Use of REDCap Policy

I. Purpose

This Policy is to protect patient privacy and confidentiality while assisting researchers in managing data using REDCap.

II. Scope

This Policy applies to all Albert Einstein College of Medicine ("Einstein" or "College of Medicine") and Montefiore Medical Center researchers wishing to use REDCap for managing research data.

III. Policy

III.A. Background

REDCap (Research Electronic Data Capture) is powerful software, created by Vanderbilt University and supported by the REDCap Consortium to facilitate Institutional Review Board (IRB)-approved clinical research and basic research. Data collected in the course of the research are managed by the program, and can be exported to commonly used statistical packages, including SAS, Stata, SPSS, and R.

REDCap has a flexible and fine-grained authorization matrix, allowing different members of the study team to have different levels of access (none, read-only or edit) to data collection instruments, and access to database management and data export tools. There are provisions to restrict access to data export to allow export of de-identified data only. REDCap enforces authorization granted to each user by providing and/or enabling certain functions, tabs, links and buttons according to granted privileges.

REDCap includes a full audit trail, recording all operations on the data, including viewing and exporting. The audit log records operation, date and time, and the user performing the operation, permitting review of the audit trail as necessary.

REDCap enforces data integrity protection by design; all "databases" (called "projects" in REDCap) created by users are logical data sets on top of a relational database with built-in integrity protection controls. Additionally, REDCap can help to ensure data quality through use of Double Data Entry mode, forms and records locking and electronic signatures.

III.B. Policy and Procedure

To get approval for a REDCap project, users should submit an ICTR Core Facilities Services Request Form using the following procedure (The procedure is also detailed in "Getting Started Checklist" at https://redcap.einsteinmed.org/rc_training/getting_started.html):

1. Go to the ICTR Services website at https://www.einsteinmed.org/intranet/research/ictr/services/
2. Click the "Research Informatics Core" option and select "Access Services" to open the form
3. Fill out the form, checking "Biomedical Informatics (Atlas, Redcap, etc.)" as core facility requested, and "REDCap" as the specific service.

4. Wait for the Clinical Research Informatics (CRI) administrator to approve the project or request clarification.

Approved users can access REDCap at: https://redcap.einsteinmed.org and request the creation of a new project or the copying of one of their existing projects. Once a project is created, an assigned member of the research team can grant project access and specific user permissions to other members of the team.

Montefiore Active Directory (AD) username and password serve as the authentication source for logging into REDCap. To grant access to team members who do not have a Montefiore AD account, please email the Clinical Research Informatics (CRI) at redcap-help@einsteinmed.org to create user accounts for these users so they can then be added to a project.

New users are strongly encouraged to attend a two-hour introductory training session conducted by CRI each month and review REDCap's built-in training videos prior to creating their initial study project. See also additional training resources in "Getting Started Checklist" at https://redcap.einsteinmed.org/rc_training/getting_started.html

Any new project will be created in Development mode. When in Development mode, the user cannot enter any identified patient information. For testing purposes, users should enter made-up identifiers. CRI will periodically review contents of all projects in Development mode to ensure compliance and report violations to the Privacy Officer of the institution whose data is being used.

In the case of data regarding patients or subjects of Montefiore or Einstein, all users must comply with Montefiore's "Policy for the Use of Patient Medical Records in Research" Policy # PNP29 and "Electronic protected health information security" Policy # JH69.1.

It is the responsibility of the PI to:

- Build the REDCap project (Data Collection Instruments, schedule of Events, and designation of DCI to Events) in such a way that it corresponds to the study design and provides a proper data collection tool for testing the study hypothesis (hypotheses)
- Collect all the data necessary for testing the study hypothesis (hypotheses)
- Collect only the minimally-necessary set of PHI, in addition to those required by the study design or operational requirements, to positively identify the study subject during the data collection phase

Alternatively, the PI may request that CRI assist with development of the REDCap project for the study.

To move a project into Production mode, the study PI or authorized PI representative must request a review by CRI, providing the following information:

- IRB-approved research protocol (for clinical studies) or final version of the research protocol (for studies not requiring IRB approval)
- IRB approval letter (for clinical studies)
- A signed copy of this policy.

