**Data Management & Security Plan**

A data management and security plan is a formal document that describes what you will do with your data throughout the study life cycle. Many funding agencies, including the NIH, require a data management plan as part of the application process and it is best practice to include this plan with non-funded research studies, as well. The completed form, once approved, will be the official **Data Management & Security Plan (DMSP)** for the study protocol. This plan should comprehensively describe the access, use, and sharing of data and/or biospecimens throughout the life cycle of the study. Consider the DMSP a “living” document and as such, changes to this plan will require that a revised form be submitted for review to the UVM Research Protections Office (UVM RPO) to ensure that it still satisfies the requirements of your study.

***Why is this information needed?*** The UVM RPO, in collaboration with the University of Vermont Health Network (UVMHN), has created this DMSP with the goal of consolidating information required sections of the DMSP:

[**1 – STUDY TITLE, LEADS & TEAM**](#_1_–_STUDY)

*Identifies the primary individual(s) responsible for the study and training of the study team, as well as their role(s) and relationship(s) to the institutions.*

[**2 – DATA SOURCE/CUSTODIAN**](#_2_–_DATA)

*Defines the source or custodian of the data and/or biospecimens being collected, helping to establish the conditions under which the data can be used or disclosed for research*

[**4 – STORAGE & SECURITY**](#_4_–_STORAGE)

*Inquires as to the safeguards that are in place to protect the privacy of individually identifiable information, as well as the security and integrity of institutional systems*

 collects details about the source or custodian of the data or biospecimens accessed for the study which will dictate the IRB review and/or HIPAA-compliant pathway.

[**3 – DATA SETS**](#_3_–_DATA)

*Distinguishes the types of data sets that will be created/derived over the course of the study which will dictate the type of IRB review and/or HIPAA-compliant pathway*

 collects details about the source or custodian of the data or biospecimens accessed for the study which will dictate the IRB review and/or HIPAA-compliant pathway.

[**5 – DATA SHARING**](#_5_–_DATA)

*Facilitates the formal documentation of any data sharing activities in accordance with relevant regulations so that data/biospecimens will not be misused.*

[**6 – RETENTION & DISPOSAL**](#_6_–_RETENTION)

*Ensures the justifiable retention or proper destruction of identifiable data/biospecimens after completion of the study, all in accordance with institutional policies & procedures*

**Helpful Resources**

[Helpful Resources](#_Helpful_Resources_1) can be found at the end of this document. A [Glossary](#_Glossary_1) has been included to provide definitions and other information related to specific terms used throughout the DMSP. Also included are [Links](#_Links_1) to relevant institutional policies & procedures, as well as external websites, to provide guidance when completing the DMSP.

**Instructions for completing the DMSP:**

# **1 – STUDY TITLE, LEADS & TEAM**

Below you will find the six sections that comprise the DMSP, as described on page 1. Please complete all relevant fields under each of the six sections. Refer to [Helpful Resources](#_Helpful_Resources_1) for guidance.

* 1. **Version Date** Click or tap to enter a date.
	2. **Study Title** Click here to enter the study title.

**1.3** **Principal Investigator (PI)**

**1.3.1 Contact Information**

Name Click here to enter the PI name.

Email Click here to enter the PI email.

Department Click here to enter the PI department.

**1.3.2 PI’s Role (Select all that apply)**

[ ]  UVM Faculty or Employee

[ ]  UVMHN Employee Click here to select from list:

[ ]  Student/In-Training Click here to select from list:

[ ]  Other - Describe Click here to describe the PIs other role.

**1.4 Faculty Sponsor**

[ ]  **Not Applicable – Skip to 1.5 Training for the Study Team**

**1.4.1 Contact Information**

Name Click here to enter the faculty sponsor name.

Email Click here to enter the faculty sponsor email.

Department Click here to enter the faculty sponsor department.

**1.4.2 Faculty Sponsor’s Role (Select all that apply)**

[ ]  UVM Faculty

[ ]  UVMHN Employee Click here to select from list:

**1.5 Training on the DMSP for the Study Team.** Describe the plan to train the study team regarding implementation of this DMSP, and how this training will be updated and documented as the plan changes over the life cycle of the study.

