A DUA Primer

Introduction[1]:

When a ***Covered Entity***[2] collects ***Health Information***[3] in the course of business, much of what it collects from patients is known as ***Individually Identifiable Health Information (IIHI)***[4]. Once that IIHI is committed to any medium or transmitted in any medium it becomes ***Protected Health Information (PHI)***[5]. The HIPAA Privacy Rule establishes the conditions under which PHI may be used or disclosed by Covered Entities (or Hybrid Entities[6]) for research purposes. In general, patient data falls into 3 categories. These categories are:

---

[1] The Office of Civil Rights at the DHHS has an excellent Summary of the HIPAA Privacy Rule.

[2] **Covered Entity** – A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard.

[3] **Health Information** – Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

[4] **Individually Identifiable Health Information (IIHI)** – Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

[5] **Protected Health Information (PHI)** – PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

[6] **Hybrid Entity** – A single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, nonhealth care components of a hybrid entity may be affected because the health care component is limited in how it can share PHI with the non-health care component. The covered entity also retains certain oversight, compliance, and enforcement responsibilities.

Any single legal entity may elect to be a hybrid entity if it performs both covered and noncovered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse. To become a hybrid entity, the covered entity must designate the health care components within its organization. Health care components must include any component that would meet the definition of covered entity if that component were a separate legal entity. A health care component may also include any component that conducts covered functions (i.e., noncovered health care provider) or performs activities that would make the component a business associate of the entity if it were legally separate. Within a hybrid entity, most of the requirements of the Privacy Rule apply only to the health care component(s), although the covered entity retains certain oversight, compliance, and enforcement obligations.

For example, a university may be a single legal entity that includes an academic medical center's hospital that conducts electronic transactions for which HHS has adopted standards. Because the hospital is part of the legal entity, the whole university, including the hospital, will be a covered entity. However, the university may elect to be a hybrid entity. To do so, it must designate the hospital as a health care component. The university also has the option of including in the designation other components that conduct covered functions or business associate-like functions. Most of the Privacy Rule's requirements would then only apply to the hospital portion of the university and any other designated components. The Privacy Rule would govern only the PHI created, received, or maintained by, or on behalf of, these components. PHI disclosures by the hospital to the rest of the university are regulated by the Privacy Rule in the same way as disclosures to entities outside the university.

1. Protected Health Information (PHI) with full identifiers—Identifiable Data.
2. Protected Health Information (PHI) with most identifiers removed—Limited Data Set
3. Patient Data with all identifiers removed—De-identified Data.

Because these categories are distinct and the requirements for disclosure are different for each category, it is important to understand what is in each category and what requirements must be met for a Covered Entity/Hybrid Entity to be able to disclose data that fall within them[7]. It is also important to remember that both an Identifiable Data Set and a Limited Data Set contain PHI, thus they fall under the HIPAA Privacy Rule.

PHI with Identifiers:

Patient data that has identifiers as part of the data set have the most stringent requirements for use and disclosure. Those identifiers are:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
    b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.

[7] It is important to remember that not all individually identifiable health information is PHI. Unless the data was collected by a Covered Entity for the purposes of providing health care/insurance it is not PHI. The HIPAA Privacy Rule is only concerned with PHI.

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.

17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification[8].

Once a data set has any of these identifiers (with the exception of the 3 modified identifiers listed below for Limited Data Sets), it cannot be either a Limited Data Set or De-identified Data and requires more than just a DUA to be able to use and disclose.

The Privacy Rule requires Covered Entities to receive one of the following forms of approval or assurances in order for it to be able to disclose or use fully identified PHI for research purposes:

1. Authorization by Subject[9]
2. Waiver or Alteration of Authorization by an IRB[10]
3. Activities Preparatory to Research[11]
4. Research on PHI of Decedents[12]

HIPAA Authorization:

Of the four types of approvals, this is the most common in the research environment. In fact, Authorization by Subject is the way most clinical trial data is collected and also is common for

[8] This category of identifiers acts as a catch all and requires a holistic or totality of circumstances type of analysis when determining if health information is identifiable. There are circumstances where a condition or other form of information is unique enough that including it in a data set will cause it to remain identifiable to an individual.

