User Rights *Best Practices*

HOW TO USE THIS DOCUMENT

This document has four sections identified below. It will familiarize you with user rights and roles in terms of adding users to your project.

Section 1: User Rights Glossary – this chart defines all the user rights that are available to be assigned for each project user, either directly or through the use of user roles (described next).

Section 2: Suggested User Roles – this chart provides a sample listing of user roles and their descriptions. Setting up user roles for your project is optional. User roles are useful for when there are several users on a project with clearly defined roles. User roles may not be necessary for only a handful of users.

Section 3: Suggested REDCap Access by Project Role – this chart combines user rights with user roles, and display the suggested assignment of user rights for each role.

Section 4: PHI and User Rights – this chart analyzes how certain user rights can be granted or restricted for each user on your project, and how their assignment affects access to PHI.

SECTION 1: User Rights Glossary

User Right	Description
Expiration Date	Provide a date for user accounts that you would like disabled after a specific date (e.g., contract employees or temporary staff)
Project Design & Setup	Allows for access to the Online Form Editor/Data Dictionary, and Event Definitions. This privilege allows users to make changes to the structure of the project (e.g. variable names, labels, etc. - aka the metadata) but has no bearing on access to project data.
User Rights	The ability to change individual user privileges. Any person with User Rights access can alter all privileges for all other users. This privilege should only be granted to the highest level users.
Data Access Group	Data Access Groups restrict viewing of data within a project. A typical use of Data Access Groups is a multi-site study where users at each site should only be able to view data from their site but not any other sites. Users at each site are assigned to a group, and will only be able to see records created by users within their group.
Data Exports (No Access)	The Data Export Module allows you to export your project data to Microsoft Excel, SAS, Stata, R, or SPSS for analysis. If No Access is chosen, this link does not appear for the user.
Data Exports (De-identified)	The Data Export Module allows you to export your project data to Microsoft Excel, SAS, Stata, R, or SPSS for analysis. If the De-Identified option is chosen, this means all free-form text fields will be removed, as well as any date/time fields and Identifier fields.
Data Exports (Remove all tagged Identifier fields)	The Data Export Module allows you to export your project data to Microsoft Excel, SAS, Stata, R, or SPSS for analysis. If the Remove all tagged Identifier fields option is chosen, this means, the user would not have the option to export any data that have been marked as an identifier by the project designers.
Data Export Tool (Full Data Set)	The Data Export Module allows you to easily export your project data to Microsoft Excel, SAS, Stata, R, or SPSS for analysis. If full data set option were chosen, the user would have access to all data collected, including identifiers.
Add/Edit Reports	The Report Builder module builds and saves custom reports, which will query the project in real time and display the resulting data in a table format.
Stats & Charts	This module is designed to assist in data cleaning and evaluation. The Plots tab displays graphical representations for all numerical and categorical variables and provides links for cleaning notable data (missing, highest, lowest values). The Descriptive Stats tab displays descriptive statistics for all variables. This includes the number missing values for all questions, and for any questions with numerical answers, it displays minimum and maximum values, mean, median, standard deviation (StDev), and first and third quartiles (Q1, Q3).

Calendar	The Calendar module was designed to track events for the project. When used in a longitudinal design, the calendar is used in conjunction with the scheduling module to link records, events, and data entry forms. The Calendar application also can be used as a project calendar to help organize your schedule and keep track of any upcoming events. It will allow you to add or modify calendar events.
Data Import Tool	The Data Import module may be used for importing data into a project from a CSV (comma delimited) file.
Data Comparison Tool	Necessary only if double-data entry is enabled; allows for the comparison of data entered between 2 users. Is also used to compare any 2 records.
Logging	This module lists all changes made to the project, including data exports, data changes, and the creation or deletion of users. For security purposes, this feature should be restricted to the highest level users.
File Repository	The File Repository is used for storing and retrieving files and documents used for the project. You may upload files to save for retrieval later, or you may download previously uploaded files.
Data Quality (Create and Edit Rules)	The Data Quality module allows users to view potentially problematic data to assist in data cleaning. You may create your own data quality rules or edit, delete, or reorder the rules you have already created.
Data Quality (Execute Rules)	This module will allow you execute data quality rules upon your project data to check for discrepancies in your data. To find discrepancies for a given rule, simply click the Execute button next to it, or click the Execute All Rules button to fire all the rules at once. It will provide you with a total number of discrepancies found for each rule and will allow you to view the details of those discrepancies by clicking the View link next to each.
Create Records	Users with the ability to create records can create a new "Study ID" on the first data entry form by entering a new record name into the text field. If users do not have this privilege, they will not see the text field on that page and will only be able to access and edit existing records.
Rename Records	Renaming a record means that you are changing its "Study ID" to another value. Users with this user privilege will see an editable text field at the top of the first data entry form after selecting a record. That text field will contain the current record name, and by changing its value and saving the form, that record will now be changed to the new value that was designated. If a user attempts to rename a record to a value that already exists, they will be prevented from doing so.
Delete Records	Users with the ability to delete records have the ability to permanently delete all data for a given record. This is done by clicking the Delete Record button at the bottom of any data entry form after selecting a record. For databases with multiple events (databases that are longitudinal), this action will delete all data for all events across all arms. Once performed, there is no way to retrieve the data that was deleted. It is recommended that only the highest level users be given this user privilege since it causes permanent data loss.
Record Locking Customization	Only users with 'Record Locking' privileges can lock and unlock records for a specific form. Once a form is locked for a record, the form will display (for all users) the time it was locked and the user who locked it, and all fields on the form will be disabled/read-only until someone with Lock/Unlock privileges unlocks the form. Access to this module will allow the user to optionally include custom text when the record is locked for each form.

