User Rights and Roles

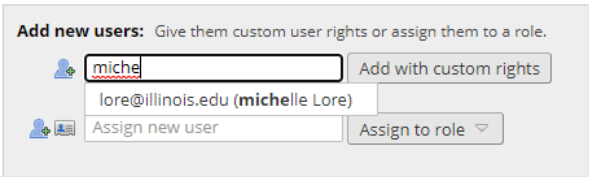
Limiting who has access to what information in REDCap is one of the best ways to ensure that data is protected and validity is maintained. One of the great features in REDCap is the ability to limit access to various data features, such as editing, exporting, or locking records. This can be done by assigning individual user rights, or by creating "User Roles" that have defined rights, then adding users to a role.

In accordance with the HIPAA Privacy Rule, user rights should be set according to the "minimum necessary" standard – limiting access to data and data privileges according to the minimum necessary for individuals to complete their assigned tasks. This document provides suggestions about how to create user roles and assign user rights to maximize data protection. These suggestions may not be appropriate for every project, nor will every project have all the roles defined.

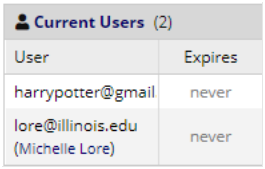
Adding Users to Projects

Only people with REDCap accounts will be able to access projects, even if their email address has been added to a project. There are two ways to tell if someone has a REDCap account.

First, when typing in the name of a potential user, REDCap will suggest people who already have accounts. Below, note that REDCap has suggested "Michelle Lore" as a user, but did not suggest anything for "Harry Potter." Michelle has a REDCap account, but Harry doesn't.



The second way to check is by looking at the table of "Current Users" on the "Project Home" tab. For people with REDCap accounts, both their email address and name will appear. For email addresses not attached to a REDCap account, only the email address will appear.



Current Users (2)

User	Expires
harrypotter@gmail	never
lore@illinois.edu (Michelle Lore)	never

User Rights Definitions

The following are explanation of user rights. Rights that are in **bold** should be limited to select members of the research team.

- *Expiration*: Sets an expiration date for a user's access to a project; an expiration date can be set when the user is added or by clicking in the "Expiration" column next to the user's name on the "User Rights" page after the user is added.

- ***Project Design and Setup***: Allows the user the ability to change the structure of the project (e.g., variable names, instrument fields), utilize the data dictionary, and enable/disable project features and modules.
- ***User Rights***: Gives the user the ability to assign and change rights for other users on the project; any individual with this right can alter privileges for all other users.
- *Data Access Groups:* Gives the user the ability to create and assign users to Data Access Groups (DAGs); see below for more information on using DAGs.
- ***Privileges for Viewing and Exporting Data:*** This table lists all instruments (surveys and forms) in the project and the data viewing and export rights that can be set for each instrument. To set the same privilege to all instruments, click on the name of the privilege you would like to assign under the "Data Viewing Rights" and/or "Data Export Rights" title.
    - ***Data Viewing Rights***: These rights pertain to a user's ability to view or edit data on a web page in REDCap (e.g., data entry forms, reports) and can be customized for each instrument within a project; this privilege has no effect on a user's ability to import or export data. There are three, mutually exclusive options for viewing data:
        - *No Access:* User will not be able to view the data entry form for any record, nor will they be able to view fields from that instrument on a report; any text (e.g., names, MRN) used for custom record labeling will still be visible.
        - *Read Only*: User will have the ability to view records but cannot edit records.
        - *View & Edit*: User will be able to view and edit records; this includes filling in or finishing surveys for participants.
            - ***Edit Survey Responses***: This is a privilege specific for users with "View & Edit" rights that allows users to edit participant-submitted answers; this is typically reserved for highest level users.
    - ***Data Export Rights:*** These rights pertain to a user's ability to export data from the project, whether through the Data Exports page, API, Mobile App, or in PDFs of instruments containing record data. This privilege has no effect on a user's ability to view or import data. There are four, mutually exclusive options for exporting data:
        - *No Access:* User is not allowed to export any data from the instrument.
        - *De-identified:* User can only export de-identified data from the instrument; this export would remove any free-form text fields, date/time fields, and other fields marked as identifiers in the instrument prior to export.
        - *Remove All Tagged Identifier Fields:* This export would remove any fields marked as identifiers prior to export.
        - *Full Data Set*: User can export data from the full instrument, including identifiers.
- *Add/Edit/Organize Reports*: Gives the user the ability to add and/or edit reports; data visible in any given report may be affected by a user's Data Viewing Rights.
- *Stats & Charts*: Allows the user to view graphical information of all numerical and categorical variables, links for cleaning notable data, and descriptive statistics for all variables.
- *Survey Distribution Tools*: Gives the user access to survey distribution tools (e.g., public survey link, participant list, and survey invitation logs).
- *Calendar*: Allows the user to track project events, as well as organize the project schedule; any user with this right can add, delete, or modify calendar events.

