DATA MANAGEMENT & SECURITY PLAN

GUIDANCE DOCUMENT FOR MEDICAL RESEARCHERS

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 required information in the following sections of the DMSP:

1 – STUDY TITLE, LEADS & TEAM
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
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

3 – DATA SETS
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

4 – STORAGE & SECURITY
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

5 – DATA SHARING
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
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 can be found at the end of this document. A Glossary has been included to provide definitions and other information related to specific terms used throughout the DMSP. Also included are Links to relevant institutional policies & procedures, as well as external websites, to provide guidance when completing the DMSP.

INSTRUCTIONS FOR COMPLETING THE DMSP:

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 for guidance.

1 – STUDY TITLE, LEADS & TEAM

1.1 Version Date Click or tap to enter a date.

1.2 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.

Response examples for description of the training plan:

1. The data management plan will be reviewed with the study team prior to study initiation at a scheduled study launch meeting, any updates to the DMSP will be provided to study team members for self-review. Verification of training for study personnel will be documented and stored in the study's UVMHN SharePoint folder.

2. All members of the study staff will review this document and demonstrate their understanding of its contents by their signature, either electronic or written, on an annual basis at a minimum or when a modification is required for study changes. Electronic files will be stored in the study folder on the CVMC S: drive and written forms will be stored in a locked file cabinet in the Primary Investigator's office.

3. Research team members will undergo annual training of data management processes based on the IRB approved data management protocol. The data management protocol will always be available via the UVMMC S-Drive folder for team members to reference if there are any questions regarding data management. The folder where this will be stored will be created at time of IRB approval of the protocol; attendance at team training sessions will be recorded and stored in the same folder.

2 – DATA SOURCE/CUSTODIAN

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 **AND** specific criteria apply. Refer to the Glossary for the definition of a 'Data Custodian' and 'Disclosure', and the Links section for ***UVMHN Privacy32 Policy*** and ***HIPAA Privacy Rule Accounting of Disclosure*** relating to disclosures of PHI.

2.1 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 for the definition of a 'Data Owner'.

Response examples for description of 'Other' source/custodian:

1. We will be using an existing research dataset developed for the Cardiac Inpatient study (STUDY00000000) and collecting additional data from manual chart review. The Primary Investigator has authorized access to data from STUDY00000000 for this cardiac research.

2. This study will utilize resident application data through the online portal. Permission to utilize this data for this study has been granted by J. Smith, who has designated authority of the database. He confirmed the conditions of use for this data and I have provided that statement in an attachment to this IRB protocol.

2.1.1 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:

- 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 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 review & approval.

2.2 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 for definitions.

Response examples for description of the non-UVM/UVMHN source/custodian:

1. Study team will request faxed health records from subject's non-UVMHN care providers during study participation (i.e., ER visits, primary care, etc.). Authorization to use this data was provided by J. Smith, the designated authority for this data at Signant Health.

2. The information is being provided to me by the collaborating university's research program administrators via the university's secure portal. Access to this data has been approved by J. Smith, the university's clinical research program administrator, and N. Jones, the Information Specialist at the Office of Health Information Management.

3. Additional responses may describe sources such as external study collaborators in industry or a study sponsor.

3 – DATA SETS

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, for any period of time (i.e. hours, weeks, months). Refer to the Glossary for definitions of a 'Limited Data Set', 'Coded Data Set' and 'De-Identified Data Set'.

3.1 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.

Response example for description of master key storage location:

Master key will be stored in a separate research folder on the UVMHN institutional shared drive (S:\Groups\Department) for which access is restricted to selected individuals on the IRB-approved study team.

☐ **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.

3.2 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 and for any period of time, you will be deriving a limited, coded, or de-identified data set from an initial data set containing direct identifiers.

Response examples to describe process throughout the study:

1. Data will be extracted by study investigators, through retrospective review of medical records. Identifiers will be maintained so the investigator has all the information needed in making the decision on the correct data to transfer to the sponsor. To maintain the privacy and confidentiality of subjects, once relevant clinical variables are extracted on each eligible subject, identifiable subject data (i.e. all direct identifiers) will be removed and it will be a limited data set, each subject will be assigned a unique patient code instead of a name or medical record number. The data set with direct identifiers (Master Key) will be retained by the Primary Investigator and the Limited Data Set will be shared with an external collaborator once a DUA is executed.

2. The Data Management Office will create the initial data set with direct Identifiers. In addition, the DMO will create a directory on the UVMMC shared drive: S:\Groups\\Medicine\Study Folder where the data will be stored and the PI will temporarily have full access. The PI will collect additional data through chart review, and will then create a limited data set by removing all identifiable patient information except for Visit Date and Zip Code, and a master key which will be stored in a separate folder.

