Terms of Use

UIC CCTS Biostatistics Core

January 2023

Glossary

REDCap
A secure, web-based application for building and managing online surveys and databases. REDCap was created by Vanderbilt University in 2004.

CCTS
UIC's Center for Clinical and Translational Science. CCTS administers the UIC-specific installation of REDCap and provides training and consultation services for UIC health researchers.

IHRP
UIC's Institute for Health Research and Policy. IHRP manages the REDCap server and IT infrastructure at UIC.

REDCap project
A database created in REDCap with associated data collection forms and settings. Each REDCap project is independent and only accessible by approved users.

Project owner
The creator or manager of a project in REDCap, usually the project's principal investigator or a delegate. The project owner has access to all design options for a REDCap project. The project owner can grant, adjust, and revoke project permissions for other users.

Full Access (Creator or Owner) user
A REDCap user who can create or copy projects.

Access Only (Collaborator) user
A REDCap user who can access one or more projects but cannot create or copy projects.

Sponsor
A full-access user who has requested the creation of accounts for one or more limited-access users. All non-UIC users must have a sponsor affiliated with UIC health research.

DAG
Data access group. DAGs may be created to control which users can access which records within a REDCap project.

Superuser
A REDCap user who can create user accounts and access any project at the request of the project owner. All members of the REDCap admin team are superusers.

User Accounts

New Accounts

1. Any UIC-affiliated health researcher who needs to create or copy REDCap projects can request a full-access user account. To request an account, the user must submit a service request through the UIC REDCap support form and agree to the REDCap Terms of Use.
2. Any individual working on a UIC REDCap project can obtain a limited-access user account, provided he or she is sponsored by a full-access user. Either the limited-access user or the sponsor can request the account by submitting a request through the UIC REDCap support form. Requests must include the limited-access user's name and email address and the sponsor's UIC email address.
3. When a new REDCap account is created, the user will receive an automated email with login information. Upon receipt of this email, the user must choose a secure password and set up security questions for future password resets.
4. A user may request a password reset for his or her own account by submitting a service request through the UIC REDCap support form. A sponsor may also initiate a password reset for a sponsored user via the Sponsor Dashboard.

User Authentication

1. REDCap validates the identity of end users by the table-based authentication method, which relies on the storage of username-password pairs in a database table.
2. Each individual who accesses a REDCap project must have a unique username and password. Users must keep their login credentials private and must not share these credentials with any other person. Group accounts or email addresses (e.g., team@uic.edu) are not permitted.
3. Five failed login attempts will result in a user being locked out.
4. After 30 minutes of no activity by a logged-in user, the user will be automatically logged out.
5. Each user's password will expire after one year.

Project-Level User Access

1. The REDCap admin team creates user accounts at the system level but will not manage users' ability to access individual projects.
2. A project owner may grant or revoke project access to any active REDCap user via the project's User Rights page.
3. A project owner can control each user's level of access to a project, including the ability to edit forms, view or edit records, download data, and control the rights of other users.
4. Users with adequate permissions can create data access groups (DAGs) to control which users can access which records within a REDCap project. DAGs may be useful to partition data for multi-site or multi-group projects.

Account Expiration, Suspension, and Deletion

1. When a REDCap user leaves the university, the user or his or her sponsor must email the REDCap admin team to request that the user account be deleted.
2. Before a project owner leaves the university, it is his or her responsibility to designate a new project owner via the project's User Rights page.
3. Users with no activity for at least one year will have their accounts automatically suspended.
    1. A suspended user can submit a service request through the UIC REDCap support form to request account reactivation.
    2. A sponsor can request a sponsored limited-access user's account reactivation through the Sponsor Dashboard.
4. Limited-access user accounts have a default expiration date of one year from creation. A user's sponsor can manage expiration dates via the Sponsor Dashboard.

5. Users may request deletion of their own accounts from the REDCap system by emailing the REDCap admin team. Account deletion may be initiated by a third party, but no account will be deleted unless the account owner confirms the request by email.

User Responsibilities

General Responsibilities

1. All project users should familiarize themselves with basic REDCap options and capabilities. Introductory training resources, including videos and written manuals, are available on the CCTS website. Additional resources are available through Vanderbilt University, the developer of the platform.
2. Users should carefully consider research design and data analysis needs when designing a project in REDCap.
3. The first field in the first data collection instrument of a project must be an unique identifier (ID) field. This ID cannot be renamed or removed.

