Data Use Agreement Guidance

- When sharing University of Iowa data with a person or entity outside the University, it is generally required or recommended the sharing be documented with a data use agreement.
- If you are depositing data in a repository, individual repositories may have unique requirements for both the investigator and the institution.
- For assistance with data use agreements, please contact the appropriate office listed at the end of this guidance.

Purpose

The purpose of this guidance is to assist its users in assessing whether a proposed outgoing transfer of data that is in the possession of the University of Iowa (UI) and/or a UI investigator (developed in his or her work for UI) to a third party outside of the UI (i) is permissible; and (ii) if so, whether a Data Use Agreement (DUA) is necessary or recommended to affect the transfer. This guidance contemplates the outgoing* transfer of data to third parties who have a bona fide research use or practical application for the data (e.g., collaborating research institutions, academicians, public policy makers, community service providers, etc.).

*Note: This guidance does not address incoming data to be accepted by UI, or a UI investigator, from a third party. Where incoming transfer of data is proposed, the data provider, subject to similar principles described herein, will ultimately determine the appropriate terms for sharing data. This guidance does not address sharing data internally within the UI.

Introduction

DUAs are contractual documents used for the transfer of non-public data that is subject to some restriction on its use. DUAs serve to outline the terms and conditions of the transfer. Specifically, 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, publication, and privacy rights that are associated with transfers of confidential or protected data. The understanding established by a DUA can help avoid later issues by clearly setting forth the expectations of the parties (provider and recipient). Having a signed DUA in place may be a required precondition to transfers of certain data, or it may simply be a good idea. Determining whether a DUA is required is necessarily context dependent. When a DUA is required, it must be purpose specific – i.e., data cannot be transferred pursuant to “master” or blanket sharing agreements without a unique implementing letter identifying the specific data set and uses.

DUAs shall be signed by a UI official who has the appropriate delegated signature authority. DUAs to share data for research purposes shall be signed by the Vice President for Research or the Executive Director of the Division of Sponsored Programs. DUAs for UI Health Care data stored in the hospital's electronic medical record shall be signed by the Chief Executive Officer of University of Iowa Hospitals and Clinics or the Vice President for Medical Affairs. All other DUAs shall be signed by the appropriate authorized UI official depending on the type of data involved, such as the UI’s Business Manager, in accordance with the UI’s Operations Manual, Part V, Section 6.1.

Is the Proposed Data Sharing Permitted? (See Flow Chart Exhibit A to be added later)

1. If the data is derived from human subjects research:
   a. Does the associated informed consent form that subjects signed upon entering the study, or the relevant IRB waiver of consent, permit disclosure for the contemplated DUA purpose?
• No. Sharing is not permitted as is. Contact the Human Subjects Office to inquire about potential options that would allow data sharing.
• Yes. Proceed to #2.

b. Has the IRB or Privacy Board reviewed and approved the data sharing proposal underlying the potential DUA?

• No. Sharing is not permitted as is. Contact the Human Subjects Office to inquire about potential options that would allow data sharing.
• Yes. Proceed to #2.

2. If the data was collected pursuant to a sponsored research project, has the sponsor placed restrictions on the subsequent transfer of the data?

• No. Proceed to #3.
• Yes. Sharing is not permitted as is. Contact the Division of Sponsored Programs to inquire about potential options that would allow data sharing.

3. If the data was initially received from, or derived from data received from, a third party pursuant to a written agreement, does that agreement place restrictions on the subsequent transfer of the data?

• No. Proceed to #4.
• Yes. Sharing is not permitted as is. Contact the Division of Sponsored Programs to inquire about potential options that would allow data sharing.

4. Does any policy, law or regulation prohibit the proposed data sharing? (See also #3 in the following section “When is a DUA Required”).

• No. Data sharing is permitted. Contact the appropriate office listed below for assistance with a Data Use Agreement.
• Yes. Sharing is not permitted as is. Contact the appropriate office listed below to inquire about potential options that would allow data sharing.

**When is a DUA Required? (See Flow Chart Exhibit B to be added later)**

1. Is the data to be transferred derived from human subject research?

• No. If the data does not involve human subjects (either directly, or indirectly via animal or bench research), privacy concerns may no longer drive the need for a DUA, but the data may still be subject to contractual restrictions (see #4 & 5 below) or constitute proprietary data (see #6 below).
• Yes. Proceed to #2.

2. Is the data personally identifiable or HIPAA-protected (i.e., clinical data belonging to a Covered Entity or to the clinical component of a Hybrid Entity)? Use of HIPAA protected data may also require UI Health Care Data Governance Committee Review.

• No. If it is completely de-identified with no remaining personally identifiable information within the meaning of HIPAA and is not disclosed with a code or other means to re-identify the data proceed to #3.

