### The University of Vermont Committees on Human Research

### Research Data Management and Security Plan

**This form once completed and approved, will be the official data management and security plan for the protocol. This includes biospecimens. Any changes to this plan must be submitted for prior review and approval.**

|  |
| --- |
| **Project Title** |
|  |
| **Principal Investigator** |
|  |
|  |
| **1. Data Collection Methods (check all that apply)** |
|  | Paper and pencil (i.e. written consent forms, written questionnaires, data extracted from records onto written forms, paper source documents, etc.) |
|  |
|  | Electronic data capture (i.e. surveys completed in redcap; electronic case report forms) |
|  | Audio/video recordings, photographs and/or other medical images (MRI, x-rays, etc.) |
|  | Mobile application (data entered into app) |
|  | Smart device (fitbit, smart phone, applewatch, etc) |
|  | Interactive medical or research device (i.e. pace maker, electronic pill dispenser) |
|  | External web-based surveys |
|  | Other: please describe |
|  |  |
| **2. Plan for Protecting the Stored Data** |
| **a. Data Stored on Paper** |  | **Not applicable** |
| i. | Describe how individual participant **paper** research data forms will be identified. *(check all that apply)*  |
|  |  | Data will retain direct identifiers *(names, medical record number, social security number)* |
|  |  | Explain why direct identifiers need to be maintained. *Written consent always has direct identifiers, we are inquiring about all other research data associated with the protocol.* |
|  |  |  |
|  |  | Data will be coded *(A master key to the code (used to identify subjects) kept separately from the data.)* |
|  |  | Describe the process used to code the data. |
|  |  |  |
|  |  | List who has access to the master key. |
|  |  |  |
| ii. | Describe how and where will **paper** forms (including consent forms) be stored (locked office, file cabinet, scanned to shared drive)? |
|  |  |
| **b. Data Stored Electronically****Hospital users** should reference the Information Services Security Policy and Standards on the UVMMC site. **UVM users** should reference the Information Security Procedures policy on the UVM site. |
| i. | Check which IT dept. is assisting you with the protection of your **electronic** research files. |
|  |  | UVMMC  |  | UVM |
|  |  | UVM COM  |  | Other | Describe |  |
| ii. | How will subjects be identified within **electronic** research data files? *(check all that apply)* *Please note that if you scan paper forms (including consent forms) these would be considered electronic research data files.* |  | NA |
|  |  |
|  |  |
|  |  | Data will retain direct identifiers *(e.g. names, medical record number, social security number)* |
|  |  | Explain why direct identifiers need to be maintained. *Written consent always has direct identifiers, we are inquiring about all other research data associated with the protocol.* |
|  |  |  |
|  |  | Data will be coded *(A master key to the code (used to identify subjects) kept separately from the data.)* |
|  |  | Describe the process used to code the data.  |
|  |  |  |
|  |  | List who has access to the master key. |
|  |  |  |
| iii. | What is the physical security of the **electronic** research data files? *(check all that apply)* |
| a. |  | **Local computer hard drive** *(Will require encryption if data contains directly identifiable private information.)* |
|  |  | Describe the plan to ensure that the computer(s) will be protected. *(physical security, encryption, password protection, etc.)* If you have a written SOP, you can attach or copy/paste the relevant section here. |
|  |  |  |
| b. |  | **Institutional server**  |
|  |  | Identify which server will be used. |
|  |  |
|  |  | Server folders can be set up so that only specific personnel have access to specific folders. Describe how the folder permissions will be maintained. If you have a written SOP, you can attach or copy/paste the relevant section here. |
|  |  |  |
| c. |  | **Thumbdrives, External Hard Drives, Other Storage** *(Devices will require encryption if data contains directly identifiable private information.)* |
|  |
|  | Describe the process used to ensure that other types of storage, as listed above, are properly protected. If you already have a written SOP, you can attach or copy/paste the relevant section here.  |
|  |  |
| d.  |  | **Collection through Online Applications or SMART Devices**If research data is being collected electronically, online, through an app, or through a smart device list name of company(ies)/host(s).  |
|  |
|  |
|  |  |  |
|  |  | Describe how the research team receives and stores that data including how subjects are identified. (e.g. downloaded into excel with no identifiers; exported from redcap in de-identified format) |
|  |  |  |
|  | Do you have approval from the IT department that this collection method meets institutional requirements.  |
|  |  |
| **3. Plans for Sharing Research Data** |
| a. | Do you intend to share research data with colleagues other than key personnel or the project sponsor/funder? |
|  |  | Yes |  | No, skip to 3.c. |  |
|  | *If yes, sharing data outside of either institution whether identifiable or not, requires a data use agreement (DUA). UVM investigators should contact Sponsored Projects Administration at 656-3360 to speak with the Executive Director for Research. UVMMC investigators should contact the Office for Clinical Trials Research at 847-8990.* |
| b.  | Will you include direct identifiers with the data that you will be sharing? |
|  |  | Yes |  | No, skip to 3.c. |
|  | If yes, provide justification for sharing identifiers.  |
|  |  |
|  | Describe the method you will use to share the data.  |
|  |  |
|  | If sending files through email, explain the process you plan to use to encrypt files. *(Encryption is required even if sending to and from uvmhealth.org, med.uvm. and uvm.edu email addresses.)* If you have a written SOP, you can attach or copy/paste the relevant section here. |
|  |  |
| c. | Are you sharing identifiable data with the protocol sponsor/funder? (*signed consents are identifiable)* |
|  |  | Yes |  | No |
|  | If yes, describe how that data is shared. |
|  |  |
| **4. Research Data Retention and Disposal** |
| a. | Do you intend to retain the research data once the protocol is complete? |
|  |  | Yes |  | No, proceed to 4.f. |
| b. | If yes, indicate reason for keeping the data. |
|  |  | As a basis for my future work only |  |  |
|  |  | As a resource for other investigators\* |
|  |  | Sponsor requirement only |  |  |
|  |  | Other  |  |  |
|  | *\*If the intention is to have the data be a resource for other investigators, the data should be moved into a repository where rules for future data release are in place. (This includes biospecimens)* |
| c. | If you intend to move the data or biospecimens into a repository, list the IRB number assigned to the repository.  |
|  |  | IRB # |  | Not applicable |
| d. | Do you intend to keep identifiers of any kind, direct or coded?  |
|  |  | Yes |  | No |
|  | If yes, justify why you will need to keep the identifiers. |
|  |  |
|  | 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. |
| e. | 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. |
|  |  |
| f. | Describe your data destruction plan. If you have a written SOP, you can attach or copy/paste the relevant section here. |
|  |  |
| **5. Training for the Research Team** |
|  | Describe how you will ensure that your research team members understand and will follow this data management and security plan. If you have a written SOP, you can attach or copy/paste the relevant section here. |
|  |  |