[9] The Privacy Rule also permits covered entities to use or disclose protected health information for research purposes when a research participant authorizes the use or disclosure of information about him or herself. Today, for example, a research participant's authorization will typically be sought for most clinical trials and some records research. In this case, documentation of IRB or Privacy Board approval of a waiver of authorization is not required for the use or disclosure of protected health information.

[10] Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an IRB or a Privacy Board. See 45 CFR 164.512(i)(1)(i). This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants' authorization were required.

[11] For preparatory to research work access is only given to PHI for screening purposes. A researcher is not allowed to remove, save, or otherwise use any of the PHI they access for preparatory work. If you have something that is seeking this approval, please consult the Privacy Office.

[12] Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, *and*, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii).

establishing prospective registries. The benefit of a HIPAA Authorization[13] is that it allows for uses and disclosures of PHI not otherwise allowed by the Rule. An authorization is a detailed document that gives Covered Entity permission to use PHI for specified purposes, which are generally other than treatment, payment, or healthcare operations, or to disclose PHI to a third party specified by the individual. Thus, once a subject signs an Authorization the other requirements under the Privacy Rule (such as IRB waiver or a Limited Data Set) are no longer required.

This does not mean that once an Authorization is signed that the data can be freely transferred. The Authorization stipulates what data may be disclosed, to whom the data may be disclosed, and what the data may be used for. Thus, while an Authorization carries many advantages, it does require that the obligations contained in it are enforced by the Covered Entity. We see this in the language used in both the Annotated CTA and the ACTA:

"Sponsor shall own and have the right to use the Data in accordance with the signed informed consent and authorization form, applicable laws, and the terms of this Agreement." (ACTA)

And

"Sponsor shall own and have the right to use or transfer the Data in accordance with the ICF and HIPAA authorization form, applicable laws, and the terms of this Agreement." (Annotated)

IRB Waiver or Alteration:

A waiver of authorization or an alteration of an authorization requires review and approval by an IRB and carries much of the same use and disclose requirement issues as do the Authorization. Once the IRB has reviewed and approved either a waiver or alteration of an authorization, the Covered Entity can use and release PHI for research purposes ***only*** as allowed by the IRB approval. Thus, the same type of protective language used for Authorizations should be utilized for waivers and alterations. The purpose is to affirmatively constrain the use of PHI via contract language with whomever we transfer the PHI to for the purposes of research.

The last 2 allowable uses and disclosures of PHI with Identifiers (Identifiable Data) for research are rarely seen by a contracting office but should be understood by the team members.

Activities Preparatory to Research:

For use and disclosure of PHI under the Privacy Rule for this category, there must be representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is

[13] The HIPAA Authorization and the Informed Consent are 2 separate requirements that are often conflated. The informed consent is the process by which a subject agrees to participate in a clinical trial, or research study, by being provided with all relevant information about the research activity. The informed consent process is documented by the signing of an Informed Consent Form (ICF). The HIPAA Authorization authorizes the release of PHI as specified in the document for research purposes. The HIPAA Authorization and the Informed Consent are often incorporated into the same document, but they have separate requirements and do not cover the same ground. A good description of the required elements of both can be found here.

solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, *and* representation that protected health information for which access is sought is necessary for the research purpose. See 45 CFR 164.512(i)(1)(ii). This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study.

Research on PHI of Decedent:

For use and disclosure of PHI under the Privacy Rule for this category, there must be representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, *and*, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(i)(1)(iii).

Limited Data Sets:

A Covered Entity may still use PHI for research if it doesn't fit into one of the four categories described above, but then the data must be culled of full identifiers into a Limited Data Set[14]. To make PHI acceptable to be released as a Limited Data Set only the following identifiers can be included in the data:

- Dates, such as admission, discharge, service, and date of birth (DOB)
- City, state, and zip code (not street address)
- Any other unique code or identifier that is not listed as a direct identifier.