Data which is collected for this study includes:

a) Data will be collected on paper case report forms, signed consent forms, and printed UVMHN EHR notes; identifiable data will be coded by applying a sequential alphanumerical assignment to each individual's sample and data as assigned by the Sponsor. The coded data set will be manually entered directly into the secure online electronic data capture (EDC) database.

b) Data is also obtained through remote medical spirometry testing by the subject using a home monitoring device with the associated application downloaded onto a study-provided Android device for wireless data transfer for analysis. All data collected in this way is identified only by the unique coded subject ID. Identifiers collected by this app will be limited to date of birth, which will only be visible on the device and hidden on the web portal, as necessary for accurate documentation of study data. The coded subject ID can be used to re-identify study subjects only when referring to the master key containing direct identifiers.

c) Data is also obtained through remote entry by the subject into the electronic patient questionnaire application, which will be downloaded on the same Android device as the one supporting the home monitoring app. For the app, subjects will enter password, email address, and telephone number for password recovery only, and all data collected in this app is identified only by the unique subject ID.

d) Data is also obtained in-office at study visits through direct measurement using the CT system. All data collected in this way is identified only by the unique coded subject ID. Identifiers collected by this app will be limited to date of birth, which will only be visible on the device and hidden on the web portal, as necessary for accurate measurement & documentation.

e) Enrollment, Randomization, and study drug assignment will be completed through the Sponsor's online portal. All data collected in this way is identified only by the unique coded subject ID. Identifiers collected by this app will be limited to sex and year of birth.

3. A full data set with direct identifiers is needed in order for the study team to verify the cohort provided by the UVMHN Data Management Office to determine inclusion criteria and screening/follow-up rates as well as to direct identifiers will be retained on a secure UVMMC drive by the PI; the de-identified data for each patient will include: UVMHN affiliate, Primary Care clinic, PCP, Age (age over 89 will be listed as 89+), Sex, Race, Ethnicity, Insurance type, referred for follow up (Y/N), time frame for follow up (in months), follow up within 1 year (Y/N), diagnoses, and treatment performed. Further, the collaborating study team will interview staff directly and audio/video record interviews and clinic activities that will only be stored at the collaborator's study site. These recordings are necessary in order for the collaborator's team to validate the intervention adherence and implementation execution so that the intervention may be properly tailored to the UVMHN clinic's individual workflow.

4 – STORAGE & SECURITY

Describe the data storage method, location, and security for protecting all study data described in **Section 3 – DATA SETS** (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 for applicable guidance.

4.1 Biospecimens or Data Stored on Physical Mediums (e.g., written questionnaires/surveys, paper source documents, microfilm, or radiology imaging). Note that even if documents are scanned/entered electronically, all original paper source documents must be retained.

☐ **Not Applicable – Skip to 4.2 Data Stored Electronically**

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

***Response examples for description of storage location**:*

1. Data stored on physical mediums will be stored in the laboratory at 1111 College Parkway, Colchester VT 05446. A copy of signed written consent forms to be scanned directly into the UVMHN electronic medical record. Upon study closure, archived paper records will be stored at Health Information Management at 327 Holly Court in South Burlington, VT. Biospecimens will be stored at the Research Center at Colchester Ave in Burlington, VT until shipment to collaborating laboratories.

2. Paper forms from patient questionnaires will be stored in the Primary Investigator's locked office in a locked file cabinet located at UHC, 1 South Prospect St. Burlington, VT 05401.

4.1.2 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)?*

***Response examples for description of security**:*

1. Paper copy source documents will be stored in binders in double-locked offices in the laboratory at 792 College Parkway in Colchester VT 05446. Biospecimens will be stored at the Research Center at 000A Colchester Ave in Burlington, VT in a locked freezer within a locked laboratory within a locked facility. Data is stored securely within UVMHN systems or facilities and only accessed by authorized study team members and the sponsor's monitor per protocol.

2. Paper forms will be kept in a locked file cabinet in a locked office located within a locked suite in the Department of Pathology. Only the PI and active study team members will have access to this storage location. To protect the study subjects, the master key to identify the subjects will be stored electronically on the restricted-access UVMHN Teams channel created for this study.

4.2 Data Stored Electronically

☐ **Not Applicable – Skip to 5 – DATA SHARING**

4.2.1 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 for the definition of 'External Data Source'.

