REDCap User Policies

Center for Informatics

Prepared by: Sarah Farzinkhou

Table of Contents

1. BACKGROUND

REDCap (Research Electronic Data Capture) is a secure, web-based application developed by Vanderbilt University to support data capture for research and operational purposes. It is widely adopted across academic, clinical, and research institutions due to its validated data entry workflows, audit trails, and automated export capabilities. REDCap's flexibility and scalability make it an ideal platform for managing sensitive data while supporting compliance with institutional policies and regulatory standards.

At City of Hope (COH), REDCap is implemented and maintained by the Center for Informatics to facilitate secure, efficient, and compliant data collection and management across both research and operational (non-research) projects.

2. PURPOSE

This document defines the policies and procedures for the use of REDCap at City of Hope. It is intended to:

- Ensure consistent and secure use of REDCap across research and operational teams
- Promote compliance with institutional policies, IRB protocols, and applicable regulations, including:
  - The Health Insurance Portability and Accountability Act (HIPAA)
  - 21 CFR Part 11 (Electronic Records and Electronic Signatures)
  - California Code of Regulations, Title 22
  - 21 CFR § 56.11
  - 45 CFR § 46.115(b)
  - Health and Safety Code 123149

- Establish clear roles, responsibilities, and access controls for REDCap users
- Safeguard Protected Health Information (PHI) and other high-risk data

This document serves as a foundational document for all REDCap users and administrators at COH, supporting ethical, secure, and compliant data practices.

3. SCOPE

This document applies to all personnel involved in the collection, management, and analysis of data within REDCap at City of Hope, including Principal Investigators, research staff, data analysts, project coordinators, and system administrators.

At COH, there are two distinct REDCap instances:

Internal REDCap: Used for projects involving City of Hope employees, faculty, and affiliated research staff. This instance supports both research and operational/quality improvement projects conducted within the institution.

External REDCap: Designed for collaborators from institutions outside of COH. This instance ensures data separation and access control for external users, with projects created and managed independently from internal system.

The below requirements are subject to validation by the REDCap administrative team, COH compliance teams, COH InfoSec teams, and/or external auditors at any time.

4. ROLES & RESPONSIBILITIES

The effective use of REDCap at City of Hope relies on clearly defined roles and responsibilities. This section outlines the key duties of REDCap users, project owners, study teams, and administrative support units such as Research Informatics. By establishing accountability and role-based access, City of Hope ensures secure, compliant, and efficient data management throughout the lifecycle of each REDCap project.

4.1 Data Steward (PI)

The Principal Investigator (PI) serves as the designated Data Steward and holds primary responsibility for the ethical, compliant, and effective management of the REDCap project. This includes oversight of data collection, user access, and adherence to institutional and regulatory requirements.

PI Responsibilities:

Project Management

- Manage the development of the REDCap project, including data collection instruments and workflows
- Oversee data collection and ensure alignment with study or operational goals

User Access Control

- Responsible for managing user access and roles, ensuring that users only have the privileges necessary to complete their responsibilities
- Manage the addition of users to the project and assignment of appropriate permissions (Internal REDCap only)
- Ensure all study personnel are listed on the IRB protocol (for research projects)

- Ensure that users have completed appropriate training, such as HIPAA, data security, CITI training and other institutional compliance requirements, before granting access if applicable.

Project Compliance

- Maintain compliance with HIPAA, 21 CFR Part 11, and IRB requirements
- Ensure secure handling of PHI and other sensitive data
- Specific Actions for Secure Handling of PHI
  - Limit Access to PHI.
  - Grant access only to individuals whose roles require it.
  - Use role-based access controls (RBAC) and follow the principle of least privilege.
  - Only use COH-issued/approved devices.
  - Flag PHI Fields in REDCap.
  - Mark all fields containing PHI as “Identifiers” in REDCap to control visibility and export permissions.
  - Avoid Unnecessary Exports.
  - Export PHI only when necessary and with proper authorization (e.g., IRB approval).
  - Use de-identified data whenever possible.
  - Monitor and audit access.
  - Regularly review user access logs and audit trails.
  - Remove access for users who no longer need it.
  - If PHI is printed or stored physically, keep it in locked, access-controlled environments.
  - Report Incidents Promptly.
  - Immediately report any suspected data breaches or unauthorized access to the Compliance Office or IT Security.