Click here to describe the training plan.

To ensure all proper approvals are in place, please specify below the source or custodian through which the study data and/or biospecimens will be collected (check all that apply*).* For UVMHN data, complete Section 2.1.1; a separate ***Accounting of Disclosures*** form is required when Protected Health Information (PHI) will be disclosed.Refer to the [Glossary](#_Glossary_1) for the definition of a ‘Data Custodian’ and ‘Disclosure’, and the [Links](#_Links_1) section for ***UVMHN Privacy32 Policy*** and ***HIPAA Privacy Rule Accounting of Disclosure*** relating to disclosures of PHI.

# **2 – DATA SOURCE/CUSTODIAN**

* 1. **UVM or UVMHN (originating from any affiliate) Source/Custodian (check all that apply)**

[ ]  **Not Applicable** (i.e., the study data is originating from a source outside of UVM or UVMHN)

[ ]  **Study team will access data directly** (e.g., from subject [verbal or written]), or via chart review of the electronic health record.

[ ]  **UVMHN Data Management Office (DMO)**

[ ]  **Data/Biospecimens Repository:**

 *PI Name* Click here to enter the name.

 *Protocol Number* Click here to enter the repository protocol number.

[ ]  **Other** – Describe the UVM or UVMHN source/custodian, and if available, provide the name of the Data Owner that authorized access to the data and/or biospecimens for this research (i.e., the individual responsible for dictating practice decisions or authorizing access to the data). Refer to the [Glossary](#_Glossary_1) for the definition of a ‘Data Owner’.

 Click here to enter other institutional sources.

* + 1. **Disclosure of UVMHN PHI.** Specify if you will be disclosing UVMHN PHI. The HIPAA Privacy Rule requires that there must be an accounting of each disclosure including repeated disclosures; this is relevant for the initial study and any study modifications when the following three criteria apply to a research study (Note: An accounting of disclosures is not needed when the research participant has signed an authorization):
* PHI will be disclosed by the investigator **AND**,
* the research disclosure involves at least 50 records (i.e. 50 unique patients/subjects) **AND**,
* either provisioning of access to the PHI has been approved by an IRB/Privacy Board through a HIPAA Waiver of Authorization, **OR** the research utilizes information for a population explicitly defined as requiring records for deceased individuals only

[ ]  **Not Applicable - Skip to 2.2**

[ ]  **Yes - UVMHN PHI will be disclosed**. Completion of the ***Accounting of Disclosures of Protected Health Information (PHI)*** form is required when a disclosure is made. Refer to the [Links](#_Links_1) section for the IRB Forms Library link. This completed form must be submitted separately to DataGovernance@UVMHealth.org to ensure details of the disclosure for an initial study and/or study modifications is accurately recorded. Note, this process is independent of IRB approval.

* 1. **Non-UVM/UVMHN Source/Custodian**

[ ]  **Not Applicable**

[ ]  **Yes** - Describe Non-UVM/UVMHN Source/Custodian, and if available, provide the name of the Data Owner that authorized access to the data and/or biospecimens for this research (i.e., the individual responsible for dictating practice decisions or authorizing access to the data). Refer to the [Glossary](#_Glossary_1) for definitions.

Click here to provide description

A ‘Data Set’ can include the terms data, information and biospecimens. Indicate and describe all the type(s) of data set(s) that will be collected, derived, and utilized at any point over the course of this study; this includes any data collected through the research that will be stored onsite, with a sponsor and/or a third party. Refer to the [Glossary](#_Glossary_1) for definitions of a ‘Limited Data Set’, ‘Coded Data Set’ and ‘De-Identified Data Set’.

# **3 – DATA SETS**

* 1. **Type of Data Set be collected, derived or utilized at any point during this study (Check all that apply)**

[ ]  **Data set contains direct identifiers***.* This may include but is not limited to the following forms of data: personally identifiable information (PII) or protected health information (PHI), e.g., a name, student address on educational record, medical record number, social security number, participant study ID or other unique identifier.