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

***Response example for description of 'Other' electronic storage location**:*

1. Additional/supplemental data is abstracted by UVMMC study staff from EPIC onto paper Data Collection Forms, and then subsequently entered into the Electronic Data Collection (EDC) tool provided by the lead study site once all data is collected. The EDC tool is a web-based, direct entry platform provided by the American College of Surgeons and is integrated with the study's data center.

2. The collaborating site's study team will interview CVMC staff directly and audio/video record interviews and clinic activities that will only be stored at the collaborating site, accessed by their study team and stored securely on their university servers. These recordings are necessary to validate the intervention adherence and implementation execution so that the intervention may be properly tailored to the CVMC clinic's individual workflow.

4.2.2 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. See the Helpful Resources section for guidance.

***Response examples**:*

1. S:\Groups\Medicine

2. The S: drive research folder, which is limited to UVMMC Key Personnel will be used to store study data sets. Each data set will receive its own, protected folder, based on year and type. (i.e. Identified/de-identified 2012-2022 data, or identified/de-identified baseline which would be the 2010-2012 data).

3. Data within UVMMC will be stored in S/groups/Department/ Project PI Name; Data within UVM LCOM will be stored within L:\Groups\Department\Project PI Name. We will also be utilizing the UVM Vermont Advanced Computing Core (VACC) for data storage through throughout this study until study closure in early 2027.

4. The hospital [UVMMC] S: drive will be used along with the secure cloud-based platform provided by [Industry Sponsor] as designated in the Data Sharing Agreement and Collaboration Agreements signed by the Recipient Scientist and the UVMMC Primary Investigator. These documents are currently awaiting final signatures and will be finalized prior to receiving data from the UVM Health Network Data Management Office or sharing data with the study sponsor.

5. All data used for analysis in this project will be stored on the UVM LCOM secure server called SEDRC. The name of the folder is D:\Groups\DEPARTMENT\Project Name. Access to this folder is limited to the research staff. Aggregated results and manuscripts will be stored on SEDRC and saved on the UVM shared drive (L:\Groups\DEPARTMENT\Project Name).

☒ **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 section for guidance.

***Response example**:*

At the time of study closure, Electronic Database Capture (EDC) data will be backed up on UVMMC-provided encrypted removable USB drive and stored with archived binders. The password used for removable USB encryption will be stored on the UVMMC S: drive (S:\Groups\DEPARTMENT\Project Name). Electronic data collected from smart devices [Device Name; described below] will be backed up on two Sponsor-provided removable USB drives and stored with archived binders.

☒ **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).

Response examples:

1. Electronic data capture (EDC) online database (Provider/Administrator: Name), home spirometry mobile application (Provider/Administrator: Name), electronic patient questionnaire mobile application (Provider/Administrator: Name), sponsor's online portal (Provider/Administrator: Name)

2. Data is obtained during study visit procedures and recorded on paper. That data is manually entered directly into the secure online EDC database; all data collected in this way is identified only by the unique subject ID. Enrollment, Randomization, and study drug assignment will be completed through the sponsors online portal. Identifiers collected by this app will be limited to sex and year of birth.

☒ **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.

Response examples:

1. Android smartphone device with pre-downloaded applications [Application Names]. Data for both applications will be wirelessly remotely downloaded to the respective servers. All data collected is identified only by the unique coded subject ID. Identifiers collected by this app will be limited to date of birth, which will only be visible on the device and hidden on the web portal, as necessary for accurate measurement of spirometry. Identifiers collected by this app will include subject-entered password, email address, and telephone number for password recovery only, and all data collected in this app is identified only by the unique subject ID. No other apps besides the two spirometry apps may be downloaded onto this Android device, and access to camera and messaging functions is restricted; access to these devices will be restricted to authorized study team members and will not be used for any other purpose.

2. Patient cardiac data is collected and automatically transmitted to the study platform [Device Description] for central analysis. The participants will be provided with a handheld device at the Baseline Visit. The handheld device may also be referred to as a handheld or an eDiary. This device is securely encrypted. Any assessment completed by the participant in the handheld device will be transferred via Wi-Fi or Mobile network (embedded SIM card, automatically connects) from the site/ participant to the vendor and from the vendor to the CRO and/or sponsor. No additional source documents are required assessments completed by the participant in the handheld device. A coded study ID, gender and age will be collected using this device during the baseline visit.

☒ **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.

Response example:

The graders for the images will be on the key personnel list for the study. Because the [Software Name] automatically grades the images and could potentially bias the graders, the graders will access the images digitally in our local office instead of through the software. They will grade the images separately with the grades stored in a password protected excel spreadsheet that will be stored on the hospital S drive. The images will be uploaded to the software separately for automatic grading. Along with one retinal image, the patient ID number (randomly assigned using the master key) and year of birth will be uploaded to the software as well as the embedded date of service on the image – no other identifiable information will be collected.

