# Table of Contents

- Building a REDCap Project ................................................................. 2
  - Guiding Principles and Background .................................................. 2
  - Procedure ......................................................................................... 2
- Installation Qualification Test .............................................................. 5
- Sample Project Validation Documentation ............................................. 7
- Assigning User Rights ....................................................................... 8
  - Background ..................................................................................... 8
  - Procedure ......................................................................................... 8
- Sample User Rights Grid ................................................................... 9
- Instance Management Database in MS Access ..................................... 10
  - Background ..................................................................................... 10
  - Solution ............................................................................................ 10
  - Advantages/Use cases .................................................................... 10
  - Disadvantages ............................................................................... 11
- MS Access Database Structure ........................................................... 11
- Data Import Procedures .................................................................. 12
Building a REDCap Project

Guiding Principles and Background
The Research Management Team (RMT) provides research staffing support to investigators at the Duke School of Nursing and throughout Duke University Medical Center. RMT personnel are trained in research procedures and operations and are available for assignment to research projects on a short or long-term basis. The RMT is recognized as a Duke Managed Service through a funding partnership with DTMI. The RMT will provide oversight and support for all studies that choose to work with RMT as a managed service.

REDCap is a web application that allows researchers and administrators to quickly create secure, online databases. Data stored through DTMI’s instance of REDCap is stored in secure servers managed by DHTS.

Study investigators who choose to build their own REDCap templates will assume responsibility for all data management and data security activities. RMT will provide assistance with REDCap questions and will push the project into production but will not build the database or train the users to use REDCap.

Procedure
1. Document Collection. Prior to meeting, the RMT may request the grant, study protocol or CRFs for review.
2. Initial Meeting. The RMT manager and RMT database developer meet with the investigator/client to assess project data management needs and recommend appropriate solutions. The RMT may request the attendance of the client’s statistical team if needs include data export for analysis. We may also request the attendance of any potential database users to be present to maximize input for overall database design.
   a. If desired and REDCap is appropriate for the project, then:
      i. RMT personnel introduce the REDCap application to the client, showcasing an actual REDCap Database Project, if available.
      ii. RMT personnel discuss what it takes to build a REDCap Database Project. They acquaint the client with a metadata file, if available, and explain the iterative process of creating, revising, and uploading a file.
   b. The clients have an opportunity to decide if they would like to build the database themselves or have RMT create it for them. Estimates will be provided for both options, if desired by the client.
   c. NOTE: Any PHI collected under a VA IRB and consent may NOT be stored in the DTMI/RMT REDCap instance.
3. Client Build
   a. After the initial meeting, RMT staff emails the client with an example metadata file attached.
   b. RMT personnel create a development-mode REDCap Database Project for the client.
   c. The client edits the metadata file and re-uploads it into the development-mode database until the database is accurate. This process can be repeated as many times as necessary to create a satisfactory database. RMT staff will be available for limited consulting.
d. Once the client is happy with the database, the RMT will review it to make sure that all PHI Identifier fields have been marked, document the database contact persons and purpose in REDCap Control Center’s “Edit Database Settings” tab, then put it into production mode, which will delete all data already entered into the database. The database will then be ready for use.

e. After the database is pushed into production mode, any database changes must be approved by a REDCap administrator.

4. **RMT Build**

   a. **Initial Estimate.** The RMT manager and RMT database developer provide an estimate for proposed work, based on pertinent study info and documents provided by the client. The estimate will include percent effort and fringe of the RMT database developer involved for initial build and a maintenance/support period.

   b. **Document Collection.** The client presents RMT staff with all finalized project documents.

   c. **Metadata Drafting.** RMT personnel build the metadata file to match client project documents.

   d. **Metadata Troubleshooting.** RMT staff proofread each row of the metadata file. In a separate column within the file, RMT staff sign off on each row when it is determined to be accurate.

   e. **Database Drafting.** RMT personnel create a development-mode REDCap Database Project based on the metadata file.

   f. **Database Troubleshooting.** RMT personnel check each question in REDCap’s graphical user interface (GUI) against the project documents, if available. Errors are corrected in a copy of the metadata file. After making one or more edits, RMT personnel update the development-mode database. In a separate excel file with a list of all variable names, RMT personnel puts a mark next to each variable name that has been double-checked for accuracy within the GUI.

      This step will be repeated until each variable name has been double-checked and signed-off upon.

   g. **Client Viewing.** The data manager will meet with the client (and pertinent study team members, if applicable) to present the REDCap Database Project. User rights are assigned to project personnel based on list from client.

   h. **Production.** The database will be reviewed to verify that all PHI Identifier fields have been marked, then pushed into production mode and ready for use.

   i. **Documentation.** The database contact persons and purpose will be recorded under REDCap Control Center’s “Edit Database Settings” tab.

