study team, so that any new team members may be appropriately briefed, trained, and authorized (as defined by the DUA and Harvard policy) before they are granted access to the data, and so any departing team members' authorization may be promptly discontinued.
  - When the DUA lists team members with access to the data, promptly notifies the appropriate Negotiating Office of any changes to the team.
3. *Research Team*: Each research team member will be listed in the Safety Application submission (and/or Agreements Application submission, if named in DUA), and is responsible for meeting and complying with the specific Harvard Policy(ies) and DUA security and access requirements, including any required training. Team members shall promptly notify the appropriate parties, per HEISP processes, if they become aware of any breaches of security or unauthorized access.
4. *The Negotiating Offices*:
  - Responsible for negotiation of the DUA and is the Institutional Signatory for all DUAs for schools within their purview.
  - Generates a summary outlining key points of each DUA for the PI.
  - Negotiates and signs modifications to previously executed DUAs (amendments).



- Reports any confirmed breaches of security or unauthorized access as reported by the research team to the Provider promptly, and in accordance with the terms of the DUA and the HEISP.
  - Confirms that the PI has completed appropriate reviews or obtained necessary approvals, including Security Review in Safety Application, and any needed IRB review in ESTR, and manages timing of DUA execution accordingly.
5. *Information Security Reviewer*: Reviews the Harvard Data Requestor's draft Data Security Plan in the Safety Application. Works with the Research Team, including Responsible Faculty Member, to determine the Data Security Level (DSL). Ensures that the data storage location and method are compliant with the applicable DSL and the terms set forth in the DUA. Notifies the Research Team, the appropriate Negotiating Office and other appropriate parties (such as the IRB) if they become aware of any breaches of security or unauthorized access promptly, per the HEISP.
  6. *Institutional Review Board (IRB)*: Responsible for review and approval of research protocols involving the participation of human subjects, and Not Human Subjects Research determinations (as needed) in ESTR Application. The IRB classifies the project as Sensitive or non-Sensitive as part of their review.
  7. *Office of General Counsel (OGC)*: The Negotiating Offices may consult with OGC, if necessary, to negotiate a particularly problematic term of the DUA, including if the other party is a foreign government.
  8. *Office of Technology Development (OTD)*: The Negotiating Offices may consult with OTD if the other party requests non-standard rights in Harvard's project intellectual property.
  9. *Office of the Vice Provost for Research (OVPR)*: Responsible for all regulatory and policy compliance related to research activities, as well as review and approval of any exemption requests under DUA Policy and HRDSP.
  10. *Harvard University Information Technology (HUIT)*: Responsible for ensuring compliance with regulatory requirements and internal policies regarding data security, as well as approval of exemption requests under the HRDSP.



## PROCEDURES



### 1. Types of Data Requiring a Data Use Agreement

Whether or not a DUA is required depends on applicable laws and regulations governing the particular data type, the policies and/or requirements of the Provider and/or Requester, and Harvard's Data Ownership Policy.

**When Harvard is the Provider**, a DUA is required to transfer the following data types:

- Individual identifiable health information or protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA) privacy requirements, even if the data is not identifiable
- Student information derived from education records that are subject to Family Educational Rights and Privacy Act (FERPA)
- Data on individuals originating in the European Economic Area (EEA) or the United Kingdom (UK) that is subject to the General Data Protection Regulation (GDPR) or UK GDPR
- Data that is controlled by laws or regulations, domestic or foreign, other than or in addition to those listed above
- Data obtained from another individual or organization under obligations of confidentiality
- Data whose storage, use, and transfer must be controlled for other reasons (e.g. DSL 3 data that will be shared with individual(s) outside of Harvard, or proprietary concerns)
- As necessary to comply with the [Data Ownership Policy](#), Section 4, *Transfer in The Event A Researcher Leaves Harvard*

**When Harvard is the Recipient**, a DUA is required for any of the reasons listed above, and as otherwise required by the Provider.

If it is unclear whether a DUA is needed, please contact the appropriate Negotiating Office for assistance in making a determination.