[ ]  **Data set contains indirect identifiers, thus meeting the criteria for a Limited Data Set.** A Limited Data Set can include indirect identifiers, e.g., dates more specific than the year and some components of address.

[ ]  **Data set is coded**, i.e., a coding scheme is applied that can be used to directly link the information to an individual. Will a master key to the code be retained to allow for re-identification of individuals?

[ ]  No

[ ]  Yes – Describe how the master key will be stored separately from the study data.

 Click here to provide a description.

[ ]  **Data set is de-identified**. All direct and indirect identifiers and any codes that could be used to link the information to specific individuals are removed from the data set.

* 1. **Process Used to Collect/Derive the Data Set(s) selected in 3.1.** Please describe the process used to create or derive any study data sets, such as for analysis or for data sharing with collaborators since this will dictate the type of IRB review and/or HIPAA-compliant pathway. For example, describe if, at any point in the study, you will be deriving a limited, coded, or de-identified data set from an initial data set containing direct identifiers.

Click here to provide a description.

Describe the data storage method, location, and security for protecting the study data (complete all that apply). Be sure to indicate whether resources are institutionally provided, or sponsor provided. Note: This section is not seeking information about billing/financial reconciliation processes or data. Refer to the [Helpful Resources](#_Helpful_Resources_1) for applicable guidance.

# **4 – STORAGE & SECURITY**

* 1. **Biospecimens or Data Stored on Physical Mediums** (e.g., written questionnaires/surveys, paper source documents, microfilm, or radiology imaging). Note that if you scan paper forms, including consent forms, these would be considered electronic files.

[ ]   **Not Applicable – Skip to 4.2 Data Stored Electronically**

* + 1. **Location.** Specify where the biospecimens or physical mediums will be stored (include institution name/department & building name).

Click here to provide a description.

* + 1. **Security.**  Describe the security measures for the stored biospecimens or physical mediums, taking into consideration the following: *How will the data/biospecimens be protected against inappropriate use or disclosure, or accidental loss or destruction (e.g., locked research coordinator office in UVM Given Building, locked freezer in UVM research laboratory)? Who will have access to the securely stored data/biospecimens and how will access be granted? If creating or collecting data in the field, how will you ensure its safe transfer into your main secured system(s)?*

Click here to provide a description.

* 1. **Data Stored Electronically**

[ ]  **Not Applicable – Skip to 5 – DATA SHARING**

* + 1. **Internal or External Server.** Indicate which server you will be using to store your electronic data (check all that apply).

[ ]  **UVM**

[ ]  **UVM LCOM**

[ ]  **UVMHN** – It is not permitted to store electronic data within UVMHN systems that is generated by an external source (i.e. from UVM, including UVM LCOM, or any entity or system outside of UVMHN); all data stored within UVMHN systems must originate from a UVMHN source or system. Refer to the [Glossary](#_Glossary_1) for the definition of ‘External Data Source’.

[ ]  **Other** (e.g., data stored through sponsor-provided electronic data capture)

 Click here to provide a description.

* + 1. **Location**. Specify the storage location of the electronic data (check all that apply). Please note that institutional servers are the preferred storage locations.

[ ]  **IT-approved server, shared folder, or cloud-based service.** Identify which drive, IT-approved server, or cloud-based service will be used; provide the server’s name at a minimum (and full pathway if possible) for storing each data set and master key described above in **Section 3 – DATA SETS**. UVMHN permits storage within Microsoft OneDrive or SharePoint or on the S-Drive. For guidance on UVM storage, refer to [UVM Enterprise Technology Service Catalog – Backup & Storage](https://www.uvm.edu/it/catalog/services/category/backup-and-storage). See the [Helpful Resources](#_Helpful_Resources_1) section for guidance.

 Click here to provide a description.

