****

**General Security Overview**

**Infrastructure and Security**

REDCap is deployed in a multi-tiered architecture with separate web, file, and database servers. The REDCap platform is hosted on premise at UConn Health (UCH) and managed by Academic IT Services (AITS) and the Clinical Research Center (CRC). It is secured using the technical controls stipulated by HIPAA. These controls include (but are not limited to): protection behind the firewall in the IT data center with controlled physical access, servers kept up to date with operating system and application patches and upgrades, role-based access to projects, data encrypted while in transmission, daily backup, and regular audits of system events and logs. Servers are patched regularly and scanned for vulnerabilities as well as viruses and malware. UCH REDCap is a **HIPAA-compliant** web platform; however, it is **NOT a 21 CFR Part 11-compliant system** and should NOT be used for studies reporting to the FDA (i.e., IND, IDE, abbreviated IDE, etc.)

In REDCap, all incoming data gets intentionally filtered, sanitized, and escaped to protect against methods of attack, such as Cross-Site Scripting (XSS) and SQL Injection. REDCap has implemented mitigation techniques to prevent common cybersecurity attacks, such as Cross-Site Request Forgery (CSRF), Denial of Service (DoS), and BREACH attacks.

**Security and Human Subjects Research Data**

REDCap allows you to protect fields that contain PII (Personally Identifiable Information) and/or Protected Health Information (PHI) data by directly identifying the fields in the project, employing fine-grained user rights to control who can view, modify, or add data and/or forms. All activities are also system-logged and are available in a full audit trail. We encourage research PIs to collect the least amount of PII or PHI as possible if such collection is absolutely necessary. *Recommended reading before collecting Protected Health Information (PHI):* [A beginner’s guide to avoiding Protected Health Information (PHI) issues in clinical research – With how-to’s in REDCap Data Management Software](https://www.sciencedirect.com/science/article/pii/S1532046418301345?via%3Dihub).

**User Accounts**

**Account Types**

REDCap implements authentication to validate the identity of end-users who log in to the system. There are two classifications of users – Internal and External.

Internal users consist of UCH students, staff, and faculty members. Internal users access REDCap with their institutional login once added to the internal REDCap allow-list.

External user accounts will be given to users via sponsorship by their UConn Health/UConn Principal Investigator (PI). On the application, they need to use an institutional email address and identify their UCH/UConn PI – the PI must have a REDCap account already. We will then create an external account for them, which is linked to the PI’s account. External users will not have the ability to create new projects; they can only access projects to which they are formally added. A unique username will be created by REDCap administrators and a password will be set by the external user. Passwords **must** be changed every 90 days.

**Auto-logout & Suspensions**

REDCap contains an auto-logout setting that will automatically log a user out of the system if they have not had any activity (e.g. clicking, typing, moving the mouse) on their current web page for 15 minutes. Additionally, REDCap will lock a user out of the system after 3 failed login attempts for 5 minutes.

A user account may also be automatically suspended due to overall inactivity for more than 180 days. Suspending a user allows their account to remain in the system but denies them access to the entire REDCap application until their suspended status has been revoked by a REDCap administrator.  An account may also be suspended by an administrator due to an inappropriate use of the system as deemed by the administrators. For non-UConn/UCH users, accounts can only be unsuspended by request from the user’s sponsor.

**User Privileges**

Each user has their own account, and their user account will only have access to REDCap projects that they themselves have created or to projects to which other users have granted them access.

[User privileges](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fhealth.uconn.edu%2Fclinical-research-center%2Fwp-content%2Fuploads%2Fsites%2F50%2F2024%2F02%2FProject-Users-and-User-Privileges.docx&wdOrigin=BROWSELINK) are granular on the project level and can be modified within any given project by someone with proper privileges. The creator of a project will automatically be given full rights to the project, after which they may grant other users access. External (non-UConn/UCH) user accounts will not be allowed to create their own project to ensure they have a collaboration with UCH/UConn staff on each project.

[Data Access Groups](https://health.uconn.edu/clinical-research-center/wp-content/uploads/sites/50/2023/11/Data-Access-Groups.pdf) can be implemented to help segregate users and the data they enter by placing users into data access groups, after which they will only be able to access records created by someone in their group. This particular feature is entirely optional but is especially helpful in certain situations, such as for multi-institutional projects where the data entered by one institution should not be accessible or viewable by other institutions with access to that same project.

**Data Considerations**

**Logging and Audit Trail**

REDCap has a built-in audit trail that automatically logs all user activity and logs all pages viewed by every user, including contextual information (e.g. the project or record being accessed). A project user granted 'logging' privileges will have the ability to view an audit trail on their own project. This built-in audit trail also allows REDCap administrators to be able to determine all the activity and all the data viewed or modified by any given user.

**Data Export and De-Identification**

REDCap allows users to export any and all data from their REDCap projects, supposing they have been given full data export privileges.

The Data Export Tool has advanced export features that allow one to implement data de-identification methods. User privileges can also be set so that some users may be allowed to export data from the project but will have the data de-identification methods imposed as a means of preventing them from exporting sensitive data, either mistakenly or intentionally.

**Data Retention**

UCH REDCap cannot be used for project or data storage beyond the active life of the project. Once data collection has ended, project files/data need to be exported then the project needs to be removed from the system. Please ensure you are following all applicable institutional policies and procedures.

**Data Interoperability**

The REDCap API is an interface that allows external applications to connect to REDCap remotely. The REDCap API implements the use of tokens as a means of authenticating and validating all API requests that are received.