## 2. Data Request, Transfer, and Disposition

*When Harvard is the Provider (in cases other than submission of research to a data repository or data bank), the following steps are generally involved:*

- a. An external researcher (the “Recipient Data Requestor”) submits a data request to the Harvard Principal Investigator (“Harvard PI”) of the study under which the data was generated.
- b. The Harvard PI reviews the request and determines whether it should be approved.
- c. If approved, the Harvard PI reviews the criteria set forth in Section 1 above and/or consults with the appropriate Negotiating Office to determine whether a DUA is needed in order to transfer the data outside of Harvard.
- d. If a DUA is needed, the Harvard PI submits the request through the Agreements Application for an outgoing DUA to the appropriate Negotiating Office, and links any relevant Data Safety and ESTR reviews.
- e. In consultation with other offices and individuals as needed, the Negotiating Office prepares a DUA to send to the Recipient Data Requester, negotiates the DUA as needed, and signs when complete.
  - i. Outgoing DUAs require Security Review in the Safety Application to ensure data handling is consistent with applicable HEISP security requirements.<sup>4</sup>
  - ii. If human subjects data, the Harvard PI confirms with the IRB that the proposed use of the data is consistent with any relevant protocol(s) and consent form(s) signed by the subjects, and provides documentation of such confirmation upon request.
  - iii. The Negotiating Office may consult with OGC, OVPR or OTD on any regulatory, intellectual property or other legal requirements that may need to be included in the DUA.
  - iv. It is important to note that if it is determined that a DUA is appropriate by the Negotiating Office, documentation of IRB approval and information security attestation of a plan for sufficient security controls for data transfer and storage, may be required from the Recipient prior to DUA signature.
- f. The Negotiating Office notifies the Harvard PI that the DUA is complete and ensures a copy of the signed agreement is available in the Agreements Application.
- g. Data is transmitted to the Recipient Data Requestor in accordance with the DUA terms and conditions.
- h. When the DUA expires or is terminated, the Recipient Data Requestor destroys or returns the data in accordance with the DUA terms and conditions, which may involve consultation with the Harvard PI and/or the Negotiating Office.

---

<sup>4</sup> The following categories of outgoing DUAs do not require a new review in Data Safety (however, if applicable, existing relevant Data Safety record(s) should be updated to reflect the current state of the underlying data & Research Team): (i) departing PI, as described in Section 4, *Transfer in The Event A Researcher Leaves Harvard* of the Data Ownership Policy, and (ii) animal data, unless there are specific data security requirements attached.



***When Harvard is the Recipient***, the following steps are generally involved:

- a. A Harvard Data Requestor submits a data request to the Provider which describes the purpose of the study, identifies the data set being requested, and includes any other information and/or documentation required by the Provider.
- b. The Provider reviews the request and, if approved, will either send the Harvard Data Requestor a draft DUA for review and signature by Harvard, ask that Harvard provide a draft DUA, or enter into a conversation with the appropriate Negotiating Office to determine whether a DUA is needed.
- c. Once the Provider and/or the Negotiating Office have confirmed that a DUA is needed, the Harvard Data Requestor submits the DUA request through the Agreements Application, and links any relevant reviews.
- d. The Negotiating Office: Reviews information and documentation submitted by the Harvard Data Requestor, including any draft DUA received from Provider, and requests additional information as necessary to complete the review or drafting of the DUA, including confirmation of the following:
  - i. Unless the Responsible Faculty Member<sup>5</sup> is able to self-determine and certify<sup>6</sup> that the project is not human subject research, the Harvard Data Requestor must submit a request in ESTR for IRB review. The relevant ESTR submission must be linked to the Agreements Application submission by the Harvard Data Requestor prior to DUA execution.
  - ii. Information Security's approval in the Safety Application must be obtained prior to execution of the DUA. The Harvard Data Requestor should reference the DUA and all the underlying data in the Data Security Plan, and highlight any known restrictions and requirements. The Safety Application submission must be linked to the Agreements Application submission by the Harvard Data Requestor.
    - If the DUA includes explicit data security requirements, the Harvard Data Requestor must attach the DUA in the Safety Application submission.
- e. The DUA is negotiated in compliance with all applicable Harvard policies and in consultation from other offices and individuals as needed. If, after negotiation with the Provider, the Negotiating Office determines that the DUA cannot be brought into compliance with an applicable policy, the Negotiating Office will consult with the Harvard Data Requestor's School Dean, OVPR, and other offices as required. When the negotiation and all applicable compliance reviews are complete, the DUA is executed by the Negotiating Office on behalf of Harvard.
- f. The Negotiating Office notifies the Harvard Data Requestor that the DUA is complete and makes available within the Agreements Application a fully executed copy along with a summary which outlines key points of the DUA. Note that any special requirements for