- *Data Import Tool*: Gives the user the ability to import data directly into the project, bypassing manual data entry; this right is independent from Data Viewing Rights.
- *Data Comparison Tool*: Allows users to view two records side by side for comparison; if double-data entry is enabled, data entered between two users can also be compared.
- ***Logging***: Allows user to view logs of all occurrences, including data exports, design changes, record history (creation, updating, and deletion), creating users, record locking, and page views.
- *File Repository*: Allows user to utilize the file repository for storing and retrieving any files or documents used for the project.
- *Data Quality (create/edit rules)*: Gives the user access to data quality features, including creating and editing data quality rules.
- *Data Quality (execute rules)*: Allows the user to execute existing data quality rules.
- ***API (export/import/update)****:* Allows the user to access API features such as viewing API tokens, requesting tokens, and the API Playground; rights to either export or import data via API can be selected.
- *Create Records*: Allows the user to create new records in a project.
- ***Rename Records:*** Gives the user the ability to change the key identifier of a record (e.g., record_id).
- ***Delete Records***: Gives the user the ability to delete records from a project; in longitudinal projects, data for all events/arm may be deleted.
- *Record Locking Customization*: Gives the user the ability to customize record-locking text; this is a feature used to give "meaning" to the locking action.
- ***Lock/Unlock Records (instrument level)***: Locking data can help ensure data validity, as it limits the ability of some users to edit records after they've been entered. The following are the three, mutually exclusive options for locking records:
    - *Disabled:* User is not allowed to lock or unlock records.
    - *Locking/Unlocking*: User can lock/unlock records.
    - *Lock/Unlock *Entire* Records (record level)*: Allows the user to lock all forms/surveys at once for a given record.

Data Access Groups (DAGs)

Data access groups provide another way for users to customize project data accessibility. This may be useful in cases of multi-site or multi-group projects that requires certain groups of users to have limited access to project data. For example, a project administrator of a study conducted across multiple institutions may set up DAGs so that users can only access data collected from their respective institution.

Only users within a given DAG can access records created by users within that group. This includes being able to view records on data entry forms, in reports, and in exported data sets. A user can be assigned to multiple DAGs and given additional privileges (DAG Switcher Feature) to switch between DAGs at will. If a user is assigned to multiple DAGs *and* has the right to switch between them, they will see a blue banner at the top of every project page that will present them with the option to switch to another DAG. Users must have "Data Access Groups" rights to create, assign, and re-assign other users to groups.

User Access Dashboard

Any user with user rights privileges will also have a "User Access Dashboard" that is accessible on the "My Projects" tab in REDCap. This dashboard will show a user a summary of all the projects in which they have user rights privileges, as well as who has access to each project. The dashboard should be reviewed monthly to ensure that project access is accurate.

Suggested User Roles

- *Principal Investigator:* Primary individual in charge of and responsible for the proper conduct of a research project.
- *Project Administrator*: Person who fulfills day-to-day responsibilities within and pertaining to the project and the Illinois REDCap system.
- *Data Entry*: Person only responsible for the creation of records and entry of data.
- *Data Monitor*: Person responsible for monitoring the implementation, conduct, and data quality of the research project.
- *Statistician*: Person responsible for analyzing collected data or advising on analysis.

Suggested User Rights for User Roles

	Principal Investigator	***Project Administrator***	***Data Entry***	***Data Monitor***	***Statistician***
Project Design and Setup	X	X			
User Rights		X			
Data Access Groups	X	X			
*Data Viewing Rights**	View & Edit	View & Edit	View & Edit	Read Only	Read Only
*Data Export Rights**	De-identified	De-identified	No Access	No Access	De-identified
Reports and Report Builder	X	X		X	X
Graphical Data View and Stats	X	X		X	X
Calendar	X	X		X	
Data Import Tool		X	X		
Data Comparison Tool		X		X	
Logging	X	X		X	
File Repository	X	X		X	
Record Locking Customization		X			
Lock/Unlock Records	Locking/ unlocking	Locking/ unlocking	Disabled	Disabled	Disabled
Data Quality (create/edit rules)		X		X	
Data Quality (execute rules)	X	X		X	X
Create Records		X	X		
Rename Records		X			
Delete Records		X			

*Since these rights are granted at the instrument-level, privileges can vary from instrument to instrument based on content and need to meet the minimum necessary standard of HIPAA.