

**Project Users, User Privileges, and Access to PHI**

Access to project information is granted at the project level. Each user has their own account, and their user account will only have access to REDCap projects that they themselves have created or to projects to which other users have granted them access.

User privileges are granular on the project level and can be modified within any given project by someone with proper privileges. The creator of the project will automatically be given full rights to the project, after which they may grant other users access. External (non-UCH/UConn) user accounts will not be allowed to create their own project to ensure they have a collaboration with UCH/UConn staff on each project.

**Project Users:** Each REDCap project has users. These are the specific users with *REDCap accounts* that can access that project. In order for someone to be added as a user to a project, they first need a UCH REDCap account. When a user account is added to a project, the user must be assigned a role or given a set of custom permissions. The role or permissions given to a user account is determined at the project-level settings and determines a user's access to data and ability to make changes in that specific project. For a detailed review of the user rights settings that can be granted or restricted, please see Table 1 below. This table details the potential to access PHI.

**User Roles:** Each project can have pre-defined user roles. Then individual users can be assigned to a role. This is helpful, for instance, if a project will have a number of data entry staff who only need access to certain parts of the project, or a statistician who may need to export data but not enter data. By setting up a pre-defined user role, it streamlines the process of adding new users to a project.

**User Rights Management:** User rights management is the responsibility of the PI and project manager (the person who creates the project) - and/or the users they add to the project with User Rights access. User roles and individual user access rights should be set appropriately and reviewed periodically.

Data Access Groups can be implemented to help segregate users and the data they enter by placing users into data access groups, after which they will only be able to access records created by someone in their group. This particular feature is entirely optional but is especially helpful in certain situations, such as for multi-institutional projects where the data entered by one institution should not be accessible or viewable by other institutions with access to that same project.

**Summary of Best Practices for User Rights Management in REDCap***(it is the responsibility of the PI and study team to ensure these practices are followed/implemented)*

* **ONLY provide needed access rights**: Only provide user rights that a person actually needs.  DO NOT just check all possible options in the User Rights section in REDCap.  This is especially important for the high-level roles of "Project Design & Setup" and "User Rights".  Additionally, DO NOT select "REDCap Mobile App" rights if you are not using the Mobile App as this complicates changes to your project.
* **Set expiration dates for users:** If you are adding a user to a project who you know will need access to the project for a limited amount of time, set an expiration date for their access at the time you add them to the project.
* **Review your User Access Dashboard periodically**: The User Access Dashboard will show all of the users for all of the projects that you managed User Rights before. Review it at least every six months to ensure that all users have the appropriate level of access to the projects they are on.
* **Create and utilize User Roles in your project:** A User Role has a pre-defined level of access. For instance, you might create a user role for Data Entry, that allows a user to enter data but not change project settings or delete records.
* **Consolidate sensitive information in one instrument**: If there are users who should not see identifiable information in the project, the best solution is to keep all of the sensitive information on one instrument and restrict read access to it.
* **Make use of Data Access Groups (DAGs) (for multi-site projects)**: Data Access Groups allow users to be assigned to a group (for instance, a study site) and then only have access to records from that particular DAG.
* **Have a process for when study team members leave their role**: If you have a study team member who is departing, make sure their access to your REDCap project is expired. It is also important to ensure that their account is not tied to any project settings (for instance, API tokens or automated survey invitations) that will need to be transferred over to another study team member.

