****

**REDCap: User Rights Definitions**

This page provides an in-depth explanation of the various user rights or permissions that REDCap offers. These rights can be set for an individual user, or by creating or editing a user role. For more general information on user rights management in UCH REDCap, please see [User Rights Management](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fhealth.uconn.edu%2Fclinical-research-center%2Fwp-content%2Fuploads%2Fsites%2F50%2F2024%2F03%2FUser-Rights-Management-1.docx&wdOrigin=BROWSELINK).

|  |
| --- |
| List and Description of User Rights Permissions |
| **User Right** | **Access** | **Notes** | **Potential to Access Protected Health Info (PHI)?** |
| **Expiration Date** | Automatically terminates project access for the user on date entered. |  |  |
| **Project Design and Setup** | Grants user access to add, update or delete any forms within the project. Also allows user 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** | **No Access:**Users are not able to see this section for any personnel on a project.**Full Access:** Grants user access to change the rights and privileges of all users on a particular project, including themselves**Read Only:** Grants user access to view the User Rights page, but without ability to change permissions. | **WARNING:** Granting Full 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.It is recommended that users have 'Read Only' access to allow them to see who is able to make adjustments to User Rights. | **YES, if Full Access.** User can change 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, user with this privilege should be able to see all project data regardless of group. | For multi-site studies this allows the ability to place barriers between sites' data (i.e. group A cannot see, export, or edit group B's data). |  |
| **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 user access to track study progress and allows user to update calendar events, such as mark milestones, enter ad hoc meetings. | In combination with the scheduling module the calendar tool can be used to add, view and update project records which 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. |
| **Add / Edit Reports** | Grants user access to build reports within the project. If 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, 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 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. |
| **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 project are displayed and can be downloaded to user 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 & 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 module, 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 user access to find data discrepancies or errors in project data by allowing user to create & edit rules; and execute data quality rules. If 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 record and data to database. | Basic tool and need of data entry personnel. |  |
| **Rename Records** | Grants user access to change key id of record. | **WARNING:**Should only be given to trained staff - can cause problems in data integrity. |  |
| **Delete Records** | Grants user 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. User 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 few team members have this right. | **Yes.** Depending on Data Entry Rights, PHI can be viewed. |
| **Privileges for Viewing and Exporting Data**Instrument Level Access |
| **Data Viewing Rights** | This section grants users access to data viewing and entry rights on an instrument level. For instruments enabled as surveys, there will also be an option allowing you to grant a user the ability to edit survey responses.**No Access (Hidden):**Users are not able to see this instrument and its associated data in their dashboard, data entry or on reports.**Read Only:** Users are able to see this instrument and its associated data, but are not able to make any changes to the data.**View & Edit:** Users are able to see this instrument and its associated data, and can edit the data. | **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 set "No Access" for those instruments. | **YES** |
| **Data Exports** | **This access does NOT affect the ability to VIEW data on reports, only the ability to export the data. To limit view rights, see the section above or limit report access within the report itself.**Grants user access to export all or selected data fields to one of the 5 default programs in REDCap (SAS, SPSS, R, Stata, Excel).**No Access:**Users are not able to export data for the instrument(s) selected.  **De-Identified:** All non-validated text and note fields will be removed from data export, as well as identifier fields for the instrument(s) selected. Additionally, all date/time fields will be shifted an unknown value between 0 and 364 days. (If you prefer to not shift dates, there is an option upon export to just remove date/time fields entirely.) \*\*This is the DEFAULT export access for all instruments.\*\***Remove All Identifier Fields:** ONLY fields marked as identifiers will be removed from export for the instrument(s) selected.**Full Data Set:** Users are able to export all data fields for the selected instrument(s).  Upon export, users with this access may also alter their exported file by removing identifiers and/or non-validated text fields and/or shifting dates. | **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. User with Full Export Rights can export ALL data from all data collection instruments. Please see “Data Exports, Reports, and Stats” FAQ for additional info. |