[ ]  **Local drive or removable media, e.g., thumb drive, external hard drive, DVD/CD, other.** Note: This is not a recommended storage option. Choose this only if there is no viable alternative. Identify which mobile storage device will be used and describe why this is your choice and why an institutionally-provided storage location will not work for your process. Digital storage devices and media that contain protected data must be encrypted, and any written records of encryption passwords must be secured in locked storage. Refer to UVMHN policies in the [Helpful Resources](#_Helpful_Resources_1) section for guidance.

Click here to provide a description.

[ ]  **Online application, mobile app, portal, gateway or institutional or sponsor-provided electronic platform.** List the name of the provider or administrator and name of the application, portal, gateway, or device (e.g., REDCap or FDA-compliant REDCap, Qualtrics, MTurk).

Click here to provide a description

[ ]  **Smart device.** Identify any Smart devices (e.g., Fitbit, smart phone, Apple Watch). Include information on the device, the type of data collected, any concerning information from the terms of service, how the data will be uploaded to a central system and what that central system is.

Click here to provide a description.

[ ]  **Audio/video recordings, photographs and/or other medical images.** Identify any recording/imaging (e.g., retinal scans, MRI, CT, X-rays). Indicate what the items are, how they will be collected, where they will be stored and whether these items will be identifiable, coded, or other.

Click here to provide a description.

[ ]  **Interactive medical or research device.** Identify any medical devices (e.g., pacemaker, electronic pill dispenser). Indicate what the items are, how they will be collected and whether these items will be identifiable, coded, or other.

 Click here to provide a description.

[ ]  **Other - Describe**

 Click here to provide a description.

* + 1. **Security.** Describe how you will ensure the proper protections are in place for your data by answering the following questions. These questions refer to the study data, we are not referring to security practices for billing data or the security procedures for sponsor-associated data dictated by the sponsor’s protocols.
* How will the data be protected against inappropriate use or disclosure, or accidental loss or destruction (e.g., encryption, password protection, management of multiple files in separate folders)?

Click here to provide a description.

* + - * + Who will have access to the data files and the master key, and/or applications, portals, gateways, or SMART devices and how will the access permissions be granted/maintained?

Click here to provide a description.

This section pertains to the sharing of research data and/or biospecimens with the study sponsor/funder and/or individuals other than UVM/UVMHN key personnel. Refer to [Helpful Resources](#_Helpful_Resources_1) for guidance.

# **5 – DATA SHARING**

[ ]  **Not Applicable – Skip to 6 – RETENTION & DISPOSAL**

* 1. **Sharing Identifiers.** Will you include direct identifiers (i.e., PII or PHI) or indirect identifiers (i.e., Limited Data Set or Coded Data Set) with the data that you will be sharing?

[ ]  **No** **–** Skip to **5.3 External Data Sharing Plan**

[ ]  **Yes –** Specify what type of identifiers will be shared and provide a justification for sharing direct or indirect identifiers outside of key personnel.

 Click here to provide the identifiers and justification.

* 1. **Data Sharing Agreements.** Sharing data with an individual or entity outside of UVM and/or UVMHN (as applicable) will require a data sharing agreement, e.g. Data Use Agreement. All research contracts/agreements and grant applications for awards of external funding must be reviewed and approved centrally by either UVM Sponsored Project Administration ([SPA](https://www.uvm.edu/spa)) or the UVM Medical Center’s Office of Clinical Trials Research ([OCTR](https://www.med.uvm.edu/clinicaltrials/regulatoryinfo)), as per policy.

**5.2.1 Indicate below where you will seek support to execute the appropriate data sharing agreement(s):**

[ ]  [OCTR](https://www.med.uvm.edu/clinicaltrials/regulatoryinfo) will be helping me with clinical trial contracting, including required data sharing/use agreements.

[ ]  [SPA](https://www.uvm.edu/spa) is completing grant paperwork, which will include required data sharing/use agreements.

**5.2.2** **If the study requires a data sharing agreement, at what time point do you intend to share the data?**

[ ]  **Throughout the course of the study**

[ ]  **At the end of the study**

[ ]  **Other** – Provide the anticipated date of initial data sharing

 Click or tap to enter a date.

