METRC Policy & Procedure Manual

Title: Data Management, REDCap, and Servers

General Description & Purpose: This document describes METRC's data management policies and procedures with regard to the use of REDCAP. It also describes METRC servers and security.

I. Data Management Oversight

All data management activities for METRC studies are overseen centrally by the staff of the Study Management Teams and the Informatics Core within the Coordinating Center. Additional programming, database and server management expertise are provided to the Informatics Core Informatics Core through their collaboration with the Johns Hopkins Bloomberg School of Public Health Biostatistics Center.

II. Case Report Form Portfolio Development

Data are collected on Case Report Forms (CRFs) designed specifically for the study. Drafts of the case report forms are developed by the study PI, MCC PI, Project Director and members of the Informatics Core, and then are subsequently reviewed and approved by the Protocol Committee. Once finalized, the CRFs are formatted according to a standard template. Survey instruments and clinical assessment items are drawn from the METRC core dataset which serves as the basis for standardized data collection across all studies and is maintained by the Data Standards and Adjudication Committee.

III. REDCap

Selection of REDCap Data Capture System

The centerpiece of the METRC data management infrastructure is the NIH-funded Research Electronic Data Capture (REDCap) project. The REDCap distributed data entry system was selected among a number of competitors because it is specifically designed for multicenter clinical studies built using a highly customizable and flexible open-source design that is publicly available. REDCap has a strong and responsive development community and is actively being used by numerous universities and medical centers.

REDCap Application

REDCap is a state of the art, metadata driven application for the organization and data management in clinical studies. It was built by a team at Vanderbilt University using non- proprietary technologies, namely PHP, JavaScript and a MySQL database engine. As such, it is highly customizable with personnel resources available to the MCC as part of our collaboration with the Johns Hopkins Biostatistics Center. The REDCap application runs from secure, dedicated servers (see server description, below) and added functionalities have been programmed into the base configuration to support project requirements.

REDCap Data Management Functions

REDCap data management functions use a web-based distributed data entry system that access an internet-connected database server. The system permits both the METRC Coordinating Center and

participating clinical sites to have access to data as soon as they are entered. This allows for near-real-time recruitment reports, detection of data anomalies, and increased data entry availability and convenience for the clinical sites. The primary functions of the METRC REDCap application include: registration of all candidates for the trial; entry of all study data forms; inventory, management, and editing of study data; maintenance of full audit trails of all data entry and editing; and real time performance report generation.

Validation Functionalities

The REDCap software also includes extensive data validation functionalities, such as field level validation, checking the correct format and range of each entered item; intra-form validation (e.g. checking for logic errors, skip pattern violations; and inter-form validation (checking for inconsistencies across forms). In addition, using REDCap's flexible open-source design, we modify the software to include clinical site management tools such as participant scheduling, serious adverse event and protocol deviation notifications, eligibility adjudication, and notifications for patient enrollment and withdrawal. Additional functionalities may be added as projects progress or updates to the software are implemented.

Import and Export Capabilities

REDCap has a number of built-in data import and export capabilities, including the capacity to upload various file types (e.g. x-rays and photos) and produce data and syntax files for several common statistical analysis and data management packages (Microsoft Excel, SPSS, SAS, R, Stata).

Identifiers

A unique study identifier is assigned at time of patient enrollment by REDCap. The study ID consists of a 3-character study code, a 3-character code (like an airport) for the METRC site, and a sequentially assigned number of at least four digits. Personal identifiers entered into the database are limited to only those required to perform the study (e.g. dates of service for key study events).

Confidentiality

Hard Copy Data: Although data collection typically occurs using electronic data entry in real time, occasionally data may be captured on hard copy documents, should it be necessary. Any hard copy documents containing patient identifiers and contact information is stored in secure document containers (file cabinets, lockers, drawers, etc.) in accordance with standard document management practices. Consent procedures and forms, and the communication, transmission and storage of patient data will follow individual site IRB and DoD requirements for compliance with the Health Insurance Portability and Accountability Act (HIPAA). The data collection case report forms (CRFs) are maintained according to FDA and ICH guidelines regarding on and off-site storage. Paper forms are shredded within five years after study completion. Each site will provides the Coordinating Center with a signed verification when the data have been destroyed.