      1. Within REDCap:
         1. Record the database contact persons and purpose under REDCap Control Center’s “Edit Database Settings” tab. (Superuser access only)

      2. Within that project’s database documentation folder within the RMT Folder:
         1. Completed Installation Qualification Test
         2. Row-by-row Excel file of verified fields (see 4.f above)
         3. Production data dictionary
         4. User-rights specifications from the PI or study coordinator. Original electronic communication preferred.

      3. Within the RMT Project Documentation binder:
         1. A printed and signed copy of the Installation Qualification Test.

   j. **Training.** The RMT will provide initial database training for database users.

   k. **Support.** The RMT will provide maintenance according to the terms of the agreement. Support includes:

      1. Phone support
      2. Training for new database users
iii. Adding fields to existing database forms
iv. Editing existing database forms

I. Tracking further changes to user rights or project metadata for projects in production. RMT needs to be able to identify any changes to user rights or metadata modifications that have occurred for the production REDCap project, along with when and why they occurred. Thus:

i. User rights changes
   1. These are recorded in the project’s database documentation folder. Please save copies of original communications from the PI.
   2. For Superusers: record any changes in the “Project Comments” box within REDCap’s control panel. Format: YYYY-MM-DD [comments] [initials]
   3. Remember that changes in user rights must be requested by the PI or responsible Study Coordinator and must meet RMT user rights restrictions for REDCap. Please see REDCap user rights policy for more information.
   4. REDCap users are never to be deleted from a project, only expired.
   5. REDCap users are never to be deleted from the REDCap system, only suspended.

ii. Metadata changes for projects in production are recorded in the database documentation folder.
### Installation Qualification Test

<table>
<thead>
<tr>
<th>Item</th>
<th>Specification / Installation Activity</th>
<th>Tester Name</th>
<th>Signature &amp; Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Confirm that new database has been created.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Verify that database builder has access to the database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Based on model (e.g. CRFs), write project metadata in data dictionary file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Upload the data dictionary into REDCap database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Test that the REDCap database matches the model (e.g. CRFs).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Correct any problems identified during testing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Confirm that user rights have been accurately assigned to project personnel based on list from PI or project coordinator.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Verify that client has been given the opportunity to view the database and make suggestions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Incorporate client suggestions into the database as appropriate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Test that the client suggestions, if any, have been accurately incorporated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Verify that all identifier fields in the database have been flagged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Verify that the ID field (i.e. the first field in the database) is not a PHI field such as MRN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Push the database into production</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Verify that database information page lists database as “in production.”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Test Result:</td>
<td>☐ Pass</td>
<td>☐ Fail</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Tester Signature:</td>
<td>Print Name:</td>
<td>Date:</td>
<td></td>
</tr>
<tr>
<td>Reviewer Signature:</td>
<td>Print Name:</td>
<td>Date: _______</td>
<td></td>
</tr>
</tbody>
</table>
## REDCap Database Production Documentation

### Exercise and Prostate Cancer

<table>
<thead>
<tr>
<th>Date Verified</th>
<th>Notes</th>
<th>Date Fix Applied</th>
<th>Variable / Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>study_id</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>first_name</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>last_name</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>mrn</td>
</tr>
<tr>
<td></td>
<td>Drop down displaying &quot;4 = Dropped Out&quot;</td>
<td>6/30/2010</td>
<td>study_status</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>age</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>race</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>race_other</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>ethnicity</td>
</tr>
<tr>
<td>6/30/2010</td>
<td></td>
<td></td>
<td>marital_status</td>
</tr>
<tr>
<td>6/30/2010</td>
<td>Text validation needs to be number</td>
<td>6/30/2010</td>
<td>education</td>
</tr>
<tr>
<td></td>
<td>Text validation needs to be number</td>
<td>6/30/2010</td>
<td>blet_hr19</td>
</tr>
<tr>
<td></td>
<td>Text validation needs to be number</td>
<td>6/30/2010</td>
<td>blet_speed20</td>
</tr>
<tr>
<td></td>
<td>Text validation needs to be number</td>
<td>6/30/2010</td>
<td>blet_grade20</td>
</tr>
<tr>
<td></td>
<td>Text validation needs to be number</td>
<td>6/30/2010</td>
<td>blet_hr20</td>
</tr>
</tbody>
</table>

**15 Variables**

---

**Name**

**Date**
Assigning User Rights

Background
As the directors of their projects, PIs have the final say over who may and may not have access to their study databases. If the PI delegates this right to a project manager, then the project manager has this right.

While RMT administers the DTMI instance of the REDCap system, RMT does not have the right to decide who has user rights within a particular REDCap database. The PI or responsible party decides which user rights to assign. RMT’s role is simply to make sure that user rights requests remain within the bounds of RMT policy (see 3a., 3b., and 3c. below), then to assign them.