**5.3 External Data Sharing Plan.** Indicate and describe the plan for external data sharing by completing all relevant sections below:

* + 1. **External Data Sharing with Individuals or Institutions other than Key Personnel or Study Sponsor/Funder.**

[ ]  **Not Applicable – Skip to 5.3.2** **External Data Sharing with Study Sponsor and/or Funder**

* **Name & address of recipient institution.** If more than one, provide all.

Click here to enter the name and address.

* **Name of external recipient(s); specify the recipient scientist**

Click here to enter the name.

* + - **Describe the data sharing/storage plan including the website/URL of the external data sharing service** (e.g., shared via Electronic Data Capture (EDC), securely transferred using an SFTP, accessed via a secure shared folder, exported from REDCap, or FDA Part 11-compliant REDCap in de-identified format). UVMHN permits external file sharing using guest access to Microsoft OneDrive, Microsoft SharePoint Online, & Microsoft Teams, or UVMHN GoAnywhere file transfer (see [Helpful Resources](#_Links_1)); for UVM file transfer, refer to the link for [UVM File Transfer Service](#_Links_1). If you have a written SOP, you can copy/paste the information below.

Click here to provide a description.

* + - **Expiration date for sharing of study data (if known)**

Click here to enter the expiration date.

* + - **Name of entity preparing the data sharing agreement (e.g., OCTR or external entity such as sponsor)**

Click here to enter the name.

* + 1. **External Data Sharing with Study Sponsor and/or Funder**

[ ]  **Not Applicable – Skip to 6. RETENTION & DISPOSAL**

* **Sponsor name, institution, and address.** If more than one, provide all.

Click here to enter the name, institution and address.

* **Name of external recipient(s); specify the recipient scientist**

Click here to enter the name.

* + - **Describe the data sharing/storage plan including the website/URL of the external data sharing service** (e.g., shared via Electronic Data Capture (EDC), securely transferred using an SFTP, accessed via a secure shared folder, exported from REDCap, or FDA-compliant REDCap in de-identified format). UVMHN permits external file sharing using guest access to Microsoft OneDrive, Microsoft SharePoint Online, & Microsoft Teams, or UVMHN GoAnywhere file transfer (see [Helpful Resources](#_Helpful_Resources_1)); for UVM file transfer, refer to the link for [UVM File Transfer Service](#_Links_1). If you have a written SOP, you can attach or copy/paste the information below.

Click here to provide a description.

* **Name of the Entity (i.e., Sponsor, Funder, or Institution) preparing the data sharing agreement between the local investigator and the Sponsor or Funder**

Click here to enter the name.

* 1. **Local Data Retention Plan**. Do you intend to retain the research data and/or biospecimens once the protocol is complete? This section refers to data retained locally; we are not inquiring about the sponsor/funder-specific requirements for retaining study data. A list of requirements for the retention of research data is described in the UVM Record Retention Schedule and can be accessed via the UVM Office of Compliance and Privacy Services website; see [Helpful Resources](#_Helpful_Resources_1).

# **6 – RETENTION & DISPOSAL**

[ ]  **No – Skip to 6.2 Data Destruction Plan.** Note, if you select ‘No’, you must ensure the study is compliant with the requirements as dictated by the Sponsor, Funder and/or associated institutional guidelines & policies.

[ ]  **Yes - Provide the following information below:**

* + 1. **Reason for Retaining the Data/Biospecimens (check all that apply):**

[ ]  **As a basis for similar or related future research conducted by the local PI**

Click here to provide a description.

[ ]  **As a resource for other investigators.** If the intention is to have the data/biospecimens be a resource for other investigators, the data/biospecimens should be moved into a repository where rules for future release are in place.

[ ]  **As a sponsor, contractual, legal, or regulatory requirement**

Click here to provide a description.

[ ]  **Other**

 Click here to provide a description.

* + 1. **Archiving the Data/Biospecimens.** If you intend to archive the data/biospecimens in a repository, provide below IRB repository number:

[ ]  **Not Applicable**

[ ]  **Not Yet Submitted**

[ ]  **Repository Number** Click here to provide the number.