The following identifiers ***must*** be removed:

- Names
- Street addresses (other than town, city, state, and zip code)
- Telephone and fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/driver's license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs and IP addresses
- Biometric identifiers
- Full face photographic images and any comparable images.

Once a data set has been culled of these identifiers, then this data may be used and disclosed for research under a Data Use Agreement (DUA). The DUA is a way for the Covered Entity to obtain the assurances that the recipient of the Limited Data Set will only use and disclose the data set for very specific purposes.

[14] It is also important to note that even though the number of identifiers has been limited in a limited data set it is still considered PHI.

As the data used in a Limited Data Set was collected for reasons other than research (no Authorization was signed), the Covered Entity is required to have a DUA with all recipients of the Limited Data Set—even with its own employees and members of its workforce[15] who want to use the data for research.

The Privacy Rule requires a DUA for a Limited Data Set contain the following provisions:

1. Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that, if done by the covered entity, would violate the Privacy Rule)[16].

2. Identify who is permitted to use or receive the limited data set.

3. Stipulations that the recipient will.

    a. Not use or disclose the information other than permitted by the agreement or otherwise required by law.

    b. Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the covered entity any uses or disclosures in violation of the agreement of which the recipient becomes aware.

    c. Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.

    d. Not identify the information or contact the individuals.

Under the Privacy Rule, only a Limited Data Set requires a DUA. That said, we have already seen that even with the "Gold Standard" of permission to use PHI for research, a signed HIPAA Authorization, we still need to have other representations made to protect the PHI and ensure compliance with the requirements of the Authorization or the IRB Waiver/Alteration of Authorization. It is important to note that in this instance (Limited Data Sets), the requirements of what must be in the DUA are stipulated by HIPAA and cannot be omitted.

De-Identified Data Sets:

Under the Privacy Rule, de-identified data is ***not*** PHI. Thus it does not need a DUA to use or transfer it for research as HIPAA does not apply to it. That said, almost every US university and research institution requires a DUA for de-identified data (including the Federal Demonstration Partnership—FDP). The reasons for this are pretty simple:

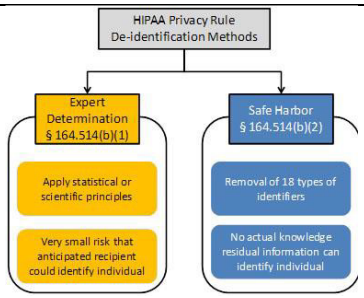
[15] See Pages 15-16 of the DHHS' Booklet "Understanding the Privacy Rule"

[16] If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated the Privacy Rule. If the covered entity providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the covered entity must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the covered entity must discontinue disclosure of PHI to the recipient and notify HHS.

1. The DUA stipulates the ownership of the data set.
2. The DUA can stipulate a time limit on the use of the data set and disposition of the data set at the end of such period.
3. The DUA will often stipulate that if anything other than de-identified data is transferred that the Recipient is to immediately notify the Provider and that the Recipient will follow Provider's reasonable instructions.
4. The DUA will often stipulate that the Recipient not attempt to re-identify any subjects.
5. The DUA often stipulates that the Recipient have all IRB approvals it may need for use of the data.

When reviewing the data elements to be transfer, it is important to make sure that not only none of the PHI identifiers are listed or present, but also to make sure that the 3 allowable identifiers for a Limited Data Set are not present.

