York and Scarborough Teaching Hospitals NHS Foundation Trust R&D Unit
SOP
R&D/S65

REDCap Database Access

IT IS THE RESPONSIBILITY OF ALL USERS OF THIS SOP TO ENSURE THAT THE CORRECT VERSION IS BEING USED

All staff should regularly check the R&D Unit's website and/or Q-Pulse for information relating to the implementation of new or revised versions. Staff must ensure that they are adequately trained in the new procedure and must make sure that all copies of superseded versions are promptly withdrawn from use unless notified otherwise by the SOP Controller.

The definitive versions of all R&D Unit SOPs appear online. If you are reading this in printed form check that the version number and date below is the most recent one as shown on the R&D Unit website: www.research.yorkhospitals.nhs.uk/sops-and-guidance-/ and/or Q-Pulse

SOP Reference:	R&D/S65
Version Number:	1.0
Author:	Monica Haritakis
Implementation date of current version:	15th May 2024

Approved by:	Name/Position: Approval Date:	Lydia Harris, Head of R&D 17th April 2024
	Name/Position: Approval Date:	Sarah Sheath, SOP Controller 17th April 2024

This SOP will normally be reviewed at least every 3 years unless changes to the legislation require otherwise

Version History Log

This area should detail the version history for this document. It should detail the key elements of the changes to the versions.

Version	Date Implemented	Reviewer	Details of significant changes
1.0	15th May 2024	Monica Haritakis Tom Szczerbicki	

Contents

1 Introduction, Background and Purpose

The Trust utilises the Research Electronic Data Capture (REDCap) system as the electronic Case Report Form (eCRF) for data collection on Trust Sponsored studies.

Access to the database is restricted and access will be provided by the Study Management Team. The access arrangements will be closely monitored by the Study Management Team to ensure that access is removed when involvement in a project ends.

2 Who Should Use This SOP

This SOP should be used by members of the Study Management Team.

3 When this SOP Should be Used

This SOP should be used when creating user accounts on REDCap and when maintaining data access groups.

4 Procedure(s)

REDCap Administrators

REDCap administrators, also known as superusers, oversee the REDCap system and its settings. They can do things that REDCap regular users can't do directly. By default, no administrator rights are given or should be granted to new users. Administrator rights will only ever be given to internal Trust staff and limited to a maximum of 4 users. The REDCap administrators will be reviewed when there are any changes in the team which may necessitate adding or removing administrator rights.

The Research Programme Manager and Research Project Manager are the R&D administrators on for the Trust with the following access:

1. **Set REDCap Administrator Privileges –** User can access the 'Administrator Privileges' page (i.e., this page), and can set admin rights for any user.

2. **Manage user accounts –** User can access, modify, and (if using Table-based authentication) create REDCap user accounts. The following pages can be accessed and utilized: Browse Users, Add Users, User Allowlist, and Email Users.

3. **Access to Control Centre dashboards –** User can access and utilize all pages listed under the 'Dashboard' section of the Control Centre's left-hand menu.

4. **Access to all projects and data with maximum user privilege**s – User has full access to all REDCap projects in the system and has maximum privileges within those projects. Within the Control Centre interface, the user can access

and use the following pages that pertain to project administration: To-Do List, Edit a Project's Settings, Survey Link Lookup, and API Tokens.

Members of the Trusts Analyst team are the IT Administrators with the following access:

1. **Access to all projects and data with maximum user privileges** – User has full access to all REDCap projects in the system and has maximum privileges within those projects. Within the Control Centre interface, the user can access and use the following pages that pertain to project administration: To-Do List, Edit a Project's Settings, Survey Link Lookup, and API Tokens.

2. **Modify system configuration pages** – User can modify settings on all system configuration pages in the Control Centre, which includes all pages listed under the 'Miscellaneous Modules' and 'System Configuration' sections on the left-hand menu. Note: If the user does not have this specific privilege but does have at least one other administrator privilege, they may still access and view the system configuration pages but only in read-only mode.

3. **Perform REDCap upgrades** – User can access tools used for upgrading the REDCap software, including notifications about new versions available and also accessing the Easy Upgrade feature (if enabled). Note: This admin privilege does not apply when upgrading REDCap using traditional methods (i.e., when not using the Easy Upgrade) because the traditional upgrade process occurs mostly outside of the REDCap user interface in a database client and via direct server access.

4. **Install, upgrade, and configure External Modules** – User has the ability to install External Modules from the REDCap Repo, and can enable and configure them at the system level. This does not apply to enabling and configuring an External Module in a project, which is governed by other user privileges. Note: If the user does not have this specific privilege but does have at least one other administrator privilege, they may still access and view the External Modules page in the Control Centre but only in read-only mode.