* + 1. **Retaining Identifiers.** Do you intend to retain identifiers of any kind including direct, indirect, or coded?

[ ]  **No - Skip to 6.2 Data Destruction**

[ ]  **Yes - Provide the following information below:**

* **Justification for why identifiers will be retained**

Click here to provide a description.

* **Type of data set(s) (i.e., Limited Data Set, Coded Data Set) that will be retained**

Click here to provide the type of datasets.

* **Describe where the data will be physically stored long term. If you have a written SOP, you can attach or copy/paste the relevant section here.**

Click here to describe the long term storage.

* **Length of time the identifiers will be retained**

Click here to describe the retention time.

* **Acknowledgement of identifier retention.** If you intend to maintain identifiers, any subsequent secondary analysis after protocol closure requires prior IRB review and approval. Please acknowledge this requirement by checking below.

[ ]  **I understand subsequent data analysis requires prior IRB review and approval.**

* 1. **Data Destruction Plan**. Describe your destruction plan for all identifiable data or biospecimens (i.e., while the protocol is active and once the protocol is complete or identifiable information is shared via a data sharing agreement). If you have a written SOP, you can attach or copy/paste the information below.

Click here to describe the plan.

# **Helpful Resources**

## **Glossary**

This glossary represents a select list of definitions and information to provide guidance within this DMSP. This information is based on [UVM Research Protections Office IRB Policies & Procedures (Section 29)](https://www.uvm.edu/rpo/irb-policies-and-procedures), [Glossary of NIH Terms](https://grants.nih.gov/grants/glossary.htm) and the [NIH Toolkit Glossary](https://toolkit.ncats.nih.gov/glossary/), [National Institute of Standards & Technology Glossary](https://csrc.nist.gov/glossary), [Payment Card Industry Security Standards Council Glossary](https://www.pcisecuritystandards.org/glossary/) and the [U.S. Department of Health & Human Services](https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html).

**Coded Data Set -** Identifying information that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a number, letter, symbol, or combination thereof and a key to decipher the code exists that would enable linkage of the identifying information to the data or biospecimens. Coded data sets are not considered “de-identified” when the “code” is the study subject number.

**Covered Entity** – Health plans, health care clearing houses and health care providers who transmit electronic health information.

**Data Custodian -** Individuals who will have actual possession of the data files or biospecimens, and who will be responsible for observance of all conditions of use, including the establishment and maintenance of security arrangements to prevent unauthorized use.

**Data Owner –** The individual/organization responsible for definitions, policies, and practice decisions about data within their area of responsibility. Data Owners may delegate some of their authorities (e.g. administration of data management policies, authorization of data use) to other administrators or stewards of the data and/or biospecimens.

**Data Set** – A dataset is a structured collection of data generally associated with a unique body of work.

**De-Identified Health Information -**Health information that has been stripped of all 18 identifiers, related to the patient and the patient’s relatives, employers, and household members, as defined by the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA), the releasing entity has no 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. Importantly, in small populations (including small states such as Vermont), characters Data sets may also be de-identified within the meaning of HIPAA using an “expert determination,” however this method is unusual in the context of research. De-identified health information is not protected by HIPAA, and therefore is not subject to its regulations. However, UVM/UVMHN policy may still require appropriate data sharing agreements.

|  |
| --- |
| **18 HIPAA Identifiers** |
| 1. Names | 10. Certificate/license numbers |
| 2. All geographic subdivisions smaller than a state\* | 11. Vehicle identifiers & serial numbers, license plate numbers |
| 3. Telephone numbers | 12. Device identifiers and serial numbers |
| 4. Fax numbers | 13. Web Universal Resource Locators (URLs) |
| 5. Electronic mail addresses | 14. Internet Protocol (IP) address numbers |
| 6. Social Security numbers | 15. Biometric identifiers, including finger and voice prints |
| 7. Medical record numbers | 16. Full face photographic images and any comparable images |
| 8. Health plan beneficiary numbers | 17. All elements of dates (except year)\*\* |
| 9. Account numbers | 18. Any other unique identifying number, characteristic or code |

*\* 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.*

*\*\* 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.*

**Direct identifiers -** An identifier that links to one specific person, can be used by itself to identify the person (e.g., name, social security number, medical record number, medical device number, email address).

