Assigning User Rights: Guidance and Troubleshooting

***It is the responsibility of the project manager or PI or Project Owner to assign users to their project and give them the appropriate rights/permissions.***

**Tip:** There should always be *at least* two users (including yourself) on your project just in case you are on vacation or sick leave and the project needs to be accessed in your absence.

**Steps for Creating a New User**

Ensure the new user has registered for a REDCap account at [https://www.ctsi.ufl.edu/research/study-design-and-analysis/redcap/](https://www.ctsi.ufl.edu/research/study-design-and-analysis/redcap/) (registration can be found under “Login to or register for REDCap,” located about 1/2 of the way down this webpage).
After the new user has registered for a REDCap account, go to the project you would like to add them to. A list of your projects can be found under “My Projects.”

Once you are in your project, go to “User Rights” which is listed on the left-hand side bar under Applications.

**Note:** If you do not see “User Rights” under the Applications menu, then you do not have permission to add users to this project. You’ll need to contact someone on the project who does have this permission.
Once you have gone into “User Rights,” you will see a list of users that already have access to your project (if applicable) and which permissions they have (see below).

To add a new user, type their GatorLink user name into the “Add new user” field (shown below) and hit the **Add with custom rights** button.

**Example:** for the user John Doe, if their GatorLink email is: john.doe@ufl.edu, their user name would be john.doe (**do not add the @ufl.edu**) when entering in their GatorLink user name).

Correct way: john.doe  Incorrect way: john.doe@ufl.edu

Once you have entered in the new user’s GatorLink user name and hit the “Add new user” button, another screen will appear that lists all the rights that are available (see next page). Now you are ready to assign this user rights! The default settings for each new user are shown on the next page.
Guide for Assigning Individuals Certain Rights (based on roles)

The Project Investigator / Project Owner is responsible for assigning, restricting and maintaining the roles and authorizations for project members to use specific features and functions in REDCap via the application’s User Rights module.

Users should be assigned minimum necessary rights and access to protected health information (PHI) based on job requirements.

In addition to the above and specific to projects collecting sensitive data it is the responsibility of the PI/Project Owner to assign only Full Data Export rights for projects with PHI to those individuals trained to protect PHI.

While we can provide general guidelines for granting User Rights, it’s important to keep in mind the specifics in your protocol when granting permissions. These lists provide an idea of what would likely be necessary in a typical research project:

PI/Lead Coordinator/Project Owner:
- Project Setup and Design
- User Rights
- Data Access Groups
- Export full data sets
- Add/edit reports
- Manage survey participants
- Logging
- Create/Rename/Delete records
- Mobile App/API privileges as needed
- View/edit all forms

Other Coordinators/Research Assistants
- Add/edit reports
- Manage survey participants
- Logging
- Create records
- Mobile App/API privileges as needed
- View/edit forms as needed

Data Entry Personnel
- Create records
- View/edit forms for which they are entering data
- Mobile App privileges as needed
In summary, the **User Rights** page enables you to:

- Add and remove access to your project for other REDCap users
- Control which Applications each user can access for your project
- Control the record operations that each user is permitted to perform
  - Create records
  - Rename records (i.e. edit a record id)
  - Delete records
- Control the level of access each user is permitted to each specific data collection form
  - No access
  - Read-only access
  - Full edit access
- Define roles – templates of permissions – to which users may be assigned

In general, users should be given access only to the modules that they require, and no more. This will increase the security of your project and aid usability by removing unnecessary clutter from a user’s view.

At the bottom of the page are three buttons:

- Save Changes
- Cancel
- Remove User: remove the user from your project

**Removing a User**

To remove a user from your project, select their name from the User Rights list and click on Edit User Privileges. You then click on the “Remove User” button.
Please note, if you wish to remove a user from your project and that user has been assigned to a role, you must first remove them from the role and then remove them as a user.

An alternative to removing the user is to expire them as a user by putting the last date they should have access to the project in the expiration date field of their user rights.

Adding a Collaborator from Outside UF

To access UF’s REDCap a user must have a GatorLink Username. Here is a link to a guide to assist with getting REDCap access for a non-UF Users.

https://www.ctsi.ufl.edu/files/2017/06/GatorLink-access-for-non-UF-users.pdf
Create a Role

Creating a role is similar to creating a user with custom rights: enter a name for the role (e.g. “Project Manager”, “Data Entry” etc.) and click “Create Role”.

Configure the rights associated with the role and click “Create role”.

