Brown University Data Use Agreement Guidance for Researchers

I. BACKGROUND

A Data Use Agreement (DUA), sometimes referred to as a Data Transfer Agreement (DTA) or Data Sharing Agreement (DSA) or other variations on these terms, is a formal, written contractual agreement into which two or more parties enter and establishes specific ways in which data may be used and how it must be protected. Often data subject to a DUA are a necessary component of a research project. Having an executed DUA in place may be a required precondition to transfer certain data, including human subject research data, protected health information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA), or other data deemed to be sensitive or confidential by the Data Provider. A DUA may also be required when a researcher intends to access protected data in an externally hosted data repository.

DUAs address important issues such as limitations on use of the data, obligations to safeguard the data, liability for harm arising from the use of the data, intellectual property and publication expectations, and privacy rights associated with transfers of confidential or protected data. DUAs legally bind the institution and the individual researcher(s) to appropriate protection and use of the data. The mutual understanding established by a DUA can help prevent future issues by clearly setting forth the expectations of both the Data Provider and Data Recipient.

Importantly, researchers may not sign DUAs on behalf of Brown University; review and signature are required by a responsible party authorized to act on behalf of the University.

II. PURPOSE

The purpose of this guidance document is to set forth the administrative procedures for the review, approval and execution of DUAs at Brown University.

The Office of Research Integrity (ORI) centrally manages the administrative procedures for DUAs that involve research data[1]. ORI coordinates all required reviews (e.g., with Computing and Information Services [CIS], Office of General Counsel [OGC], Office of Insurance and Purchasing Services, etc.) and works expeditiously to bring draft agreements to execution on behalf of the researcher.

[1] There is one approved exception: Brown's School of Public Health (SPH) leadership has authorization to review and sign DUAs for Centers for Medicare and Medicaid Services (CMS) data when such data are being used for an SPH research project.

III. ROLES AND RESPONSIBILITIES

Brown Principal Investigator (PI):

The Brown PI is responsible for compliance with Brown University's DUA review and signature procedures as well as the data protection and use requirements outlined in the DUA. Overall responsibilities include the following:

- Ensuring that the agreement is reviewed and signed by the appropriate institutional official using established submission channels;
- Approving the final language of the DUA by co-signing the agreement and acknowledging all PI and other research team members' responsibilities as indicated by the DUA;
- Ensuring that all research team members are aware of and comply with their responsibilities under the DUA;
- Administering or otherwise arranging for any required training set forth in the DUA and retaining records documenting such training;
- Ensuring that an IRB-approved protocol is in place to cover the work if it involves human subjects, including facilitating an amendment to an existing IRB-approved protocol, when needed, to add the incoming data to the project;
- Working with the appropriate departmental IT Support Consultant, as needed, to identify the appropriate Data Risk Level and adhere to all data security, storage and destruction requirements of the DUA; and
- As necessary, promptly notifying their respective IT Support Consultant or IT contact who manages access to the data in the event of any changes in composition of the study team. When the DUA lists specific research team members with access to the data, the PI must also promptly notify ORI of any changes to the research team to facilitate an amendment to the DUA, if needed.

Brown Research Team:

- Each research team member accessing the data is responsible for meeting and complying with the specific DUA security, confidentiality and access requirements;
- In some instances, research team members must sign security pledge agreements within a DUA acknowledging obligations related to use of the data. It is each research team member's personal responsibility to adhere to any security and/or confidentiality agreements signed in an individual capacity;
- Research team members shall promptly notify the appropriate parties (the PI, ORI and CIS) if they become aware of any breaches of security or unauthorized data access;
- Researcher team members are not authorized to sign agreements on behalf of the University.

Brown Data Requestor:

- This individual may be the Brown PI or a member of the Brown Research Team.

- The Brown Data Requestor initiates the DUA request form and corresponds with ORI to provide additional information, as needed, to facilitate review and negotiation of the DUA.

Recipient Data Requestor:

- This individual is typically an external researcher collaborating with a Brown PI on a research study where there is a request to access or receive data to be provided by Brown.

Data Provider:

- An entity or individual seeking to transfer data or enable access to data that has certain restrictions associated with its use, thereby necessitating a DUA;
- It is the Data Provider's responsibility to establish a DUA outlining terms and conditions for data sharing.

Office of the Vice President for Research (OVPR):

- OVPR is authorized to enter into research agreements, including DUAs, on behalf of the University. All DUAs will be executed by the Vice President for Research (VPR), or the VPR's designee(s) once all terms are negotiated to the satisfaction of the University.