☒ **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.

Response examples:

1. Data is also obtained in-office at study visits through direct measurement of echocardiogram (ECG) and spirometry using [Device Name(s)]. Data collected by the devices will be wirelessly transferred from the device application to ERT servers for professional overread. All data collected in this way is identified only by the unique coded subject ID. Identifiers collected by this app will be limited to date of birth, which will only be visible on the device and hidden on the web portal (described above), as necessary for accurate measurement of ECG and spirometry.

2. Patient ECG data is collected and automatically transmitted to the platform [Platform Name] for central analysis. An ECG machine will be provided to the site from the sponsor and the ECG will be transferred via Wi-Fi or Mobile network (embedded SIM card, automatically connects) from the site to the vendor and will be read by a central ECG reader. The ECG data will be identified with the patient's medical record number, not the study ID.

☐ **Other - Describe**

Click here to provide a description.

4.2.3 **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)?

  Response examples*:*

  1. Coded data set will be derived from source data and manually entered directly into the Sponsor-required secure password-protected EDC database, a password protected file containing the master key will be stored separately on the UVMHN department S:drive described above.

  2. Android smartphone device will be provided to subjects pre-downloaded with password-protected spirometry applications. No other apps besides the spirometry apps may be downloaded onto this Android device, and access to camera and messaging functions is restricted to authorized study personnel. No data besides that collected within the apps may be stored on the Android device. To ensure this device is secure, it will not be used for any purpose beyond the defined scope in this study protocol. The devices will be securely stored in a locked cabinet and only accessed by the study personnel.

  3. Security Protocol within (UVM department): Data in specific file locations within (the department) will only be accessible to designated people via access control lists including the Primary Investigator, authorized study personnel and the biostatistician as specified by the PI and Faculty Sponsor of this project. Physical security requires biometric and card swipe, followed by disarming of alarms by code, and is video monitored 24x7.

- 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?

  Response examples*:*

  1. Access to the Sponsor-required secure EDC database and UVMHN S: drive folder is restricted to selected individuals approved by the Primary Investigator and study sponsor. The list of approved individuals on the local study team or sponsor staff such as study monitors will be reviewed on a yearly basis, or more frequently when additions/removals are made.

  2. For the purposes of this study, we will enable the password protected study folders to only be accessible to the Primary Investigator and authorized study coordinators; de-identified data will be stored in a separate password protected folder and will be accessible to all approved study staff.

  3. The server permissions will be maintained by the PI and Faculty Sponsor in coordination with the UVM Administrator as well as UVMMC IT. User access will be managed by the PI with the assistance of UVM-LCOM COMIS. This section has been separated into the following three research activities to aid in organization:

  a) Data collection – Program Administrators from each participating department will have access to this UVMMC S: drive folder, this access will be restricted only to the initial data collection period and access will be removed at the earliest possible time once the data is validated.

  b) Data processing - the UVMMC Team will be granted access to the data in the S: drive folder for processing, and access will be removed once the coded data set and master key are uploaded to two separate secure password protected study folders.

  c) Data analysis - the coded data set created by the IT team for analyses will be securely transferred to UVM Vermont Advanced Computing Core (VACC) via secure file transfer and securely accessed by the Primary Investigator and biostatistician per protocol.

5 – DATA SHARING

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 for guidance.

☐ **Not Applicable – Skip to 6 – RETENTION & DISPOSAL**

5.1 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.

***Response example to specify type of identifiers**:*

Images are considered a biometric identifier and therefore make it impossible to complete the project without sharing them. The date of service is embedded on every image and it is impractical to remove that information from each image.

5.2 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) or the UVM Medical Center's Office of Clinical Trials Research (OCTR), as per policy.

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

☐ OCTR will be helping me with clinical trial contracting, including required data sharing/use agreements.

☐ 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:

5.3.1 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); for UVM file transfer, refer to the link for UVM File Transfer Service. If you have a written SOP, you can copy/paste the information below.

  ***Response examples**:*

  1. Data will be transferred to the (example institution) through a secure REDCap submission to the center's REDCap portal [URL]. The local PI will remove the MRN from the data and replace the MRN with a REDCap study ID to create a Limited Data Set with a code that will be shared with 9the institution). Only specified study personnel will have access to clinical data. Data will be maintained locally in a secure REDCap project file. The primary investigator will be responsible for oversight of collected data.