All study forms, reports, and electronic records that are part of the study data collection materials are identified by a unique study ID to maintain patient confidentiality. Clinical information is not released without written permission of the patient, except as necessary for monitoring by the local IRB, the MCC, the study sponsor, or Medical Monitor.

Electronic Data: REDCap is only accessible by registered and authenticated users. Individuals are not granted access to the system until properly trained and certified by the MCC (see Site Certification SOP). Authorized users are bound by strong password policies and staff are trained to recognize the sharing of passwords as misconduct.

Permissions

The REDCap Data Access Groups control functionality permits differing levels of system access. Access levels are controlled by the MCC. These include specific permissions to view, edit, and enter data, as well as higher-level permissions to modify table structures, review logs, and assign user privileges. As an example, clinical sites are able to access, edit, and generate reports for their site, but are not be able to access the data generated by other sites.

Logging

Detailed change and data entry logs are routinely maintained as part of REDCap. These serve to identify suspicious activity and provide an audit trail for all data entries and revisions.

These logs are routinely inspected as part of a Data Quality and Query System. The change logs also make it possible to recover valuable data in the case of malicious or accidental loss.

IV. Server Description and Security

Dedicated Linux servers are provided by JHU Enterprise UNIX Systems Team (EUX) and the Johns Hopkins Biostatistics Center. EUX provides redundant, HIPAA compliant, dedicated server space. EUX data centers all have controlled access and physical security (onsite security teams, biometric scanning and video surveillance). The MCC Server Administrator has the capacity to remotely manage the servers. The MCC Server Administrator can adjust firewalls and load balancers in coordination with EUX technicians. EUX technicians are available 24/7 to assist with technical difficulties. EUX provides operating system upgrades, automatic remote backups, and 24/7 security monitoring and intrusion detection. Daily vulnerability scans and more extensive monthly vulnerability scans are provided automatically by EUX. Monitoring alerts are immediately forwarded to the MCC, server administrator and EUX support via email, phone and/or pager.

Server Layout

Based on industry best practices, we utilize a server layout that can parse various types of network traffic and requests, segment server level functions, and maximize security. Server, database, and software configurations are adjusted to enhance overall system security.

Preventing Data Loss

Frequent and regular backups are established to minimize potential exposure to data loss and ensure research continuity and disaster recovery in the unlikely event of an unforeseen server or software failure. Backup of secure METRC web and database servers is provided by EUX. Full backups are performed weekly, with incremental backups performed daily. Redundant copies of backups made by EUX are stored off-site from the data storage facility where METRC servers are located.

Server Access

Direct access to secure METRC web and database servers is limited to the Director of the Informatics Core, the MCC Server Administrator, and two experienced computer programmers for development and maintenance purposes. Security is strengthened through strong password policies, two-factor authentication, and a VPN connection. Password protected, user-level access to all systems residing on secure servers is restricted to individuals certified by the MCC to conduct data collection and data entry for METRC studies.

V. Access to Data

Information collected on human subjects will only be used for the purposes of the study with the intent on publishing study results to the broader scientific and clinical community. Clinical information is not released without written permission of the patient, except as necessary for monitoring by the METRC Coordinating Center, representatives from the local site IRB, the DSMB, or the study sponsor. The communication, transmission and storage of patient data complies with individual site IRB and sponsor requirements as well as requirements of the Health Insurance Portability and Accountability Act (HIPAA).

VI. Accessing PHI

Site Research Coordinators complete the patient contact information CRF, a standard form designed by the Coordinating Center for sites to track participants over the course of a study. Any patient contact information gathered by sites remains with the site itself and is not entered into REDCap.

Last Updated: September 2021