The Office of Research Integrity (ORI):

- Within OVPR, ORI facilitates review and approval of DUAs, including modifications to previously executed DUAs. ORI is also responsible for informing the appropriate parties of any breaches of security or unauthorized access to data as reported to ORI by the Brown Research Team or CIS.

Office of General Counsel (OGC):

- ORI may consult with OGC, if necessary, to negotiate legal terms in a DUA. If the Data Provider is a foreign government or the data being provided to Brown are subject to the General Data Protection Regulation (GDPR), the PI should be prepared for the agreement to undergo OGC review.

Office of Insurance and Purchasing Services:

- ORI may also consult with the Office of Insurance and Purchasing, if necessary, to review insurance terms embedded within DUAs.

Computing and Information Services (CIS):

- ORI consults with CIS to ensure that data security requirements set forth in the DUA related to processes and systems that will be used to transfer, access, store and destroy the data can be met by Brown;

- The Brown Data Requestor may also consult with CIS to determine the appropriate data risk classification level for their research data and verify their ability to meet the minimum security standards as set forth in the DUA.

IV. PROCEDURES

A. When Brown is the Data Provider

When Brown is the Data Provider, an outgoing DUA is required to transfer the following types of data to a Recipient Data Requestor:

- Individually identifiable health information or protected health information ("PHI");
- Personally identifiable information ("PII") being shared beyond the parties named in the formal agreement or contract that governs the transfer of the data, or in the Brown IRB-approved informed consent;[2]
- Student information derived from education records that are subject to the Family Educational Rights and Privacy Act ("FERPA");
- Data that are controlled by laws or regulations other than or in addition to those listed above;
- Data obtained from an individual or organization under obligations of confidentiality;
- Data whose storage, use and transfer must be controlled for other reasons (e.g., Risk Level 3 data that will be shared with anyone outside of Brown, or proprietary concerns)

Review procedures:

- Recipient Data Requestor (outside party) requests data from the Brown PI;
- Brown PI or a designee from the Brown Research Team completes the DUA Request Form;
- Upon electronic receipt of a new request, the ORI will begin initial submission review and will contact the administrative contact listed in the submission if any of the required documentation is missing or incomplete;
- ORI will prepare a draft outgoing DUA to send to the PI and the administrative contact listed.

Approval procedures:

[2] If the data are being shared under the auspices of a Brown IRB-approved protocol in which the recipient party or parties receiving identifiable data from Brown are named in the informed consent, then an outgoing DUA is not required by Brown. However, if Brown is sharing identifiable data with a party not named in the informed consent or the data being shared are subject to special restrictions regarding their protection or use, then an outgoing DUA must be executed.

- Once the terms have been finalized to the satisfaction of Brown, the agreement will be circulated for signature;
- After the agreement has been fully executed (signed by all parties), a PDF copy will be provided to the PI and to the administrative contact listed in the submission.

Executed DUA procedures:

- Data is then transmitted to the Recipient Data Requestor in accordance with the DUA terms and conditions.
- When the DUA has expired or is terminated, the Recipient Data Requestor must destroy or return the data in accordance with the DUA terms and conditions.

B. When Brown is the Data Recipient

When Brown is the Data Recipient, an incoming DUA may be required for any of the reasons listed in IV.A., or as otherwise required by the Data Provider.

- If a Brown PI requests to receive data from an outside institution or organization, it is the responsibility of the Data Provider to determine whether a DUA must be executed prior to sharing the data with Brown. Some governmental organizations have an application process that must be completed prior to the start of negotiations. Please contact ORI when starting this type of application process to assist you with identifying and managing data use/compliance issues;
- The Data Provider will share a template with the data sharing terms. Please submit this template to ORI through the DUA Request Form.
- ORI does not, as a matter of routine practice, create DUAs on behalf of the Data Provider. If a Data Provider is requesting that Brown create a DUA on its behalf, please contact ORI at DUA@Brown.edu to discuss.

Review procedures:

- The Brown Data Requestor submits a data request directly to the Data Provider. The Data Provider will typically either 1) send the Brown Data Requestor a draft DUA for review and signature by Brown, or 2) directly engage in conversation with ORI to determine whether a DUA is needed;
- Once the Data Provider and ORI confirm that a DUA is needed, the Brown Data Requestor submits the draft DUA and request through the Data Use Agreement ("DUA") Request form to ensure the appropriate terms and conditions are negotiated;
- Upon electronic receipt of a new request, ORI will begin initial submission review and will contact the PI and the administrative contact listed in the submission if any of the required documentation is missing or incomplete;
- The DUA is negotiated in compliance with all applicable Brown policies and in consultation with other offices and individuals as needed.