|  |
| --- |
| List and Description of User Rights Permissions |
| USER RIGHT | **ACCESS** | **NOTES** | **POTENTIAL ACCESS PROTECTED HEALTH INFO (PHI)?** |
| Expiration Date | Automatically terminates project access for the user on the date entered. |   |   |
| Project Design and Setup | Grants user access to add, update, or delete any forms within the project. Also allows users to enable and disable project features and modules. | This should be allocated only to trained study members and should be limited to a very few number of users per study. |   |
| User Rights | Grants user access to change the rights and privileges of all users on a particular project, including themselves. | **WARNING:** Granting User Rights privileges gives the user the ability to control other users’ project access. This user should be very trusted and knowledgeable about the project and REDCap. Giving user rights to team members should be a carefully thought-out decision. The consequences of poor user rights assignments could be damaging to both the security and integrity of your project. For instance, giving record deletion or project design rights to an unqualified person could result in data loss or database integrity issues. | **YES.** Users can change their own User Rights and grant access to any module where PHI can be viewed or downloaded to a device. |
| Data Access Groups | Grants user access to create and add users to data access groups. User should not assign their self to a data access group or they will lose their access to update other users to data access groups. Therefore, users with this privilege should be able to see all project data regardless of group. | For multisite studies, this allows the ability to place barriers between sites' data (i.e. group A cannot see, export, or edit group B's data). |   |
| Data Exports | Grants user “No Access”, “De-identified Only”, “Remove all tagged Identifier fields” and “Full Data Set” access to export all or selected data fields to one of the 5 default programs in REDCap (SAS, SPSS, R, Stata, Excel). Default Access: De-Identified; De-identified access shifts all dates even if they are not marked as identifiers. Non-validated text fields and note fields (free text) are also automatically removed from export. "Remove all tagged Identifier fields" ONLY removes fields marked as identifiers, and does NOT automatically remove non-validated text fields or field notes, and does NOT date shift. In reports and in the API data exports, any fields that have been tagged as "Identifier" fields will be removed from the export file. In the PDF exports, it will include the Identifier field but it will indicated with text [\*DATA REMOVED\*]. | **WARNING:** The "de-identified" and "remove all tagged identifier field" options are contingent upon correctly flagging identifiers in each field. It is advised to mark all PHI fields as identifiers and restrict export access to “de-identified”. | **YES.** PHI can be exported and downloaded to a device. Exporting data is NOT linked to Data Entry Rights. Users with Full Export Rights can export ALL data from all data collection instruments. Please see the “Data Exports, Reports, and Stats” FAQ for additional info. |
| Add / Edit Reports | Grants user access to build reports within the project. If the user does not have access to a data collection instrument that the report is pulling data from, those fields will not appear in the report | For complex querying of data, the best results are acquired by exporting data to a statistical package. | **YES.** Depending on Data Entry Rights, PHI can be viewed. |
| Stats & Charts | Grants user access to view simple statistics on each field in the project in real-time. If the user does not have access to a data collection instrument, that instrument will not be listed on the page. | Outliers can be identified and clicked on which will take you immediately to the record, form, and field of the individual with the outlier data. | **YES.** Depending on Data Entry Rights, PHI can be viewed. |
| Survey Distribution Tools | Grants user access to manage the public survey URLs, participant contact lists, and survey invitation log. |   | **YES.** Email addresses (PHI) may be listed for the participant contact lists and invitation logs. Emails can be downloaded to a device. |
| Alerts & Notifications | Grants user privileges in order to access the Alerts & Notifications page. | Previously, only users with “Project Design and Setup” privileges could access the Alerts & Notifications page. Now, users must explicitly be given “Alerts & Notifications” privileges in order to access the Alerts & Notifications page. | **YES.**Email addresses (PHI) may be listed for the alert logs. Logging can be downloaded to a device. |
| Calendar | Grants users access to track study progress and allow users to update calendar events, such as mark milestones, and enter ad hoc meetings. | In combination with the scheduling module, the calendar tool can be used to add, view, and update project records that are due for manipulation. | **YES.** PHI can be entered and viewed in the “notes” field. Data entered can be printed to PDF and downloaded to a device. |
| Data Import Tool | Grants user access to download and modify import templates for uploading data directly into the project bypassing data entry forms. | **WARNING:** This will give the user the capability to overwrite existing data. Blank cells in the data import spreadsheet do not overwrite fields with data. |   |
| Data Comparison Tool | Grants user access to see two selected records side by side for comparison. | Extremely helpful when using double data entry. | **YES.** PHI can be viewed. Data can be printed and downloaded to a device. ALL data discrepancies for all fields in the project are displayed and can be downloaded to users with access to this module – NOT linked to Data Entry Rights or Data Export Tool Rights. |
| Logging | Grants user access to view log of all occurrences of data exports, design changes, record creation, updating and deletion, user creation, record locking, and page views. This is the audit trail for the project. | Useful for audit capability. | **YES.** ALL data entered, modified, and changed is listed in the module, and can be viewed and downloaded to a device. |
| File Repository | Grants user access to upload, view, and retrieve project files and documents (ex: protocols, instructions, announcements). In addition, it stores all data and syntax files when data is exported using the Data Export Tool. | **WARNING:** While users with restricted data export rights will not be able to access saved identified exports, they will be able to view any other sensitive information stored in the file repository such as photos or scanned documents. Limit this privilege to those who should have access to PHI. | **YES.** Depending on Data Export Tool rights, PHI can be downloaded to a device. |
| Data Quality | Grants users access to find data discrepancies or errors in project data by allowing users to create and edit rules; and execute data quality rules. If the user does not have access to a data collection instrument that the query is referencing, access will be denied for query results. |   | **YES.** Depending on Data Entry Rights, PHI can be viewed. |
| Create Records | Grants user access to add records and data to the database. | Basic tool and need of data entry personnel. |   |
| Rename Records | Grants user access to change the record ID. | **WARNING:**This should only be given to trained staff - can cause problems in data integrity. |   |
| Delete Records | Grants users access to remove an entire record. | **WARNING:** Records deleted are records lost. Few, if any, team members should have this right. |   |
| Record Locking Customization | Grants user access to customize record-locking text. | Will only be applicable to users with Lock/Unlock rights. Sometimes used for regulatory projects to provide “meaning” to the locking action. |   |
| Lock/Unlock Records | Grants user access to lock/unlock a record from editing. Users without this right will not be able to edit a locked record. Users will need “Read Only” or “View&Edit” to lock/unlock a data collection instrument. | A good tool for a staff member who has verified the integrity of a record to ensure that the data will not be manipulated further. Works best if a few team members have this right. | **Yes.** Depending on Data Entry Rights, PHI can be viewed. |
| Data Entry Rights | This section grants users access to data entry rights on an instrument level. Users can be given "No Access", "Read Only", or "View & Edit" access. For instruments enabled as surveys, there will also be an option allowing you to grant a user the ability to edit survey responses. | **Important!** These are the rights you should utilize if you are looking to restrict all access to PHI for certain users. To do this, you will need to restrict all PHI fields to one or more instruments, and then not allow read access for those instruments. | **YES** |