**Disclosure –** Disclosure of PHI refers to the release, transfer, access to, or divulging of information in any other manner outside the entity that maintains the information (e.g. REDCap or other UVM systems, research collaborators external to UVMHN). In contrast, use of PHI refers to the sharing, employment, application, utilization, examination, or analysis of the information within the entity that maintains the information. The Privacy Rule issued under HIPAA (Health Insurance Portability & Accountability Act) requires that investigators conducting a research study that utilize PHI must account for all disclosures of PHI when specific criteria applies. Per HIPAA and as noted within [UVMHN Privacy32 Policy](#_Links_1), upon request from an individual, a written accounting of disclosures of PHI made within the six years prior to the request must be provided for disclosures to and by business associates for purposes other than treatment, payment, and health care operations. Research disclosures of de-identified or limited data sets, and disclosures for research made pursuant to an authorization do not need to be included in the accounting. HIPAA’s Privacy Rule requires that there must be an accounting of each disclosure including repeated disclosures, this is relevant for each initial study and/or study modification when the following three criteria applies to a research study:

* PHI will be disclosed by the Investigator. Note, PHI obtained through a review preparatory to research is not to be removed (disclosed) from UVMHN IT systems, **AND**,
* The research disclosure involves at least 50 records (i.e. 50 unique patients/subjects), **AND**,
* Either provisioning of access to the PHI has been approved by an IRB/Privacy Board through a HIPAA Waiver of Authorization, OR the research utilizes information for a population explicitly defined as requiring records for deceased individuals only.

**External Data Source -** Electronic data/information that is generated by, or originates from, a source or system that exists outside the secure UVMHN electronic systems. External data includes but is not limited to:

* Data originating from UVM and LCOM as these systems are external to UVMHN systems
* Data generated from collaborations through the UVMHN/UVM partnership, and collaborative or multi-site studies containing UVMHN data in combination with externally sourced data
* Data that is subject to regulations and protections other than HIPAA (e.g., Federal Education Rights and Privacy Act (FERPA), General Data Protection Regulation (GDPR)). Such data must reside outside UVMHN (e.g., LCOM, VACC) provided these systems are compliant with applicable regulations which may include HIPAA security & privacy rules.

**HIPAA Privacy Rule -** The HIPAA Privacy Rule for the conduct of research (45 CFR 164.501) establishes the conditions under which protected health information may be used or disclosed by covered entities for research purposes.Refer to [HHS.gov](#_Links_1) for additional information regarding the conduct of research.

**Indirect Identifiers** – An identifier that does not link to one specific person but can be used in combination with other information to identify a person (e.g., dates including dates of birth, dates of death, zip codes, cities, counties).

**Limited Data Set (LDS) -** Protected health information that excludes direct identifiers of individuals, and their relatives, employers, or household members, including:

|  |
| --- |
| **Direct Identifiers that Must be Removed from Limited Data Sets** |
| 1. Names | 9. Account numbers  |
| 2. Postal address information, other than town, or city, state and zip code | 10. Certificate/license numbers  |
| 3. Telephone numbers | 11. Vehicle identifiers & serial numbers, license plate numbers  |
| 4. Fax numbers | 12. Device identifiers and serial numbers  |
| 5. Electronic mail addresses | 13. Web Universal Resource Locators (URLs) |
| 6. Social Security numbers | 14. Internet Protocol (IP) address numbers  |
| 7. Medical record numbers | 15. Biometric identifiers, including finger and voice prints  |
| 8. Health plan beneficiary numbers | 16. Full face photographic images and any comparable images |

Limited data sets contain indirect identifiers and therefore are not considered to be de-identified. Specifically, limited data sets may include dates more specific than the year and geographic information including town, city, state and zip code. Research relying on data from a limited data sets does not require IRB review and approval. However, the process for creating the limited data set, may be considered human subjects research and require IRB review.