After review and approval, CRI will move the project into Production and the study team can safely begin data collection.

WARNING: Users should not start data collection in Development mode. Changes to the project occur in real-time in Development mode without the benefit of review, so CRI will not be able to detect structural errors. Furthermore, some changes to the project in Development mode can result in data loss. Once in Production mode, all future changes to the project are subject to automated structural checks, and are referred to review by REDCap admin if there is a danger of data loss.

REDCap is supported by CRI which bears responsibility for maintenance of the software, project deployment (moving to production), data security and integrity.

The PI is responsible for managing access to the PI's project(s) to ensure compliance with HIPAA and other state and federal regulations protecting patient privacy and confidentiality.

Review of audit trails of any user over any period of time will be undertaken at the request of the Decision Support Group, Director of MIS, Director of HIPAA Security or Chair of the Institutional Review Board.

IRB-approved research protocols utilizing REDCap will be recorded by the CRI in a project, which will keep the name of the PI, the title of the protocol, the IRB protocol number, the date of access provision, and date of access deactivation.

III.C. IRB Auditing

- The IRB will receive on demand an auditing report on the activity and authorized users of all human research projects. The report will allow IRB to monitor protocol compliance.
- Upon request, the IRB will have access through CRI to an audit report of IRB-approved use.

IV. Definitions

PI
Principal Investigator. A person responsible for the conduct of the clinical research study, including assignment of the roles and authorizations to use specific forms and functions of the REDCap clinical research project to the members of the research team.

Research Team
PI, Research assistants, nurses, data entry persons and other personnel granted access to the REDCap clinical research project.

Project
Clinical Research or other Research Project ("database") implemented in REDCap. A set of data collection instruments, schedules and other REDCap objects pertaining to a specific study or research project.

Development mode
A state of project that allows authorized research team members to add, modify or delete data entry forms and other elements of the study design. In the development mode, the project is temporary and is not backed up. No data is guaranteed to be preserved in the project in this mode.

Production mode
A state of project that allows authorized research team members to add, modify or delete clinical research data. Any data entered in this mode will be protected by regular mirroring to the stand-by server and periodic backups. Any modification to the data collection design in this mode will need to be approved by the CRI (by REDCap design). CRI offers as a service to review proposed changes before approval to ensure data integrity; should PI opt out by requesting that CRI automatically approve any changes, it will be PI's responsibility if the changes violate data integrity or consistency.

CRI

Clinical Research Informatics of the ICTR. A group responsible for implementation and maintenance of REDCap, for user education, and for management of projects (moving to production, approving changes when in production, restoring from backup etc.).

ICTR
The Harold and Muriel Block Institute for Clinical and Translational Research at Einstein and Montefiore

Authentication
A confirmation from an authoritative source (e.g., Montefiore Active Directory) that the user credentials (user name and password) are valid.

Authorization
A set of rights to access specific objects (data collection instruments, tabs, controls) in specific mode (read-only, read-write or edit, full data set, de-identified data set) granted to a user.

V. Effective Date

Effective as of: 28 January 2021

VI. Policy Management and Responsibilities

Einstein's Research Informatics Core of the Institute for Clinical & Translational Research is the Responsible Office under this Policy. Einstein's Executive Dean is the Responsible Executive for this Policy. Einstein's Research Informatics Core Administrator is the Responsible Officer for the management of this Policy.

VII. Approved (or Revised)

Responsible Executive

01/29/2021
Date

Investigator Sign-Off

I reviewed this Policy, and agree to abide by its provisions. I also understand that data collection with REDCap is subject to the requirements of the Federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"), and I agree to comply with the requirements of HIPAA applicable to the activities contemplated by this Policy.

I understand that violating the provisions of the Policy constitutes grounds for disciplinary action as determined by applicable privacy laws and Montefiore's policies and procedures.

Print User's Name: _____

User's Signature: _____ Date: _____

User's Montefiore or Einstein title: _____

User's Montefiore or Einstein Department: _____