---

<sup>5</sup> Only a faculty member can self-certify that a project is not human subjects research

<sup>6</sup> [Investigator Self-Certification Form](#)





individual users must be completed *before* access is granted or, in some cases, before the DUA may be signed.

- g. It is the Harvard Data Requestor's responsibility to understand and comply with the terms of the DUA and to ensure data is only used as specified in the DUA. Therefore, prior to accepting the data from the Provider, the Harvard Data Requestor should read the DUA and accompanying correspondence from the Negotiating Office and seek clarification on any requirements that remain unclear.
- h. Data is transmitted to the Harvard Data Requestor in accordance with the DUA terms and conditions.
- i. The DUA may contain specific conditions on publication review and/or the final disposition of the data such as destruction, limited time archiving, etc. The Harvard Data Requestor is responsible for following any such requirements. Any requested updates to the DUA are to be submitted by the Harvard Data Requestor in the Agreements Application. The Agreements Application will notify the Harvard Data Requestor when the expiration date of the DUA is approaching, and the Harvard Data Requestor is responsible for requesting an extension of the expiration date if additional time is needed to complete his or her research. If an extension is not needed, the Harvard Data Requestor is responsible for ensuring data is destroyed, returned or otherwise appropriately stored, and confirming any such disposition requirements are accurately recorded in the Safety Application.



## RELATED RESOURCES

### University-Wide

Office of the Vice Provost for Research (OVPR)

<https://vpr.harvard.edu/2020/06/26/research-data-management/>

Harvard Enterprise Information Security Policy (HEISP)

<https://policy.security.harvard.edu/>

HEISP Reporting Possible Breach, Loss or Theft of Confidential Information

<https://security.harvard.edu/report-incident>

Harvard Data Ownership Policy

<https://vpr.harvard.edu/2020/06/26/research-data-management/#dataownership>

Harvard Research Data Security Policy (HRDSP)

<https://vpr.harvard.edu/2020/06/26/research-data-management/#hrdsp>

Negotiating and Signing Authority for Agreements Related to Research

<https://osp.finance.harvard.edu/Negotiating-and-Signing-Authority-for-Agreements-Related-to-Research>

Research Data Security Training Course (includes section on DUAs and Agreements Application)

[https://trainingportal.harvard.edu/Saba/Web\\_spf/NA1PRD0068/common/ledetail/cours000000000020423](https://trainingportal.harvard.edu/Saba/Web_spf/NA1PRD0068/common/ledetail/cours000000000020423)

### Harvard Medical and Dental Schools

Office of Research Administration (ORA)

<https://researchadmin.hms.harvard.edu/>

Harvard Biomedical Research Data Management

<https://datamanagement.hms.harvard.edu/>

### Harvard T.H. Chan School of Public Health

Office of Research Administration (ORA)

<https://www.hsph.harvard.edu/financial-services/sponsored-programs-administration/>



**All other Harvard Schools (Harvard University Area)**

Office of Sponsored Programs (OSP)

<https://osp.finance.harvard.edu>

**System Resources**

- Agreements Application: [Information & Job Aids](#)
- ESTR Application: [Information & Job Aids](#)
- Safety Application: [Information & Job Aids](#)

**REVISION HISTORY**

**December 1, 2018** – Data Use Agreement Policy & Guidance implemented

**February 17, 2021** – Data Use Agreement Policy & Guidance updated (reflect updates to HRDSP)

**July 27, 2021** – Data Use Agreement Policy & Guidance updated (update links, and incorporate Data Ownership Policy)