Lock/Unlock Records (disabled)	The user will not have the lock/unlock functionality available to them.
Lock/Unlock Records (locking/unlocking)	The user will be able to lock a record and all fields will be read-only until someone with lock/unlock privileges unlocks the form.
Lock/Unlock Records (locking/unlocking with e-signature authority)	The user will be able to lock a record and all fields will be read-only until someone with lock/unlock privileges unlocks the form. E-signatures are an extension of the record locking/unlocking functionality. Once a data entry form has been locked for a given record in the database, a person with e-signature privileges may then apply an e-signature to that form, if they wish.
Allow Locking on all forms	Allow locking for all forms at once for a given record.
Data Entry Rights (No Access)	The user will not have the ability to view or edit data on a web page in REDCap (e.g., data entry forms). However, they will still be able to view the data on data imports and exports.
Data Entry Rights (Read Only)	The user will have the ability to view but not edit data on a web page in REDCap (e.g., data entry forms). However, they will still be able to view the data on data imports and exports.
Data Entry Rights (View & Edit)	The user will have the ability to view and edit data on a web page in REDCap (e.g., data entry forms). And they are able to view the data on data imports and exports.
Editing Survey Responses	Users with the ability to edit survey responses can alter existing survey data, entered directly by a participant. It is recommended that only the highest level users be given this user privilege.

SECTION 2: Suggested User Roles

User Role	Description
Principal Investigator	Primary individual in charge of and responsible for the proper conduct of a research project, regardless of funding source.
Administrator	Person responsible for assisting the PI in assuring all regulatory issues are addressed and that research standards are adhered to.
Project Coordinator	Person responsible for the day-to-day management of the research project to include subject enrollment and data collection.
Data Coordinator	Person responsible for the development of REDCap data instruments and the overall management of the project data.
Statistician	Person responsible for the development of the study design and the review and analysis of collected data.
Project Staff	Assists other staff as appropriate.
Read Only	Assists other staff as appropriate with limited, read-only access.
Data Entry	Assists with the creation of records and data entry only.

SECTION 3: Suggested REDCap Access by Project Role

<table>
<thead>
<tr>
<th colspan="9">Suggested REDCap Access by Project Role
(See Glossary of Terms and Role Descriptions above)</th>
</tr>
<tr>
<th colspan="2">REDCap Project Role</th>
<th>Principal Investigator</th>
<th>Administrator</th>
<th>Project Coordinator</th>
<th>Data Coordinator</th>
<th>Statistician</th>
<th>Project Staff</th>
<th>Read Only</th>
<th>Data Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td colspan="2">Project Design and Setup</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">User Rights</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">Data Access Group (if applicable)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td rowspan="4">Data Export Tool (select one)</td>
<td>No Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>De-Identified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove Identifiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Data Set</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">Add / Edit Reports</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td colspan="2">Stats & Charts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td colspan="2">Calendar</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">Data Import Tool</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">Data Comparison Tool</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">Logging</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="2">File Repository</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Category	Subcategory								
Data Quality	**Create & Edit Rules**	✓	✓	✓	✓	✓			
	Execute Rules	✓	✓	✓	✓	✓			
Create Records		✓	✓	✓	✓		✓		✓
Rename Records		✓	✓	✓	✓				
Delete Records		✓	✓	✓	✓				
Record Locking Customization		✓	✓	✓					
Lock / Unlock Records	**Disabled**					✓	✓	✓	✓
	Locking / Unlocking	✓	✓	✓					
	Lock/ Unlock with E-sign								
Allow locking of all forms at once for a given record		✓	✓	✓					
Data Entry Rights	**No Access**								
	Read Only					✓		✓	
	View & Edit	✓	✓	✓	✓		✓		✓
Edit Survey Responses		✓	✓	✓	✓				
Manage Survey Participants (for surveys only)		✓	✓	✓			✓		
API	**Export**	✓	✓	✓					
	Import	✓	✓	✓					

SECTION 4: PHI and User Rights

This chart analyzes how certain user rights can be granted or restricted for each user, and how their assignment affects access to PHI.

- The User Right column names the right.
- The Access column explains what the right entails.
- The Notes column lists any helpful tips or warnings.
- The PHI column explains if PHI data is accessed.

User Right	Access	Notes	Potential to Access Protected Health Info (PHI)?
Data Entry Rights	Grants user "No Access", "Read Only", "View&Edit", "Edit Survey Responses" rights to the project's data collection instruments.	WARNING: The data entry rights only pertain to a user's ability to view or edit data on the web page. It has NO effect on what data is included in data exports or downloaded to a device*.	YES. If access to a form with PHI is "Read Only" or "View&Edit", user will be able to view PHI.
Manage Survey Participants	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.
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.
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 (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.	WARNING: The de-identified option is 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 Export Tool" FAQ for additional info.

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.

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. 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 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).	
Graphical Data View & Stats	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 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.

Reports & Report Builder	Grants user access to build simple queries within the project. If user does not have access to a data collection instrument that the report is pulling data from, access will be denied for 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.
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.	
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.
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.	
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.	
Expiration Date	Automatically terminates project access for the user on date entered.		

*Please Note: REDCap is a web-based system. Once data is downloaded from REDCap to a device (ex: computer, laptop, mobile device), the user is responsible for that data. If the data being downloaded is protected health information (PHI), the user must be trained and knowledgeable as to which devices are secure and in compliance with your institution's standards (ex: HIPAA) for securing PHI.