Editing Projects

1. Before making changes to a project's forms or fields, users are strongly encouraged to create a backup by downloading the data dictionary and exporting existing data.
2. Forms may be freely modified while a project is in development mode. Any data deleted as a result of modifications **will not** be retrieved by the REDCap admin team. Modifications that may cause data loss include deleting fields or forms, changing variable names or choice options, deleting events, and removing links between events and forms.
3. While a project is still in development mode, each user should thoroughly test every field on every data collection instrument. Test data can be deleted or retained when the project is moved to production.
4. Before real data collection begins, a project must be moved from development mode to production mode. This change will protect against unintended data loss due to project modifications.
5. Once a project has been moved to production mode, further changes will be subject to review by the REDCap admin team. In cases where data is at risk of alteration or deletion, the user will be contacted by email and asked to confirm the changes. Once changes have been confirmed by the user and committed by the REDCap admin team, any unexpected data loss **will not** be reversed.

Technological Considerations

1. REDCap is an online application. Study protocols should include provisions for real-time data collection in situations with weak or no internet connectivity. Possible alternatives include paper data entry forms and the REDCap mobile app.
2. Users who wish to use the REDCap application programming interface (API) and other plugins should have adequate programming knowledge and skills. The REDCap admin team can provide only general guidelines to these users.

Recommendations for IRB-Regulated Projects

REDCap has several options that are compatible with the needs of Institutional Review Board (IRB) processes. The following steps are recommended, thought not required, for human subjects research that is subject to IRB approval.

1. For all projects subject to IRB regulations, the principal investigator and the IRB number should be recorded as part of the project's settings in REDCap.
2. REDCap data collection forms must be exported in pdf format and submitted to the IRB for review and approval.
3. Projects must be moved to production status after IRB approval.
4. Database modifications in production status must be based upon IRB approval.

5. HIPAA and CITI trainings are required for all users who access project data in REDCap. For more information, see the UIC Office of the Vice Chancellor for Research website.

User Support

CCTS Support Services

1. REDCap administration and user support are provided by staff of the UIC's Center for Clinical and Translational Science (CCTS).
2. The REDCap admin team creates and maintains user accounts at no charge and provides training courses, general instructions, and limited troubleshooting to all UIC health researchers and affiliated users. To request email support or a one-on-one consultation, users should submit a request through the REDCap support form.
3. Virtual support is available Monday through Friday, 9 a.m. to 5 p.m. Limited support may be available during campus holidays and staff absences. Users will be notified a week in advance of periods of planned support downtime.
4. The REDCap admin strives to respond to account-related requests with one business day and more complex questions within five business days. In times of high volume, requests may take longer to complete.
5. As superusers, members of the REDCap admin team can access the settings, forms, and database of any project upon the project owner's request.
6. The REDCap admin team may gather some general REDCap usage statistics for reports, including number of users, number of projects, and types of projects.

Software Updates

1. UIC's Institute for Health Research and Policy (IHRP) IT team updates REDCap to the newest version once or twice a year, depending on how imperative the update is. A detailed update log is kept by the REDCap admin team and distributed to users upon request.
2. Planned server downtime due to software updates and maintenance will be announced to all users in advance via email. However, unexpected problems with network connectivity or server-related issues may cause outages with no prior notice.

Security

Infrastructure

1. View a technical overview by the developer, Vanderbilt University.
2. The REDCap server is housed in a climate-controlled, locked server room at IHRP and maintained by IHRP IT staff.
3. 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 back-end failover cluster.
4. REDCap uses SSL to encrypt all traffic between the user and the application.
5. The web server is backed up at hourly and twice-daily intervals. The backups protect against system-level failure only; they do not permit individual project-level data retrieval.
6. The database backup begins every day at 12 a.m. CST and runs for about 8 hours. During this time, users may experience connection failures. The REDCap admin team recommends that users avoid international data collection activities that require login during the system backup time.

Data Security

1. Data stored on the REDCap server is password-protected and encrypted. Once data has been exported and downloaded from the REDCap database, it is no longer encrypted. Users are responsible for

securely managing exported data, which may contain protected health information (PHI), in accordance with research protocols and IRB requirements.

Audit Trails

1. REDCap keeps a log of all changes made to a project, including form modifications, data entry or editing, and data exports. The log includes date and time, username, and details about each action.
2. The project owner and users with adequate permissions can view these audit trails in the Logging module. As superusers, members of the REDCap admin team can also view all audit trails at the request of the project owner.

CCTS REDCap and 21 CFR Part 11

UIC's 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 required to be 21 CRF Part 11 compliant. The "requirements" are subjective and vary by different organizations. In our current system, each project user is responsible for performing procedures with validation documentation.