CCTS REDCap Terms of Use

[Glossary]

- **Project Owner**- It is a Principle Investigator (PI) or a delegate who has the access control for other users and all database design options of a REDCap project. In REDCap, the project owner is the user that has access to the module called, User Rights.
- **Full Access User** - A user that has an account that allows the user to create or copy projects. This user must submit a formal request through the CCTS workflow website to set up an account.
- **Access-Only User** - A user that has an account that adds the user to a particular project. The PI or Project Owner who adds an Access-Only user, determines the appropriate user rights for that user for that particular project. The Access Only User cannot create nor copy projects.
- **Super User** - REDCap admin staff who can set up user accounts, manage REDCap Control Panels and have access to all projects when the project owner's approval is made.
- **REDCap project** – A database created in REDCap. Individual REDCap projects are independent requiring separate project setups, and only accessible by granted users.

I. Projects applied to IRB

- For all projects with a research purpose under IRB regulations, the Principle Investigator (PI) and the IRB number MUST be entered in REDCap Main Project Settings.
- Projects must be moved to production after IRB approval.
- Database modifications in production must be based upon IRB approval.
- REDCap data collection form(s) must be printed in pdf and submitted to IRB for review and approval.
- HIPAA and CITI training are required for all users who access the REDCap project data.

II. User Account

- To become a Full Access User to create or copy a REDCap project, the user should submit the online request form through the CCTS service request page.
- For an Access-Only account, a request can be sent via email to REDCap admin (REDCAPIHRP@UIC.EDU) and must include the project title, PI name and email and the account sponsor's REDCap user ID if she/he is not same as PI.
- An individual outside of UIC can have a UIC REDCap account only if their PI is affiliated with UIC health research.

- User must set their password immediately via the email link that they receive when the account is created and also set the security questions for future password resets.
- REDCap admin creates user accounts at the system level, but will not add or manage each user's access rights to projects. Project owner or PI must add other users with their user rights.
- When any user leaves the university, their sponsor or project manager/owner has the responsibility of contacting the REDCap admin team to have their account removed from the system.
- Users with no activity over 1 year will be suspended, but can send an email request to the REDCap admin team to reactivate the suspended account.
- Users cannot send a request for a password reset for other users. The user that needs to have their own password reset must send an email.

III. User responsibilities

- All project user(s) should understand the fundamental basics of REDCap by taking introductory training materials such as webinars or recorded videos provided by CCTS REDCap admin team, the developer's video tutorials, or the many other resources you can find online from other institutions.
- Users should design the REDCap project properly to collect data that can be used for their research purpose(s).
- Once data is downloaded from REDCap, users must store and share it securely to follow their research protocol. The downloaded/exported data dictionary and collected data is not encrypted when it is outside of our REDCap server.
- User ID/PW must be kept securely without sharing with any other person. If anyone needs access to your project but doesn't have a REDCap account, contact the REDCap admin team at (redcapihrp@uic.edu) and request an account.
- When a project is ready to collect real data, the user MUST move it to "Production Mode" to protect data from unwanted loss due to modifications. The modifications that may cause data loss include deleting fields/forms, changing variable names or choice options, deleting events or removing links between events and forms, etc.
- Any data deletion that occurs due to the user's modifications in development mode will not be retrieved by REDCap IT admin. In production, changes will be reviewed and committed upon the user's approval via email. Once approval is made, any unexpected data loss by the approved change action will not be restored by REDCap IT admin.
- Before moving a project to production, each user must test the database thoroughly by adding multiple test cases to every form and field.
- User must plan data back-up before making any change by downloading the Data Dictionary and exporting the entered data. Exported data containing PHI (Protected Health Information) must be stored securely following all IRB requirements.

- REDCap is an online application to access your database. For the real time data collection in an area with weak internet connection, paper data entry form(s), REDCap mobile app or other alternatives should be considered in advance under study protocol.
- To use REDCap API (Application Programming Interface) and other plugins, users should use their own programming skills and understanding. REDCap admin team only provides general guidelines.

IV. CCTS REDCap Support

- REDCap admin team creates and maintains user accounts with no charge and provides training courses and general instructions and troubleshooting via email. In person REDCap consultation meeting is set-up by user's request submitted to CCTS service request system.
- REDCap support is provided to all UIC health researchers and affiliated people.
- IHRP IT staff updates REDCap to the new version one to two times a year depending on how imperative the update is. A detailed update log will be kept by admin and distributed to users when requested.
- All REDCap project change requests in production mode are reviewed by REDCap admin using system provided review results and emailed to users to get their approval.
- All email requests and inquiries need at least 1-2 business days for REDCap admin to review and complete request(s). In times of high volume, requests may take longer than 1-2 business days to review and complete.
- Email support services for REDCap are available Monday through Friday between the hours of 9 AM and 5 PM. Limited email service for REDCap requests may occur during the campus holidays, and staffs' absence by vacation. An email notification for the closed service days will be sent a week before the closure.
- All planned server downtime due to software updates and other related maintenance tasks will be announced via email to all users. However, unexpected errors in network connectivity on campus or server related issues may cause outages with no prior notice.
- The REDCap admin team may generate some general user statistics such as number of users, projects, types of research projects.
- As a "Super User," REDCap admin can access any project to review the database or to fix any issue only upon the project owner's request.

V. Security Application of REDCap

Technical overview by the developer, Vanderbilt University:

https://projectredcap.org/wp-content/resources/REDCapTechnicalOverview.pdf

Security specs implemented by CCTS REDCap:

Infrastructure

- CCTS REDCap server is in an IHRP climate controlled locked server room and maintained by IHRP IT staff.
- The REDCap application is split between multiple server systems with a load balanced web accessible front-end and the database application stored on a firewalled backend fail-over cluster.
- REDCap uses SSL to encrypt all traffic between the user and the application.
- The web server is backed up regularly. There are two daily backups in addition to hourly backups. **The backup is system level failure only; not for individual project level data retrieval.**

User Authentication

- REDCap validates the identity of end-user by the table-based authentication method which utilizes the storage of username/password pairs in a database table.
- Your password will expire after 1 year; therefore each user must change it.
- When there is no activity on the REDCap page after 30 minutes, user will be automatically logged out.
- 5 failed login attempts will lock out a user.

Project level Access Control

- An individual user needs to have their own user ID and PW to login to our REDCap system.
- Only users selected by the PI or the database owner can access a project.
- The project owner or PI must set up other users' access levels. An access level of "view" or "edit" can be set individually to each data entry form.
- Data Access Group (DAG) is available to limit access only within the same group for multisite studies.

Audit Trails

- All activities made on a REDCap project are tracked and viewable by granted users in "Logging" which can be found in the Applications section in your REDCap dashboard. The user ID and time stamp are logged with the activity details.
- REDCap admin or the super user can view all audit trails in Logging by user's request.

CCTS REDCap and 21 CFR Part 11

Our REDCap provides some key system requirements for a 21 CRF Part 11 applicable study by having some data security tools, audit trails, backups and user access controls as described in the above sections. However, it does not cover the validation procedures and documentation to be 21 CRF Part 11 compliant. The "requirements" aresubjective and vary by different organizations. In our current system, each project user is responsible for performing the procedures with the validation documentation.