HIPAA DATA REFERENCE GUIDE		
Protected Health Information (PHI)—Identifiable Data	**Limited Data Set**	**De-Identified Data Set**
Protected health information (PHI) includes all individually identifiable health information relating to the past, present or future health status, provision of health care, or payment for health care of/for an individual that is created or received by a Covered Entity or Business Associate. Health information is individually identifiable if it contains any of the following identifiers: • Names • Geographic subdivisions smaller than a state • Dates (except year only) directly related to an individual, including birth date, date of death, admission date, discharge date; and all ages over 89 (except ages may be aggregated into a single category of age 90 or older) • Telephone and faxes numbers • Email addresses • Social security numbers (SSN) • medical record numbers (MRN) • Health plan beneficiary numbers • Account numbers	A limited data set is a data set that is stripped of certain direct identifiers specified in the Privacy Rule. A limited data set may be disclosed to an outside party without a patient's authorization only if certain conditions are met. *First*, the purpose of the disclosure must be for research, public health, or health care operations purposes. *Second*, the person or entity receiving the information must sign a **data use agreement (DUA)** with the covered entity or its business associate. **Limited Data Sets may include** only **the following identifiers:** • Dates, such as admission, discharge, service, and date of birth (DOB) • City, state, and zip code (not street address) • Any other unique code or identifier that is not listed as a direct identifier. This means that in order for a data set to be considered a limited data set, all of the following direct identifiers as they relate to the individual or his/her relatives, employers, or household members *must* be removed: • Names • Street addresses (other than town, city, state, and zip code) • Telephone and fax numbers • Email addresses • Social security numbers • Medical record numbers	The Privacy Rule permits a covered entity or its business associate to release data that have been de- identified without obtaining an Authorization and without further restrictions upon use or disclosure because de-identified data is not PHI and, therefore, not subject to the Privacy Rule. A covered entity or business associate may de-identify a data set in one of two methods. The first method, (the "Safe Harbor" method) involves the removal all 18 HIPAA identifiers. In the second method the covered entity formally determines that there is no reasonable basis to believe the data can be used to identify an individual. Under the second method, the "Expert Determination" method, a qualified statistician—using generally accepted statistical and scientific principles and methods—determines that the risk of re-identification of the individual that is the subject of the information is low. The qualified statistician must document the methods and analysis that justify his/her determination. The two de-identification methods provided in the Privacy Rule are illustrated below.

• Certificate/driver's license numbers • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web Universal Resource Locators (URL) • Internet Protocol (IP) addresses • Biometric identifiers (including finger and voice prints) • Full face photographic images and any comparable images • Any other unique identifying number, characteristic, or code. *A Business Associate Agreement (BAA) is required to be entered into between a Covered Entity and/or Business Associate and any downstream Subcontractor(s) that create, maintain, receive, access or store PHI on behalf of a Covered Entity/Business Associate prior to use or disclosure of any PHI. **Consult the University of Arizona Privacy Office (PrivacyOffice@email.arizona.edu) to determine whether your project requires a DUA	• Health plan beneficiary numbers • Account numbers • Certificate/driver's license numbers • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • URLs and IP addresses • Biometric identifiers • Full face photographic images and any comparable images. *A Data Use Agreement (DUA) is required to be entered into between a Covered Entity and/or Business Associate and any downstream Subcontractor(s) or third-party that will receive a Limited Data Set *prior* to use or disclosure of the Limited Data Set. **Consult the University of Arizona Privacy Office (PrivacyOffice@email.arizona.edu) to determine whether your project requires a DUA	 **Consult the University of Arizona Privacy Office (PrivacyOffice@email.arizona.edu) to determine whether your project requires a DUA
For questions or for more information, please contact the UA Privacy Office at P: 520.621.1465 or E: privacyoffice@email.arizona.edu		

Appendix A

Anatomy of a Standard Academic Data Use Agreement (DUA)

While data use terms can come in many forms,[17] there is a fairly common structure to academic DUAs this is worth understanding. The typical academic DUA will have the following 4 parts:

• **Face Page**: This includes the identification of the Parties (Provider and Recipient) and the Provider Scientist and Recipient Scientist, the Project title, the term of the DUA, and (normally) the data type. Additionally, it is in the Face Page where the Terms and Conditions that need to be incorporated into every DUA, regardless of the data type, are located. It is the Terms and Conditions in the Face Page that will normally give rise to the Primary and Secondary Responsibilities of the Investigator (see Appendix B).