Approval procedures:

- Once all terms have been finalized to the satisfaction of Brown and the Data Provider, the DUA will be circulated for signature;
- ORI notifies the Brown Data Requestor that the DUA is executed and provides a copy of the agreement;
- It is the Brown Data Requestor's responsibility to understand and comply with the terms of the DUA and to ensure data are only used and/or shared as specified in the DUA. Prior to receiving data from the Data Provider, the Brown Data Requestor should seek clarification from ORI if any requirements remain unclear.

Executed DUA procedures:

- Data Provider shares data with the Brown Data Requestor in accordance with the DUA terms and conditions;
- DUAs will typically contain specific conditions on publication and disposition of the data. The Brown Data Requestor is responsible for following such requirements;
- Any requested updates to the DUA must be submitted to ORI by the Brown Data Requestor;
- When the expiration date of the DUA is approaching, ORI will alert the Brown Data Requestor of the impending expiration date. The Brown Data Requestor is then responsible for requesting an extension of the term if additional time is needed to complete the research.

V. DUA PROCEDURES FOR SPECIAL CATEGORIES OF DATA

A. Data Use Agreements for Centers for Medicare and Medicaid Services (CMS) data

- The School of Public Health leadership has authorization to review and sign its own DUAs for CMS data when such data are being used for an SPH research project
- Health and Retirement Study (HRS)/Medicare and National Health and Aging Trends Study (NHAT)/Medicare requests:
    - Typically, researchers requesting these datasets will be asked to complete two separate DUAs; however, since CMS considers the submission a single request, all agreements will be reviewed and processed through the School of Public Health to ensure consistency and to streamline processes.

B. Data Use Certification (DUC) for the National Institutes of Health (NIH) data

- The NIH has established NIH-designated data repositories (e.g., database of Genotypes and Phenotypes [dbGaP], Sequence Read Archive [SRA], NIH Established Trusted

Partnerships) for securely storing and sharing controlled-access human research data submitted to NIH under the NIH Genomic Data Sharing (GDS) Policy.
- ORI is the Signatory Official (SO) for NIH data and Jennifer Welch should be listed as the SO on all dbGaP requests.
- If other data or materials repositories (i.e. EGA) require an institutional official to sign at the time of deposit, ORI will be the SO

C. Externally Hosted Data Accessed Electronically

- In some instances, 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 the equivalent) button.
- A Brown PI, or a designee of the Brown PI, may electronically accept terms and conditions associated with access to externally hosted data.
- ORI will not need to review the terms and conditions associated with electronic access to the data. However, if there is a separate, standalone DUA requiring authorized institutional signature associated with access to the data, the standalone DUA must be sent to ORI for review.
- 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.

VI. COMMONLY USED DUA TERMS

Aggregate Data: Aggregate Data is data that has been gathered, processed and expressed in a summary or report form for reporting purposes such as making comparisons, predicting trends or other statistical analyses. Aggregate data is collected from multiple sources and/or measures, variables or individual human subjects. Since aggregate data is the consolidation of data from multiple sources, it is typically not able to be traced back to a specific human subject.

Anonymous Data: Unidentified (i.e., personally identifiable information was not collected, or if collected, identifiers were not retained and cannot be retrieved) data that cannot be linked directly or indirectly by anyone to their source(s).

Authorization: When referring to a study participant, an individual's written permission to allow a HIPAA-covered entity to use or disclose specified protected health information (PHI) for a particular purpose. Authorization states how, why, and to whom the PHI will be used and/or disclosed for research and seeks permission for that use or disclosure. This term in this context is specific to data use agreements covering PHI. This term may also be used in the more general sense of permission, for instance, an authorization by one party of the data use agreement to

allow the other party to provide the data to additional third parties. Care should be taken to establish the appropriate context when using this term.

Business Associate: Per 45 CFR § 160.103, a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of PHI, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules[3], including the Privacy Rule. Business Associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of protected health information by the covered entity or another business associate of the covered entity to that person or entity. Special attention should be paid to the term "on behalf of" in the definition. Academic Institutions are rarely Business Associates since the term is not applicable to collaborative relationships.[4]

Business Associate Agreement (or Business Associate Contract): An agreement that contractually defines the rights and responsibilities between a covered entity and a Business Associate that would not otherwise be bound by HIPAA. A Business Associate Agreement (BAA) or Contract is **not** appropriate when a covered entity is disclosing PHI to a non-covered entity (like Brown) for use in a research project.

Coded Data: Direct personal identifiers have been removed from the data and replaced with words, letters, figures, symbols, or a combination of these (not derived from or related to the personal information) for purposes of protecting the identity of the source(s). The original identifiers are retained in such a way that they can be traced back to the source(s) by someone with the code. A code is sometimes also referred to as a "key," "link," or "map."