**Protected Health Information (PHI)** - Individually identifiable health information, regardless of format, that is collected by a Covered Entity and relates to the past, present, or future physical or mental condition of a patient, the provision of healthcare or past, present, or future payment for the provision of healthcare. Protected health information can include demographic information (such as names, email addresses, telephone numbers) as well as information relevant to a person’s health such as dates of disease onset, testing, treatment, a particularly rare health condition, rash, birthmark, or any other information that could be used to identify the patient (or members of the patient’s family, employer and others who live in the patient’s household. Protected health information excludes individually identifiable health information in (i) Education records covered by the Family Educational Rights and Privacy Act (FERPA); (ii) 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; however, those records are covered by other privacy laws and requirements. Additionally, data generated by a Part 2 entity (federally assisted entities that hold themselves out as providing and do provide substance use disorder treatment) are protected by heightened privacy rules set forth in separate regulations. The University of Vermont Health Network has two Part 2 programs—UVMMC’s Addiction Treatment Program and UVMMC’S DayOne Program.

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

**Payment Card Industry Data (PCI**) – Includes cardholder data that may appear in the form of the full PAN (Primary Account Number) plus any of the following: cardholder name, expiration date and/or service code. PCI may also include Sensitive Authentication Data that is security-related information including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks used to authenticate cardholders and/or authorize payment card transactions.

**Sensitive Information** - Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

## **Links**

**U.S. Department of Health & Human Services:**

* [HHS.gov](https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html)
* [HIPAA Privacy Rule Accounting of Disclosures](https://www.federalregister.gov/documents/2011/05/31/2011-13297/hipaa-privacy-rule-accounting-of-disclosures-under-the-health-information-technology-for-economic)
* [NIH Data Management & Sharing Policy](https://sharing.nih.gov/data-management-and-sharing-policy)

**UVM Resources, Policies & Procedures:**

* [UVM File Transfer Service](https://filetransfer.uvm.edu/)
* [UVM Enterprise Technology Services Catalog](https://www.uvm.edu/it/catalog/services/category/backup-and-storage)
* [UVM Privacy Policy](https://www.uvm.edu/sites/default/files/UVM-Policies/policies/privacy.pdf?t=r7f13a)
* [UVM IS Policy](https://www.uvm.edu/sites/default/files/UVM-Policies/policies/infosecurity.pdf?t=r6y1cu) & [UVM IS Procedures](https://www.uvm.edu/sites/default/files/UVM-Policies/policies/infosecurityprocedures.pdf)
* [UVM Research Protections Office IRB Policies & Procedures](https://www.uvm.edu/rpo/irb-policies-and-procedures)
* [UVM Research Protections Office IRB Forms Library](https://www.uvm.edu/rpo/uvmclick-irb-forms-library)
* [UVM Office of Compliance & Privacy Services](https://www.uvm.edu/compliance/compliance/record_retention_schedule)

**UVM Health Network Resources, Policies & Procedures**

 **File sharing:** Note that these platformsmust be accessed through the UVMHN Intranet

* [UVMHN Add Guest to Microsoft Teams/Sharepoint/OneDrive](https://uvmhealth.service-now.com/sp?id=sc_cat_item&table=sc_cat_item&sys_id=730ba9b887505d50c034a8ad3fbb35a2) (Add guest user from outside UVMHN)
* [UVMHN GoAnywhere File Transfer](https://uvmhealth.service-now.com/sp?id=sc_cat_item&sys_id=e50d964bdb590150b702ec95ca9619eb&sysparm_category=befe97c7db6ad740dd1a591e5e96193d) (Perform a file transfer from one location to another location)

**UVMHN policies:** Note that thesepoliciescan be accessed through[**UVM Commons**](https://uvmcom.sharepoint.com/sites/commons/dean/comclntril/SitePages/Policies%20-%20Procedures.aspx)or via the UVMHN Intranet

* UVMHN\_INFO4 Policy
* UVMHN\_INFO5 Policy
* UVMHN Privacy32 Policy
* UVMMC Research1 Policy