* Data Entry Rights - Grants user "No Access", "Read Only", "View&Edit", "Edit Survey Responses" rights to the project's data collection instruments.
* Manage Survey Participants - Grants user access to manage the public survey URLs, participant contact lists, and survey invitation log.
* Calendar - Grants user access to track study progress and allows user to update calendar events, such as mark milestones, enter ad hoc meetings
* Data Export Tool - Grants user "No Access", "De-identified Only" and "Full Data Set" access to export all or selected data fields to one of the 5 default programs in REDCap (Excel, SAS, SPSS, R, Statal). Default Access: De-Identified; De-identified access shifts all dates even if they are not marked as identifiers. Non-validated text fields and note fields (free text) are also automatically removed from export.
* Data Import Tool - Grants user access to download and modify import templates for uploading data directly into the project bypassing data entry forms.
* Data Comparison Tool - Grants user access to see two selected records side by side for comparison.
* Logging - Grants user access to view log of all occurrences of data exports, design changes, record creation, updating & deletion, user creation, record locking, and page views. This is the audit trail for the project.
* File Repository - Grants user access to upload, view, and retrieve project files and documents (ex: protocols, instructions, announcements). In addition, it stores all data and syntax files when data is exported using the Data Export Tool.
* User Rights - Grants user access to change the rights and privileges of all users on a particular project, including themselves.  **We suggest that only the P.I. and the Project Manager have user rights.**
* Data Access Groups - Grants user access to create and add users to data access groups. Users should not assign themselves to a data access group, or they will lose their access to update other users to data access groups. Therefore, users with this privilege should be able to see all project data regardless of group.
* Graphical Data View & Stats - Grants user access to view simple statistics on each field in the project in real-time. If the user does not have access to a data collection instrument, that instrument will not be listed on the page.
* Data Quality - Grants users access to find data discrepancies or errors in project data by allowing users to create & edit rules; and execute data quality rules. If the user does not have access to a data collection instrument that the query is referencing, access will be denied for query results.
* Reports & Report Builder - Grants user access to build simple queries within the project. If the user does not have access to a data collection instrument that the report is pulling data from, access will be denied for the report.
* Project Design and Setup - Grants user access to add, update, or delete any forms within the project. Also allows users to enable and disable project features and modules.
* Lock/Unlock Records - Grants user access to lock/unlock a record from editing. Users without this right will not be able to edit a locked record. Users will need "Read Only" or "View&Edit" to lock/unlock a data collection instrument.
* Record Locking Customization - Grants user access to customize record locking text.
* Create Records - Grants user access to add records and data to the database.
* Rename Records - Grants user access to change the id of record.
* Delete Records - Grants user access to remove an entire record.  **We suggest that only the P.I. and the Designated Project Manager have User Privileges to delete records.**
* Expiration Date - Automatically terminates project access for the user on the date entered.
* API -  (Application Programming Interface) The REDCap API is an interface that allows external applications to connect to REDCap remotely and is used for programmatically retrieving or modifying data or settings within REDCap, such as performing automated data imports/exports from a specified REDCap project. For details on the capabilities of the REDCap API and how to use it, please see the REDCap API documentation.