Data Risk Classifications: Brown CIS has classified its information assets into risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access. It is the data and service owner's responsibility to ensure appropriate security measures are taken depending on the risk classification. If you have any questions or need help, please reach out to the Information Security Group (isg@brown.edu).

De-Identified Data: All direct personal identifiers are permanently removed from the data, no code or key exists to link the data to their original source(s), and the remaining information cannot reasonably be used by anyone to identify the source(s). PHI is de-identified when it does not contain any of the 18 identifiers specified by the HIPAA Privacy Rule at 45 CFR Part 164 (or

[3] HIPAA Administrative Simplification Rules: http://www.hhs.gov/hipaa/for-professionals/other-administration-simplification-rules/index.html

[4] FDP Data Transfer and Use Agreement Project Glossary of Terms: http://thefdp.org/default/assets/File/Documents/dtua_glossary.pdf

has been determined to be de-identified by a statistician in accordance with the standards established by the Privacy Rule).

Family Educational Rights and Privacy Act (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.[5]

The General Data Protection Regulation (GDPR): A European law that went into effect on May 25, 2018 and establishes protections for privacy and security of "personal data" about individuals in European Economic Area ("EEA")-based operations and certain non-EEA organizations that process personal data of individuals in the EEA. This law applies in the US for activities involving identifiable information if personal data is being collected from one or more research participants ***physically located*** in the EEA at the time of data collection, regardless of whether the individual is an EEA resident. It also applies to activities involving the transfer of personal data collected under the GDPR from an EEA country to a non-EEA country (like the U.S.). DUAs with GDPR-related terms (such as "data controller" or "data processor") will take longer to negotiate and execute and will be referred to Brown's OGC for review.

Limited Data Set (LDS): A "limited data set" is defined as health information that excludes certain direct identifiers (listed below).

- The Privacy's Rule limited data set provisions requiring the removal of direct identifiers apply both to information about the individual and to information about the individual's relatives, employers, or household members.

- The following identifiers must be removed to qualify as a limited data set: Names; Postal address information, other than town or city, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; Full face photographic images and any comparable images; and Any other unique identifying number, characteristic, or code except as specifically permitted by HIPAA.
- A limited data set may include:
    1. Dates such as admission, discharge, service, date of birth, date of death;
    2. city; state; zip code; and
    3. age in years, months or days or hours.

Personally Identifiable Information (PII): Any information maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual's identity, such as

[5] https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. When allowing access to PII care should be taken that the data or combination of data elements when linked (i.e. taken in combination) do not allow the individual to be distinguished or traced.

- Examples of PII Data: Name:full name, maiden name, mother's maiden name or alias Personal identification number: social security number (SSN) passport number, driver's licenses number, taxpayer identification number, patient identification number, and financial account or credit card number(s).

Personal Health Information (PHI): Under the HIPAA Privacy Rule, "protected health information" is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses).
PHI is only considered PHI when an individual could be identified from the information. PHI includes one or more of the 18 identifiers listed above. If these identifiers are removed the information is considered de-identified protected health information, which is not subject to the restrictions of the HIPAA Privacy Rule.

Sensitive information: Information that has the potential to damage an individual's reputation, employability, financial standing, educational advancement, place them at risk for criminal or civil liability, etc.

VII. UNIVERSITY PARTNERS AND HELPFUL CONTACTS

Brown University Library: The Library helps faculty and student researchers with writing data management and sharing plans (DMPs) for sponsored research proposals and with digital curation. It assists researchers with retaining data by documenting and depositing data sets in long-term repositories for public discovery, access and reuse.

- *University contact*: Andrew Creamer (Andrew_creamer@brown.edu), Scientific Data Management Specialist

The Office of Research Integrity(ORI): ORI supports the Brown University research community by providing guidance, education and resources to facilitate the conduct of ethical research in accordance with governing federal and state regulations and University policies. ORI manages the intake, review and approval for DUAs for research. Please contact ORI through DUA@brown.edu

Computing and Information Services (CIS): CIS supports the Stronghold environment for Risk Level 3 data. Stronghold is a secure computing and storage environment that enables Brown

researchers to analyze sensitive data, while complying with regulatory or contractual requirements.

- Stronghold CIS contact: Mete Tunca (Mete_Tunca@brown.edu), Assistant Director, Cloud and Research Services

VIII. RELATED RESOURCES

- Brown CIS Data Risk Classifications
- Brown CIS Protect University Data
- Brown CIS Data Removal Recommendations
- Brown CIS Data Storing and Sharing
- CIS Stronghold Research Environment for Data Compliance
- Brown IRB Guidance and Policies
- HIPAA Privacy Rule Guidance for Brown Researchers
- Brown Openness in Research Policy