    In order to qualify as completely de-identified, there must be no actual knowledge that the information to be shared could be used alone or in combination with other information to identify an individual, and the data must be stripped of the following elements:
    • Names
• Geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes
• All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, etc.
• Telephone numbers
• Fax numbers
• Email addresses
• Social security numbers
• Medical record numbers
• Health plan beneficiary numbers
• Account numbers
• Certificate/license numbers
• Vehicle identifiers and serial numbers
• Device identifiers and serial numbers
• Web URLs
• IP addresses
• Biometric identifiers, including finger and voice prints
• Photographic images
• Any other unique identifying number, characteristic or code

Note: OHRP (Office of Human Research Protections) does not consider research involving only coded private information or specimens to involve human subjects as defined under 45 CFR 46.102(f) if the following conditions are both met:

(1) the private information or specimens were not collected specifically for the currently proposed research project through an interaction or intervention with living individuals; and

(2) the investigator(s) cannot readily ascertain the identity of the individual(s) to whom the coded private information or specimens pertain because, for example:

(a) the investigators and the holder of the key enter into an agreement prohibiting the release of the key to the investigators under any circumstances, until the individuals are deceased (note that the HHS regulations do not require the IRB to review and approve this agreement);

(b) there are IRB-approved written policies and operating procedures for a repository or data management center that prohibit the release of the key to the investigators under any circumstances, until the individuals are deceased; or

(c) there are other legal requirements prohibiting the release of the key to the investigators, until the individuals are deceased.

• Yes. If the data contains identifiers (see above) or constitutes a Limited Data Set (LDS) within the meaning of HIPAA proceed to #2(b)(i) and (ii) below. An LDS is Protected Health Information that excludes all of the above identifiers except for dates and geographical information at the zip code, town or city level.

i. If the data is being transferred pursuant to authorizations contained in a Business Associate Agreement (BAA) and in accordance with a signed underlying agreement stating what data will be transferred between the parties and how the receiving party will use the data to assist the sending party in a healthcare function, then a data use agreement is not required. A BAA should not be used for data
generated from a research project. It is designed for protection of health care data transmitted to a provider’s business partner for execution of business responsibilities.

ii. Otherwise, a data use agreement is required.

3. Does the data contain:
   (i) “Identification Information” as defined by Iowa Code §715A.8—laboratory’s identity theft statute;
   (ii) “Education Records” as defined by the Family Educational Rights and Privacy Act (FERPA);
   (iii) “Customer Record Information” (CRI) as defined by the Gramm Leach Bliley Act;
   (iv) “Card Holder Data” as defined by the Payment Card Industry (PCI) Data Security Standard;
   (v) employee personnel file information of the type mentioned in Iowa Code §91B.1—an Iowa statute protecting such information;
   (vi) information deemed confidential in accordance with Iowa Code Chapter 22—the Iowa Public Records Law, including trade secrets;
   (vii) any other information that is protected by UI policy or federal or state law from unauthorized access, such as University Internal Data, Restricted Data, or Critical Data as defined in the UI’s IT Security & Policy Office’s Policy on Institutional Data Access available [here](#);
   (viii) any proprietary data? With respect to determinations about whether the data to be shared contains any “proprietary data”, UI’s default position is that the work product of faculty is not proprietary to UI. Unless the data was collected under a sponsored research agreement that allocates ownership of the data and/or imposes restrictions on use (see #4 below), UI is willing to share and the question of “proprietary” becomes one for the principal investigator (see #6 below).

   • No. Proceed to #4.
   • Yes. A data use agreement is required.

4. Was the data collected pursuant to a sponsored research project?
   • No. Proceed to #5.
   • Yes. Does the sponsor require data sharing, claim ownership of or licensing rights to the data, or restrict disclosure and use of the data? Check the terms and conditions of the grants, contracts, agreements, etc. governing the sponsored research project. Sponsor may require a data use agreement, institutional certification, or deposit in a specific repository. Contact the Division of Sponsored Programs for assistance.

5. Are there other restrictions on the contemplated data transfer? Was the data initially received from, or derived from, data received from a third party or other source that restricts use or disclosure?
   • No. Proceed to #6
   • Yes. Data use agreement may be required or recommended to flow through the limitations and restrictions placed on UI’s use and disclosure of the data. Contact the appropriate office listed below for assistance with third party requirements.

6. Even if not required, is a data use agreement a good idea?
   • Does the principal investigator (PI) consider the data to be “proprietary” (i.e., internally generated, not publicly available, and containing technical or other types of information that the PI would like to safeguard to protect his/her/UI’s competitive edge)?
   • Does the PI wish to restrict use of the data, secure publication review and acknowledgement rights, or otherwise direct and control use of the data post-transfer?
   • Does the PI want to obtain a determination IRB approval is not required for use of the deidentified data?
• Yes to either (a) or (b). Data use agreement is recommended to clarify the expectations, rights and responsibilities of the data recipient. Contact the appropriate office listed below for further assistance. Yes to (c) contact the Human Subjects Office for assistance.

• No. Data use agreement is not required.

For more information regarding:

• Data use agreements related to research please contact the Division of Sponsored Programs, dsp-contracts@uiowa.edu or 335-2123.
• Data sharing related to human subjects research please contact the Human Subjects Office, irb@uiowa.edu or 335-6564.
• Data use agreements related to UI Health Care data please contact the UI Health Care Legal, 356-4760
• Other data use agreements, please contact the Office of the General Counsel, general-counsel@uiowa.edu or 335-3696.
• Citing and creating references in publications to datasets shared via DUAs, contact Library Data Services, lib-data@uiowa.edu or 467-0069.