REDCap User Access

REDCap users must be given access to the database by an R&D Administrator. Instructions for adding a user account can be found in Appendix A. Access will only be given using an email address only they have access to for security and audit purposes. No accounts will be created for shared mailboxes. This access will grant users access to the system and not to a specific project.

Internal staff who will directly be involved in the management of the project will be given privileges related to Project Design and Setup, User Rights and Data Access Groups. These staff will be referred to as the Project Managers. Details on how to set up and design a project using REDCap can be found in SOP XXX.

Users who are responsible for data collection on a research study will be given access to Projects by the relevant Project Manager. Instructions for providing access to a project can be found in Appendix B. The Project Manager will not be able to give access to specific projects until an Administrator has created a user account for the individual.

Access to projects must only be given to individuals on receipt of a copy of a research CV (and GCP if appropriate) and the delegation log detailing that they have been delegated responsibilities for data collection and/ or data querying. Training on the use of REDCap will be provided at the Site Initiation Visit (SIV) for the users.

For studies involving more than one participating site Data Access Groups (DAG) will be required. Instructions for creating a DAG can be found in Appendix C. Only users within a given DAG will be able to access records created by users within that group. Users not involved in the management of a project will be assigned to project specific DAGs made up of other users from their Trust/Institution to ensure data access is as limited as possible. Responsibility for this will lie with the project manager. For studies involving a single site a DAG will generally not be required unless there are masking requirements that may necessitate restricting access to the data for some staff.

Project Managers will be responsible for removing users from individual projects when access is no longer required. They should also notify the R&D administrators to allow user accounts no longer linked to any projects to be disabled.

5 Related SOPs and Documents

Cross-reference any other SOPs, documents or forms that are related to the SOP you are writing.

6 Appendix A- Adding a user account

1. Requests for a user account made to the REDCap administrator (Research Programme or Project Manager). The request should include:
    a. Name
    b. Email address (this must be an individual email address, accounts will not be created for mailboxes)
    c. Institution and projects being worked on
    d. Brief reason for request
    e. If access to a DAG is required this must be authorised by PI or delegate member of the study site team.
2. Upon receipt of a complete request the administrator should access the control center home page within REDCap
3. Under Users – “Add Users (Table-based Only) – create single user.
4. Usernames will be the same as Trust usernames for internal staff. For external staff the first 3 letters of their ODS code to easily manage site staff
5. User’s sponsor should be listed as the PM of the project requiring access
6. Expiration date should be left blank as standard
7. Users site and projects they are working on should be added in the miscellaneous comments section.
8. “Allow this user to create or copy projects?” should be unticked before creating any accounts for ALL external users. As standard this should also be unticked for internal users except those who have obtained explicit permission from the Programme Management team for this and undertaken appropriate training.
9. Click save

7 Appendix B- Giving access to a Project

1. Select the project that you need to provide access to.
2. Under ‘Applications’ which can be found on the left of the page select ‘User Rights’.
3. On this page you can create standard roles for the project which will allow for consistency across users.Alternatively you can add users
4. To create a role:
   4.1 Enter a role name into the free text box
   4.2 Select ‘Create Role’
   4.3 Assign the relevant ‘Basic Privileges’ which are located to the left of the page. N.B the highest level privileges should always be unchecked.
   4.4 Assign relevant ‘Privileges for Viewing and Exporting Data’ which are located to the right of the page.
   4.5 Select ‘Create role’
   4.6The role should now be available to assign to users.
5. To add a user to a specific role you will need to add the individuals name to the ‘Assign new user role’ box and select the appropriate role from the assign role box.
6. To add a user with custom rights you will need to add the individuals name to the ‘Add new user’ box and select the ‘Add with custom right box’. From here you will be given the option to select the right that can be assigned to the user.
7. From this page you can view the users assigned to a project and make any changes to them.

8 Appendix C- Creating Data Access Groups

1. Only existing project users can be assigned to data access groups. Users must first be added to a project as usual, through the User Rights page.
2. Select the project that requires a Data Access Group.
3. Under ‘Applications’ which can be found on the left of the page select ‘DAGs’.
4. To create a Group add the name of the site to the ‘Enter new group name’ box and select ‘add group’
5. To ‘Assign a user to a group’ select the user from the list and the appropriate group and select ‘assign’.
6. A list of all project DAGs and users will be shown in the table on the DAG page. The DAG users can be edited on that table.
7. When a user’s involvement in a project ends or they change sites the DAG must be amended accordingly.