Add a New User to a Role

Enter the user’s name or username into the “Assign new user” text box, click “Assign to role” and select the role to which the user should be assigned.
Change a User’s Role

You can change a user’s role (or assign an unassigned user to a role) by clicking on the user’s name, then clicking “Assign to role” or “Re-assign to other role” and then selecting the role.
Summary of Basic User Rights

Expiration Date – Gives user access up until a specified date. Used mostly for temporary employees, such as students performing data entry.

Project Design and Setup – Allows user to design/setup project. Allows user to rename a project. Allows user to make changes to a project. Allows user to delete the project. It is highly recommended that only the highest-level users be given this privilege since editing and deleting a project could cause permanent data loss.

User Rights – Allows user to assign and change user rights for all those assigned to the project, including themselves.

Data Access Groups – Allows user limited access to certain project records by using Data Access Groups, in which only users within a given Data Access Group can access records created by users within that group. This may be useful in the case of a multi-site or multi-group project that requires that groups not be able to access another group's data.

Data Export Tool – Allows user to export data into Excel, SPSS, SAS, R and Stata.
No Access: No data exporting can be done.
De-identified: Can only export data that is not classified as PHI in the project.
Remove all tagged Identifier fields: Excludes tagged PHI fields from data export.
Full Data Set: All data can be exported, including PHI, from the project.
Add/Edit/Organize Reports: Allows user to view all reports (but not necessarily all data in the reports), create/edit reports.
Reports & Report Builder – Allows user to build and save custom reports, which will query the project in real time and display the resulting data in a table format.
Stats & Charts: Allows user to view all project data in aggregate graphical format and as descriptive statistics.

Survey Distribution Tools – Allows user to distribute surveys via links, survey invitations, survey reminders, create custom survey links.

Calendar – Allows user to view calendar and schedule patients (internally only, not connected to EPIC) using the scheduling module and the Calendar Application.

Data Import Tool – Allows user to import data into project using the data import template (Excel).

Data Comparison Tool – Allows user to compare two records currently in the project.

Logging – Allows user to view all project activity (which users have done what) under ‘Applications.’

File Repository – Allows user to view and open the files that are stored in the file repository under ‘Applications.’
Data Quality - Allows user to execute data quality rules upon project data to check for discrepancies in the data, such as missing values, field validation errors, and outliers.
Create & Edit Rules: Allows user to create/edit Data Quality Rules.
Execute Rules: Allows user to execute existing Data Quality Rules.

API – The REDCap API is an interface that allows external applications to connect to REDCap remotely, and is used for programatically retrieving or modifying data or settings within REDCap, such as performing automated data imports/exports from a specified REDCap project.

REDCap Mobile App – Allows user to collect data offline in the mobile app. User could also be allowed to download data for all records to the spp.

Create Records – Allows user the ability to create new records. If users do not have this privilege, they will not see the option to create new records, but will only be able to access existing records.

Rename Records – Allows user the ability to change record names. If a user attempts to rename a record to a value that matches the name of another record that already exists, they will be prevented from doing so.

Delete Records – Allows user the ability to permanently delete all data for a given record. Once performed, there is no way to retrieve the data that was deleted. It is highly recommended that only the highest-level users be given this privilege since it causes permanent data loss.

Record Locking Customization – Allows user to have access to the Record Locking Customization Application, used for customizing the Record Locking option and E-signature option on data collection instruments.
Disabled: User cannot lock or unlock records
Locking/Unlocking: User can lock and unlock records
Locking/Unlocking with E-Signature Authority: User can lock and unlock records and gives them e-signature privileges to apply an e-signature to forms.
Allow locking of all forms at once for a given record: Allows user to lock all records across the project for an individual subject.
# Summary of Data Entry Rights

The Data Entry Rights section allows you to control access to individual forms and surveys. The default setting is that all users will have access to view and edit every form in the project but this can be changed by selecting either “No Access” or “Read Only” for each form.

- **No Access**: User cannot view or edit form at all.
- **Read Only**: User can view the form but cannot change or add data to the form.
- **View & Edit**: User can view and change data to the form.
- **Edit Survey Responses**: User can change survey responses.

### Data Entry Rights Table

<table>
<thead>
<tr>
<th>Form Type</th>
<th>No Access</th>
<th>Read Only</th>
<th>View &amp; Edit</th>
<th>Edit Survey Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demographics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Exam</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Survey (survey)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultation Survey (survey)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*NOTE: The data entry rights *only* pertain to a user’s ability to view or edit data on a web page in REDCap (e.g., data entry forms, reports). It has no effect on data imports or data exports.*