Procedure
1. Before the database goes into production, email responsible party REDCap User Rights Roles.xls.
2. In the Excel file, responsible party enters user rights for users. For each user, responsible party may choose:
   a. One of the pre-packaged user roles.
   b. A customized combination of rights.
3. We receive an email reply with requested user rights. Verify the following:
   a. No users have access to User Rights and Data Access Groups. Access to these two areas always remains strictly among RMT staff and REDCap superusers.
   b. Users lacking Full Data Export rights cannot access to the Audit Log or Report Builder. This is because full data exports are available – either as built-in buttons or as copy-and-paste datasets – in those areas.
   c. No user has e-Signature authority. We do not use this feature because the e-signature functionality is underdeveloped.
   d. Users lacking “create” rights may not have access to the data import module.
4. If 3a., 3b., and 3c. are all verified, assign the requested user rights. If not, communicate with responsible party to find user rights that do meet requirements 3a., 3b., and 3c.
5. Save copy of the email with attached Excel File in the project’s documentation folder.
# Sample User Rights Grid

<table>
<thead>
<tr>
<th>Role</th>
<th>Data Entry</th>
<th>Pi, unblinded</th>
<th>Project Manager, full export</th>
<th>Project Manager, deidentified</th>
<th>Statistician</th>
<th>User Name</th>
<th>Role*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Entry</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pi, unblinded</td>
<td>Y</td>
<td>Y</td>
<td>FULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Manager, full export</td>
<td>Y</td>
<td>Y</td>
<td>FULL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Manager, deidentified</td>
<td>Y</td>
<td>Y</td>
<td>DEIDENTIFIED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistician</td>
<td></td>
<td></td>
<td></td>
<td>DEIDENTIFIED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*reminder: please assign no more rights than users need to do their jobs
Instance Management Database in MS Access

Background
The current security structure of REDCap requires a user be given “superuser” status in order to access statistical modules or generate emails to users. Unfortunately, by making these users “superusers”, you are presented with potential system/security issues and data access concerns.

Solution
To address this, we created a separate tracking database in MS Access. Each week, an authorized user imports selected fields from five MySQL tables that do not contain research data – redcap_auth, redcap_data_access_groups, redcap_projects, redcap_user_information, and redcap_user_rights – into the MS Access database. The MS Access database’s import procedure calculates metrics to match those available in REDCap. The database provides tables to store additional data locally and also provides functionality that has limited availability within REDCap. The database is stored in a secure directory administered by the local IT group, who may grant access to it on a case-by-case basis.

![Screenshot of Access database switchboard. Some text is hidden.](image)

Advantages/Use cases
- Allows users to see general project information without “superuser” designation

The database allows authorized users to see a list of all project within the REDCap system (as of the last data import), as well as associated information such as date created and date moved to production. Because a copy of these data is within MS Access, they may be queried via MS Access’ query tool.

- Allows users to view system metrics without “superuser” designation
The database calculates a subset of the metrics visible within the REDCap Control Center. It also allows users to create their own metrics based on tracking fields not currently available within REDCap, such as “department.”

- Ability to contact users during system outage

The database stores a list of all REDCap users’ email addresses. This externally-stored list allows us to email users with information during server outages, when system unavailability makes it impossible to email users from within the REDCap.

- Facilitates user rights verification

To make sure that REDCap user rights remain current, it is helpful to email the administrators of each REDCap project annually and request that they verify their project’s user rights. The database facilitates this process. It reminds administrators to send emails at the appropriate time, can auto-generate the notification emails on command (including an Excel spreadsheet containing the project’s last known user rights), and provides an area to record all user-rights correspondence.

- Global user rights validation

Because REDCap’s User Rights Schema is module-based, it is possible to unknowingly assign users more access than they require. For example, as of REDCap version 4.3.18, assigning “audit log” rights allows users to export all data entered into the database and assigning “report builder” rights allows users to print a PDF of all data in the database. Utilizing database queries, we can identify instances where inappropriate levels of user access may have been inadvertently given.

Disadvantages

The database does not provide real-time data as downloads are performed on a weekly basis. In addition, many of the features in the database may now be programmed in PHP and direct connections to the REDCap database are available via a REDCap Plug-In.

MS Access Database Structure

The Access database contains two types of tables: tables that contain data dumped straight from REDCap, and data that are hosted locally in the Access database. In order to minimize data curation outside of REDCap, RMT relies on REDCap-dumped data as much as possible. Other tables are only added when REDCap does not have the needed data, such as the data pertaining to the periodic user rights checks.
Data Import Procedures
Data is imported from the REDCap MySQL database into the MS Access database via ODBC. First, a user account is created in the MySQL database with the singular purpose of importing data to MS Access. For this reason, the user account is restricted to SELECT queries (i.e. read-only access) and may only connect to the MySQL database server from an approved IP address. Second, an ODBC DSN is created within the downloader's Windows Control Center's Administrative Tools page. Third, whenever data needs to be downloaded, the downloader opens the MS Access database backend file and clicks a button. The button starts a procedure, which archives the previously-downloaded REDCap data and appends the new REDCap data to the local MS Access tables. To ensure protection of patient confidentiality, data arrives from the following administrative tables only: redcap_auth, redcap_data_access_groups, redcap_projects, redcap_user_information, and redcap_user_rights.
To better ensure account security, password-related fields are not imported into the database.