  2. We will be sharing de-identified data with collaborators at University of Wisconsin, Madison via the UVMHN secure file transfer data sharing service (URL).
- **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)**
  ***Response examples**:*
  1. The Office of Clinical Trials Research is preparing the DUA

2. Other responses may include other external study collaborators

5.3.2 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); for UVM file transfer, refer to the link for UVM File Transfer Service. If you have a written SOP, you can attach or copy/paste the information below.
  ***Response example**:*
  Data will be transferred to the sponsor's EDC system [EDC's URL] by authorized local study personnel. A Sponsor Monitor will be assigned & authorized to review and validate the data in the study data in the EDC system.
- ■ **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.

6 – RETENTION & DISPOSAL

6.1 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.

- ☐ **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:**

6.1.1 Reason for Retaining the Data/Biospecimens (check all that apply):

- ☒ **As a basis for similar or related future research conducted by the local PI**
  ***Response example**:*
  Data will be retained in the study database for future planned studies, we will utilize the same patient population. New studies will explore new study objectives associated with current patients in the study database and will utilize data from new patients to expand the same population or collect additional data to meet new study objectives for a related population.
- ☐ **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**
  ***Response example**:*
  The sponsor requires a list of participants to be maintained at the local study site for a period of 5 years in case new safety information needs to be relayed to them.
- ☐ **Other**
  Click here to provide a description.

6.1.2 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.

6.1.3 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**
  Response example to describe justification*:*
  The sponsor requires a list of participants to be maintained in case new safety information needs to be relayed to them. No further analysis is intended.
- **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.**
  Response examples*:*
  1. Upon study closure, archived paper records will be stored at Health Information Management at 327 Holly Court, Suite 50 in South Burlington, VT.
  2. We will maintain all study records according to ICH-GCP guidelines. Records will be retained for a minimum of 2 years after the last marketing application submission or 2 years after formal discontinuation of the investigational product. We will contact the sponsor prior to destruction of study records. Location of all study data and records is described in the attached SOP [Filename].
  3. Refer to attached Data Management SOP [Filename]; all data will be stored by the University of Vermont Medical Center Health, Information Management, 327 Holly Court, Suite 50, Burlington, VT 05495.
- **Length of time the identifiers will be retained**
  Response examples for length of data retention:
  1. Data will be retained for up to two years to allow for validation during publication period.
  2. We will retain the master list with the participant study ID for 12 months after study closure per sponsor's requirements.
- **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.**

6.2 **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.
Response examples to describe data destruction plan for all identifiable data or biospecimens*:*
1. Data, regulatory files, and subject records to be destroyed at earliest possible time as determined by the industry sponsor and UVM Health Network Record Retention Guidelines policy (refer to attached SOP)
2. Plan for deletion of the data: data will be retained within the department for the entirety of this project (completion on 07/2027). At completion of the study, the PI of this study will send a formal request to destroy the stored research data, and a formal request will be made to the UVM-LCOM COMIS to delete the :L drive folders which contain coded data.
3. Data files will be deleted on the hospital [UVMMC] shared drive once they are no longer needed upon study closure. Retinal images will be deleted from the local UVMMC server and from the collaborator's cloud server.

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), Glossary of NIH Terms and the NIH Toolkit Glossary, National Institute of Standards & Technology Glossary, Payment Card Industry Security Standards Council Glossary and the U.S. Department of Health & Human Services.

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, 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 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 for which the loss, misuse, or unauthorized access to or modification of, 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
- HIPAA Privacy Rule Accounting of Disclosures
- NIH Data Management & Sharing Policy

UVM Resources, Policies & Procedures:

- UVM File Transfer Service
- UVM Enterprise Technology Services Catalog
- UVM Privacy Policy
- UVM IS Policy & UVM IS Procedures
- UVM Research Protections Office IRB Policies & Procedures
- UVM Research Protections Office IRB Forms Library
- UVM Office of Compliance & Privacy Services

UVM Health Network Resources, Policies & Procedures

File sharing: Note that these platforms must be accessed through the UVMHN Intranet

- UVMHN Add Guest to Microsoft Teams/Sharepoint/OneDrive (Add guest user from outside UVMHN)
- UVMHN GoAnywhere File Transfer (Perform a file transfer from one location to another location)

UVMHN policies: Note that these policies can be accessed through **UVM Commons** or via the UVMHN Intranet

- UVMHN_INFO4 Policy
- UVMHN_INFO5 Policy
- UVMHN Privacy32 Policy
- UVMHN Privacy33 Policy
- UVMMC Research1 Policy