• **Attachment 1**: This attachment includes information related to the project specifics. Typically it will include a description of the data being transferred (including PHI, if any), a description of the Project for which use of the data is being authorized, how the data is being transmitted, information regarding reimbursement of costs (if any), and what the Recipients needs to do upon the termination or expiration of the DUA (called the Disposition Requirements). It will be this information that is needed to fill out this Attachment that a University's contract office will interact most with the Investigator. Please see Appendix C below for a better explanation for what is usually required to complete Attachment 1.

• **Attachment 2**: This attachment includes the terms required based on the specific type of information being transferred. Because of the vast amount of different types of data that can be transferred for academic purposes, it is not possible, nor is it practical, to list all of the potential terms that could be in a DUA in the Terms and Conditions contained in the Face Page. Just some of the possible laws that may be directly applicable depending on the type of data being transfer are: the HIPAA Privacy Rule (human subjects data collected for health care); FERPA (Family Education Rights and Privacy Acts of 1974); and the Common Rule (used when there is Personally Identifiable Information as defined by OMB Memorandum M-07-16 that is not covered by HIPAA or FERPA (or some other similar law or regulation). Someone from the Contracts Office will draw your attention to any terms that the Investigator should be aware of.

• **Attachment 3**: This attachment includes information on the involvement of any third party collaborators approved by the Provider.

[17] Data use terms may also be present in many different types of agreements. It is not uncommon to see data use terms in Clinical Trial Agreements, Non-disclosure Agreements, Material Transfer Agreements, Collaborative Research Agreements, and Professional Services Agreements. \

Appendix B

Investigator Responsibilities—Incoming Data

While DUAs are signed by the institution receiving it[18], the Investigator plays a primary role in the administration of the data and thus has some responsibilities. As the DUA exists only because a particular investigator has requested a non-public data set, all DUAs list the Recipient Scientist (the Investigator) and the Project under which the data will be used. Many DUAs also require the Investigator to sign the DUA as "Read and Understood" or "Acknowledged."[19] It is important to note that while the Recipient and Recipient Scientist have been granted access to the data by the Provider, this access is a very limited license and the Provider retains all rights and ownership in the data.

Initial Responsibility

An added nuance that is becoming more common in academia is when the university does not own the hospital where the majority of its medical school faculty practice. In this instance, like with the UA and Banner, there are 2 entities involved and the faculty often wear 2 separate hats—1 hat as a practicing physician (a Banner employee) and one hat as an academic researcher (a UA faculty member). Under HIPAA, the Privacy Rule restricts when information collected for the purposes of providing health care to patients (a Banner function) can be used for research (normally a UA function). Another aspect of HIPAA is that access equals disclosure. So long as a faculty member is accessing the patient information for the purposes of patient care, they are functioning as a Banner employee and no additional agreement is needed. Once a faculty member wants to access patient information (data) for research, and the data will be moved to a UA storage facility (hard drive, cloud device, or even paper) they are functioning in their capacity as a UA faculty member and there must be a DUA in place with the UA prior to accessing (disclosure) the medical records of Banner patients for their research. Thus, the initial responsibility of a UA faculty member wishing to access patient information for research and to move that data to a UA facility/device is to ensure that a DUA is in place before he/she accesses the patient medical record for research purposes and transfers it to the UA.

Primary Responsibilities under an Academic DUA

Once a DUA has been negotiated and signed, typically the only people that will have any access to or interaction with the data is the Investigator and his/her study team. Most DUAs allow the Recipient to use the data solely to conduct the Project and solely by the Recipient Scientist and the Recipient's faculty, employees, fellows, students, and agents that have a need to use, or provide a service in respect of, the data in connection with the Project. Additionally, the Recipient agrees to retain control over the data so that it is not disclosed outside of those allowed to access it for the Project. Finally, DUAs require that the Recipient use the data in compliance all applicable laws and professional standards. These requirements give rise to the Investigator's primary responsibilities under the DUA. Those are:

[18] In almost all DUAs this party is typically called the "Recipient" —in the case of most academic research, that entity is the University.

[19] To be clear, this does not make the Investigator a party to the DUA. The legal entity that bears all responsibility for the breach of the DUA is the Recipient.

