Title: Core Standard Operating Procedure for Software and Data Management Technology

I. Procedure Statement
To describe the processes, backup, and documentation requirements related to utilizing specialized software and/or data management technology related to a research study.

II. Definitions
1. Standard MU Health Software and Applications: Software and applications that are standard for MU Health computers and systems. Includes items such as Microsoft Office Suite, PowerChart, PowerTrials, REDCap.
2. Research Specific Software and Applications: Includes software and applications that are not standard for the MU Health system. These are most generally purchased from an outside vendor or provided by a sponsor and must be installed on a research investigator or staff computer.
3. Protected Health Information (PHI): Refer to the MU Healthcare policy specific to Protected Health Information and Research for those identifiers that are classified as protected and require additional security and approval including a Business Associate Agreement (or contract specific terms) with a third party vendor prior to sharing research participant data.

III. Procedure/Content/Scope
This SOP will apply to all clinical trials research within MU Health including the School of Medicine, School of Health Professions, School of Nursing, and MU Healthcare. This SOP will outline the processes, backup, and documentation requirements for utilization of software, applications, and data management technology specific for a research project. This will ensure data and participant security as well as data availability throughout the life of a research project.

1. Prior to utilizing any software/application or data management system for a research study, ensure approval has been granted through the IRB and that either the contract terms or a Business Associate Agreement (through the Privacy Officer) has been signed detailing the participant data to be captured, the PHI that might be involved, and the method for sharing information.

2. Standard MU Health Software and Applications have built in processes for security and backup. However, any Research Specific Software/Application purchased from a third party vendor (or provided by a sponsor) or accessed online must also meet the same level of security and backup requirements including:
   a. Installed/approved by a MU Health IT expert from either the Tiger Institute or by a School or department IT professional.
   b. There must be a standard process for the backup of data from the software/application to a location other than the computer hard drive of one individual.
      a. Processes must be in place to ensure the software/application and any
associated data is transferred or maintained regardless of any investigator or staffing turnover. No data or information is to be deleted from a computer until it is confirmed that there is a backup of the software/application as well as any associated data.

c. Any login information should be maintained within the research unit. Usernames and passwords should be specific for each individual and usernames or passwords should not be shared from individual to individual.

d. If the software/application becomes obsolete and is not able to be used with new technology, there must be a data capture of all study specific information into a format that can be transferred into a media that can be utilized by new technology.

3. Documentation of the location (research area, computer ID, individual) of any Research Specific Software/Application should be included in the study binder. In addition, information regarding the backup of data should exist in the research area as well as with IT professionals providing support to the research unit.

IV. REFERENCES:

1. MU Healthcare policy specific to Protected Health Information and Research