Title: Standard Operating Procedure (SOP)
REDCap Project User Management (Clinical Trials)

Document ID: N/A

Version: 1.0

Author: Luke Stevens, Research Data Systems Manager, CEBU

Author Signature: **Date:** 06-May-2022

Recoverable Signature

X 

Signed by: 96637f12-a7c0-419e-b794-686a7fcb7ff8

The author is signing to confirm the technical content of this document

Reviewed and Approved by:
Professor Katherine Lee, Co-Group Leader Clinical Epidemiology & Biostatistics (CEBU)

Signature: **Date:** 06-May-2022

Recoverable Signature

X 

Signed by: 3954ba31-81b4-4c75-9c2c-67c09b00b993

These signatures confirm the reviewers agree with the technical content of the document and that this document is approved for implementation at MCRI.

This document is effective from the date of the last approval signature and will be reviewed in two years.

Document History

Revision	Modified by	Change No.	Description of Change
1.0	[Author]	N/A	New Issue

Contents

1. PURPOSE

To document procedures for managing User Roles and User Rights in order to configure access to REDCap project functionality and data appropriately.

This version of the standard operating procedure (SOP) is intended for use in projects (such as clinical trials) that are subject to the full rigors of compliance with Good Clinical Practice (GCP). For projects not subject to GCP use the counterpart SOP that is not specific to trials.

2. RESPONSIBILITY AND SCOPE

Managing access to projects in MCRI's REDCap, and thereby to the data they contain, is the responsibility of the research project team. A user with access to a project that includes the "User Rights" permission has the ability to add and remove users to the project and manage the permissions for all project users (including their own).

Having the "User Rights" permission confers the ability and responsibility for ensuring that access to the REDCap project and its data is configured appropriately: that project users have the permissions they require in order to perform the tasks expected of them, do not have access to functionality or data that they should not be able to access, and that user access is removed when no longer appropriate.

3. APPLICABILITY

This (SOP) applies to all users of MCRI's REDCap application that have the "User Rights" permission in a REDCap project either by virtue of having created the project themselves or having been granted this level of permission by another project user when developing and conducting projects that are subject to the full rigors of compliance with GCP. This includes those staff involved in all MCRI-Sponsored investigator-initiated clinical trials at MCRI: Sponsor-Investigators/CPIs, PIs, Associate/Sub-Investigator(s), research coordinators and other staff involved in research duties.

4. PROCEDURE

4.1. Project User Roles

1. Prior to adding a user to a project, review the default user roles and configure appropriately for the project's requirements.
    a. Add new roles if needed.
    b. Edit existing roles to meet project requirements.
    c. Remove roles certain not to be required.

   Follow the "principle of least privilege": users should be assigned to a role with the minimal required permissions – sufficient to perform the tasks required of them but no

more. This reduces the visual complexity of screens, the risk of inadvertent data or configuration changes, and training requirements.
2. Ensure that only a limited set of roles provide access to User Rights (i.e. the ability to configure permissions and user access).
3. Ensure that Case Report Form (CRF) access and data export permissions are appropriate for each role, particularly in relation to the viewing and export of participant-identifying data or where users must remain blinded to certain data e.g. randomised allocation.

4.2. Project Data Access Groups

1. Where there is – or may in the future be foreseen – a requirement for project users to be able to access only certain subsets of records (e.g. staff from different sites seeing only their own sites' records), create a "Data Access Group" (DAG) for each grouping.
2. Ensure that all project users are assigned to an appropriate DAG, where necessary.
3. Utilise the "DAG Switcher" functionality to enable access to multiple DAGs for users that require it.

4.3. Project Access for Users

1. Request REDCap access for users without an existing user account via email to the REDCap Administrators using the MCRI REDCap Support email address: redcap@mcri.edu.au.
    a. For each new user requested, supply first & last name and email address.
    b. When requesting more than a couple of new users it is helpful to include these details in spreadsheet form.
    c. It can sometimes be helpful to set up a separate survey form that site staff can use to make requests to the study team.
    d. Ensure all project users have signed the trial delegation log.
    e. Ensure all project users receive appropriate (and documented) training.
2. Add each user to the role that is appropriate for the tasks they are expected to perform (see section 4.1):
    a. Observe the "principle of least privilege": users should have the permissions they require and no more.
    b. Pay particular attention to the ability to view and export participant-identifying data.
3. Assign a DAG to each user where appropriate to segment access to records, e.g. by study site.
4. Apply an expiry date to each user's project access when applicable. Note that specifying a project access expiry date limits the user's access only to the specific project where it is applied: the user's access to other projects is unaffected.
5. Ensure all users are recorded on the corresponding participating sites Signature and Delegation of Authority Log and receive appropriate, documented training.
6. Review project user access periodically, ensuring users that no longer require access are removed. Note that activity in a project remains in the project log (audit trail) associated with the user that performed the action even after the user has been removed from the project.

5. ASSOCIATED DOCUMENTS

- SOP: REDCap Project User Management

6. GLOSSARY

Administrator
The REDCap Administrator(s) is a person or group responsible for administering the REDCap application within an institution. Among other tasks that administrators are required to perform is the review and approval (or rejection) of alterations to Production REDCap projects that are considered by the application to have a potentially detrimental impact to the integrity of a project's existing data.

Data Access Group (DAG)
A REDCap application construct that facilitates segmentation of record access: users assigned to a DAG have access only to records assigned to that DAG. This is commonly utilised to model site-level access in project databases: site-assigned users may view only their own site's records.

DAG Switcher
A feature in REDCap that facilitates users performing actions for multiple Data Access Groups. A user can be associated with only one DAG at a time, but the DAG Switcher enables users to switch between DAGs that they are configured to be able to access.

Project
A project within REDCap is a discrete database. The data contained within a REDCap project is completely siloed and separate from data stored within other REDCap projects. A research project may utilise multiple REDCap projects for a variety of different data capture and storage purposes.

REDCap
REDCap ("Research Electronic Data Capture") is a secure web platform for building and managing online databases and surveys. REDCap's streamlined process for rapidly creating and designing projects offers a vast array of tools that can be tailored to virtually any data collection strategy. See https://projectredcap.org for more information.

Signature and Delegation of Authority Log
A record of all staff involved in a trial, showing their name, their role, the study-related tasks that they have been delegated, and their signature.

User
A person who owns has access to a login account for REDCap project. People with MCRI Active Directory user accounts may utilise this to log into REDCap provided a REDCap Administrator has added their MCRI username to REDCap's "allow list". Non-MCRI people require an internal REDCap user account in order to log in. The password for these users is managed within REDCap.

7. REFERENCES

None

8. APPENDICES

Appendix 1: Flow chart

DOCUMENT END

APPENDIX 1: FLOW CHART

8.1. Add a User to a Project