1. Use the data only for the Project that is specified by the DUA.[20]
2. Restrict Access to the data to those that have a need to use it.[21]
3. Retain control over the data (this will be elaborated on below when discussing Privacy and Public Records).
4. Use the data only as allowed by law and in a manner that is consistent with any applicable professional standards.

Secondary Responsibilities under and Academic DUA

Aside from the primary responsibilities under a DUA, the Investigator may have secondary responsibilities if he/she decides to publish. Most DUAs require that the Investigator submit any paper or abstract to the data Provider so that it may ensure that the data is appropriately protected. The amount of time prior to submission of a manuscript or abstract to an external party will be specified in the DUA (typically 30 days for a manuscript and 10 days for an abstract). Also, most DUAs allow the Provider to delay a publication for an additional period of time to protect proprietary information. Finally, the Investigator will usually have an obligation to recognize the Provider as the source of the data in accordance with standard scholarly practice. The Investigator's secondary responsibilities are:

1. Submit manuscripts and abstracts to the Provider to ensure data is properly protected per the time periods specified in the DUA.
2. Hold the manuscript or abstracts for an additional period of time as specified in the DUA if Provider identified proprietary information it wishes to protect.
3. Acknowledge the source of the data in all publications that arise from the use of the data

Data-Specific Responsibilities

These Primary and Secondary Responsibilities for the Investigator are typical in most academic DUAs. In addition to these responsibilities, the type of data that the Investigator has requested my generate additional responsibilities. As noted in Appendix A, these will typically be listed in Attachment 2 (commonly: Data-specific Terms and Conditions). Any data-specific terms and conditions that generate an additional responsibility/obligation for the Investigator will be noted to the Investigator by the Contracts Office. If the Investigator is not certain how he/she can comply with this responsibility(ies)/obligation(s), please reach out to the Contracts Office to inquire about compliance.

Privacy and Public Records

Investigators at public institutions often have additional obligations that their colleagues at private institutions do not have. That is true of DUAs for Investigators at the University of Arizona. Because of

[20] With Human Subjects Data, this will often be the IRB approved project. This limitation includes the prohibition on using the data in ways way originally contemplated by the project. Thus, an investigator

[21] These are often defined as the "Recipient Personnel" and the "Collaborator Personnel"—collectively as the "Authorized Persons."

our public records laws, there is always the chance that someone or some entity files a publics records request seeking information about a particular project. To ensure that we protect the privacy of data that may be used to identify individuals, the University has 3 HIPAA Compliant storage options:

1. UA@Box Health Account
2. RedCap
3. HIPAA Environment CRRP

So long as data that is derived from human subjects is stored in one of these then any public records request to access the data within will generate the involvement of either the Privacy Office or the Office of the General Counsel and the Investigator has fulfilled his/her obligation to maintain the data in a secure manner.

If the Investigator does not want to use one of the 3 options listed above, then he/she may contact the Privacy Office to inquire if the device they would like to use will meet our privacy obligations. Contact the Privacy Office at: PrivacyOffice@email.arizona.edu

Appendix C

Attachment 1: Project Specific Information

In the typical academic DUA there is a section that describes the data being transferred, the project, the manner of transfer, costs, and the disposition of the data when the DUA is either terminated or it expires. For the majority of DUA, this is in **Attachment 1**.

Here is a brief description of what is expected to be in each section:

1: Description of the data:

> This section should provide sufficient information such that each party understands the information that will be transmitted under this Agreement. Examples of information that should be provided include:
>
> - Whether the data is obtained from human subjects and, if so, a description of the population included in the data (ie—what are the specific data points being requested).
> - The number of subjects and/or experiments included.
> - Name of the study that the data was obtained under.
>
> If there is a particular study that needs to be acknowledged/cited as the source of the data, this information should be included here.

For a Banner DUA, in addition to the general description of the data, Banner requires a list of any Protected Health Information (PHI) as defined by HIPAA that is being requested (Section 1b in the email from the Contracts Office). Banner also requires that the Investigator specify how he/she will be accessing the data (Section 1c. in the email from the Contracts Office). This would also be a good place to indicate how the Investigator intends to store the data while it is in his/her possession.

