**Data Transfer/Sharing Checklist**

**Data Use Agreement (DUA) Contacts:**

**Sponsored Projects Office**

* HSC-PreAward@salud.unm.edu

**Privacy Office**

* HSC-Privacy@salud.unm.edu

**Information Security Office**

* [HSC-ISO@salud.unm.edu](mailto:HSC-ISO@salud.unm.edu)

**NOTE: For any data transfer/sharing questions or for help filling out this section, please email all contacts listed above.**

**All information stated in this section must be congruently stated in all other applicable sections of the protocol.**

**Provide all information requested, meaning all questions must be answered, if the research involves transferring/sharing of data with an external entity (institution, company, etc.).**

1. Will UNM data be transferred/shared with an external entity (i.e. another institution, company, etc.) or will an external entity’s data be transferred/shared with UNM?

Yes. **If yes, all questions must be answered congruently based on protocol provisions.**

* + - If yes, does this research involve federal funding: ☐Yes ☐No
      * If yes, provide the name of the funder:

No. **If no,** **the remainder of this section does not apply.**

The data is publicly available. **If the data is publicly available a data use agreement is not required and the remainder of this section does not apply.** “Publicly available” refers to data and/or biospecimens that are accessible to anyone in the general public, without the need for special qualifications, permissions, or privileges. Examples include data/biospecimens available for public purchase, searchable online, or available at a library.

Examples of types of identifiable data/biospecimens that are not considered publicly available are as follows:

Data in the electronic medical record;

Social media data labeled as "private" by the data owner, or not readily available without permission of the site Owner/Administrator under the Terms of Service of the site;

Data protected by Copyright; and

Data or biospecimens that have access restrictions (e.g. are only available to clinicians or qualififed researchers or may only be accessed on a secure server.

1. Indicate if the data is incoming, outgoing or both:
2. Provide the name of the entity(s) that data will be transferred/shared with, if incoming:
3. Provide the name of the entity(s) that data will be transferred/shared with, if outgoing:
4. Provide the external entity(s) contact name, email and phone number with whom the data agreement is going to be negotiated and executed with (i.e. Sponsored Projects Office contact or contracts department as applicable). List contact information for each external entity(s) that are involved with the project.

|  |  |  |  |
| --- | --- | --- | --- |
| Contact Name | External Entity | Email | Phone Number |
|  |  |  |  |

1. Who is responsible for transmission of the data (include name, email address and phone number)?

1. Who is responsible for receiving the data (include name, email address and phone number)?
2. Describe how the data will be securely transmitted/shared. If using an externally managed data transfer system, please include details about the system such as the URL for the site and information about who manages the security and maintenance. **Please note data cannot be transmitted/shared without assistance from UNM HSC Central IT.** **Request UNM HSC Central IT transfer from the ISO office at HSC-ISO@salud.unm.edu. This means data cannot be transferred via email, cloud storage services such as Dropbox, OneDrive, and fax.**

UNM HSC Secure File Transfer Protocol (SFTP)

UNM HSC REDCap

Other External Solution, and clarify:

1. For data being received/shared with non-HSC locations or entities, describe the following:
2. Where will data be stored and how will it be protected? UNM HSC requires data storage on the N:\Research -Studies networkd drive (i.e. encryption, password protection, access controls, use of REDCap, etc)? 
   * **If** REDCap, who manages/owns REDCap (i.e. UNM HSC or other external entity)?
   * **If** REDCap or other external system is not UNM HSC REDCap managed/owned, please provide the name and contact information of owner and the access (login) link?

Provide IT security point of contact details for externally managed/owned REDCap:

1. What is the method being used for data collection and storage (i.e. electronic, hard copy, etc.)?
2. How long will the data be stored? Must be congruent with section 16.
3. Who will have access to data?
4. Please list all specific data elements to be sent out (outgoing) and/or received (incoming) in the table below. If there are extensive data elements being shared, please summarize in the table below, and provide the document file name that contains the full list of data elements.

|  |  |  |  |
| --- | --- | --- | --- |
| List Sponsor or Outside Entity | What is the  classification of the data? Please indicate which of the following applies:  De-identified Data;  Limited Data Set;  Protected Health Information  See definitions after question “P”. | List Incoming Data Elements | List Outgoing Data Elements |
|  |  |  |  |
|  |  |  |  |

1. If the research requires the access, use, or disclosure of **any** of the 18 individually identifiable protected health information (PHI) identifiers that can be used to identify, contact, or locate a person (e.g., name, medical record number, etc.), are the subjects going to consent to or authorize the disclosure of their individually identifiable health information?

Yes (If yes, ensure section 25. Consent Process completed)

No. If no, is HIPAA authorization altered or waived? If altered or waived, provide details:

1. Does the request to transfer/share data include clinical data that belongs to the UNM Health System? If data originates from the UNM Health System medical records, this question should be answered “Yes”. Yes No
2. Is the external entity a “covered entity”? (HIPAA-covered entities include health care providers (i.e. hospitals, doctors, academic health centers), health plans, and clearinghouses.): Yes No
3. For outgoing data, is the data that is going to be transferred/shared owned or partially owned by another party? Yes No NA, data is incoming only

If yes, please provide details:

1. Does the data have any restrictions other than HIPAA? Yes No

If yes, please provide details:

1. Does the data include information about substance abuse treatment, sexually transmitted diseases, genetic testing results, HIV/AIDS testing results, and/or mental health?

Yes No

If yes, please provide details:

**DEFINITIONS**

**DE-IDENTIFIED DATA:** Identifiers That Must Be Removed to Make Health Information De-Identified:

(i) The following 18 identifiers must be removed of the individual or of relatives, employers or household members of the individual must be removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; ***and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;*** (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers;(L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code; and (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

**LIMITED DATA SET:** A “limited data set” is a limited set of identifiable patient information as defined in the Privacy Regulations issued under the Health Insurance Portability and Accountability Act (HIPAA). A “limited data set” is information from which “facial” identifiers have been removed. A “limited data set” is information from which “facial” identifiers have been removed. Specifically, as it relates to the individual or his or her relatives, employers or household members, all the following identifiers must be removed in order for health information to be a “limited data set”: names;

street addresses (other than town, city, state and zip code); telephone numbers;

fax numbers; e-mail addresses; Social Security numbers; medical records numbers;

health plan beneficiary numbers; account numbers; certificate license numbers;

vehicle identifiers and serial numbers, including license plates; device identifiers and serial numbers; URLs; IP address numbers; biometric identifiers (including finger and voice prints); and full-face photos (or comparable images).

**The health information that may remain in the information disclosed includes:** dates such as admission, discharge, service, DOB, DOD;

city, state, five digit or more zip code; and

ages in years, months or days or hours.

It is important to note that this information is still protected health information or “PHI” under HIPAA. As a limited data set the information is still subject to the requirements of the federal and state privacy and security regulations.

**PROTECTED HEALTH INFORMATION (PHI):** PHI is defined as any individually identifiable health information collected or created as a consequence of the provision of health care by a covered entity, in any form, including verbal communications. PHI is information that can be linked to a particular person and that is created, used, or disclosed in the course of providing a health care service (i.e., diagnosis or treatment). There are 18 PHI identifiers as listed in the de-identified data definition section.