2: Description of the Project:

> This section should provide sufficient information such that each party understands the project that the Recipient will perform using the data. The content of this section will be very similar to the Statement of Work used in other types of Agreements. Examples of information that should be provided include:
>
> - Objective or purpose of the Recipient's work.
> - A general description of the actions to be performed by the Recipient using the Data and possibly the anticipated results (This can be the Project Summary from your IRB application if applicable).
> - Include whether or not you intend to link the data with other data sets.

3: Provider Support and Data Transmission:

This will explain how the data will be sent. Almost all data is transmitted electronically now. If not, please specify the physical address the data should be sent to.

This section will also explain any additional support the Recipient can expect to get from the Provider for the use of the data. This will be filled out by the Provider unless the Recipient needs to specify what special assistance will be needed to use the data being requested. Examples of this could be:

- Format of Data
- Provision of Data dictionary
- Availability of Provider to assist Recipient in understanding the Data structure (e.g. variables, code lists, etc.)
- If/how Data will be revised and resent if errors are found by the Recipient
- Specific instructions necessary to complete the transfer of the Data, if available/appropriate, and any support supplied by the Provider for the transfer.

4: Reimbursement Costs:

Some data Providers charge a fee for their data (though most academic Providers do not unless there are very special circumstances). If there are costs, then payor/payee info must be provided.

5: Disposition Requirements upon the termination or expiration of the Agreement:

This section will be filled in by the Provider and gives instructions on what the Recipient must do with the data when the DUA is either terminated or expires.

Appendix D

Attachment 3: Identification of Permitted Collaborators

Not all research is done solely by the Recipient PI and his/her study team. Sometimes they have external collaborators or those that are not employees of the Recipient institution. Because this is how a fair amount of research is conducted, most DUAs have the following term in it:

> Recipient shall not use the Data except as authorized under this Agreement. The Data will be used solely to conduct the Project and solely by Recipient Scientist and Recipient's faculty, employees, fellows, students, and agents ("Recipient Personnel") and Collaborator Personnel (as defined in Attachment 3) that have a need to use, or provide a service in respect of, the Data in connection with the Project and whose obligations of use are consistent with the terms of this Agreement (collectively, "Authorized Persons").

In Attachment 3, collaborator personnel is typically defined as:

> "Collaborator Personnel" means: faculty, employees, fellows, or students of an academic institution, which institution (i) has agreed to collaborate in the Project, (ii) has faculty, employees, fellows, or students who have a need to use or provide a service in respect of the Data in connection with its collaboration in the Project, and (iii) has executed an agreement that is substantially similar to this Agreement.

In most instances, where Collaborator Personnel are identified in a DUA, the Recipient getting the data and sharing it with its collaborators will require the collaborator to sign a DUA with the Recipient that have the identical terms are those signed by the Recipient.

Attachment 3 was created to allow the Provider the option to authorize Collaborator Personnel (individuals who are employed by another organization and are not under direct control of the Recipient, and who, by nature of their participation in the Project, need to have access to the Data) to access the data via the Recipient. These individuals might include, for example, those affiliated with another entity that also has a DTUA with your organization for this project (multi-site project), a visiting professor working at the Recipient while on sabbatical, or individuals at an institution that might receive only a portion of the Data from the Recipient under conditions that would not require a separate DTUA.

In most instances, the level of specificity for who must be named as a collaborator will be determined by the project. Typically, a collaborator does not need to specify each individual at its organization that will

have access to the data as the collaborator's institution will have entered into a DUA and under their DUA they become the Recipient and their employees become the Recipient Personnel as defined above.

While this may seem like an overly complicated process, it is necessary to demonstrate in the case of a HIPAA audit by the HHS OIG that the Provider has not only protected the data as required under law, but that it also has ensured that the protections follow the data wherever it may be transferred for the purposes of the Project.