4.2 Project Owner / Project Manager

The Project Owner or Project Manager plays a critical role in the day-to-day administration of REDCap projects. This individual may be the Principal Investigator (PI) or a designated team member with administrative privileges. Their primary responsibility is to manage user access within the project and ensure that operations align with institutional policies listed in this document.

Key Responsibilities:

User Access Management

- Can request access for new users via AccessNet/SailPoint.
- Assign appropriate roles and permissions within the REDCap project based on each user’s

responsibilities.

- Before granting access to a project, ensure that users have completed appropriate training, such as HIPAA, data security, CITI training and other institutional compliance requirements, and if applicable, before granting access to the REDCap system. Also, for research projects, ensure they are listed on the IRB protocol.

Project Configuration and Oversight

- Assist in setting up project instruments, forms, and workflows in REDCap.
- Monitor project activity to ensure data is being entered and managed according to protocol.
- Collaborate with the PI and RI to resolve access or configuration issues.

Compliance and Documentation

- Utilize REDCap's built-in change tracking in Production mode to monitor and review project modifications using versioned data dictionaries.
- Ensure that data access and usage comply with HIPAA, IRB approvals, and institutional data governance policies as listed under purpose in this document.

Liaison Role: Study Coordinator

- Serve as the primary point of contact between the project team and REDCap Admin for technical support and system-related inquiries for External REDCap.
- Communicate updates, issues, or changes in project scope or personnel to the appropriate stakeholders.

4.3 Data Entry Personnel / Research Staff

These individuals are responsible for entering and managing data within REDCap under the supervision of the PI or Project Manager.

Key Responsibilities:

- Enter data accurately and in accordance with the approved study protocol or operational workflow.
- Ensure that access is used only for authorized purposes and that PHI is handled securely.

4.4 Data Analyst / Statistician

Data analysts and statisticians may access REDCap data for the purpose of analysis and reporting, under the direction of the PI.

Key Responsibilities:

- Access and analyze data in accordance with IRB approvals and data use agreements.
    - Ensure that data exports are de-identified or handled in compliance with HIPAA.
    - Collaborate with the PI and project team to ensure data is interpreted accurately and ethically.
- Maintain confidentiality and security of all data accessed through REDCap.

4.5 Institutional Review Board (IRB) / Compliance Office

The IRB and Compliance Office play a critical oversight role in ensuring that REDCap projects meet ethical and regulatory standards.

Key Responsibilities:

- Review and approve research protocols involving REDCap, particularly those involving human subjects or PHI
- Ensure that data collection and management practices align with institutional policies and federal regulations listed in this document.
- Provide guidance on data privacy, consent, and risk mitigation strategies.
- Support audit readiness and respond to compliance inquiries related to REDCap use.

4.6 System Administrator

At City of Hope, the Center for Informatics (RI) serves as the institutional REDCap Administrator, responsible for:

- Setting up and configuring the REDCap software, including database and server setup.
- Managing user account access and deactivation in collaboration with study teams.
    a. For Internal REDCap: Reviewing and granting user access.
    b. For External REDCap: Creating, managing, and deleting user accounts, setting permissions, and managing access levels.
- Providing guidance on REDCap features, project setup, and best practices for data collection and project management team.
- Coordinating with the Database Administration (DBA) team for system maintenance, performance monitoring, and backups.
- Providing technical assistance to REDCap users.
- Performing regular system updates, patches, and backups to ensure the system's stability.
- Identifying and resolving technical issues with the REDCap system and software.

4.7 ACCESSS APPROVAL

This section outlines the responsibilities and procedures for REDCap access, divided into two categories: access to the REDCap application itself, and access to individual projects. Each category is further divided based on whether the user is accessing the internal or external REDCap instance.

4.7.1 Application Access

All users must have their own REDCap account to access the platform. Access is requested through AccessNet (to be replaced by SailPoint) and is subject to approval based on user type and project purpose.

Internal REDCap – Application Access

- **PI/Project Owner Responsibilities:**
  - Submit access requests for themselves and team members via AccessNet/SailPoint.
  - Ensure users have completed required institutional training (e.g., HIPAA, CITI, data security).
  - Confirm users are affiliated with an approved project.
- **REDCap Administration Responsibilities:**
  - Review submitted access requests.
  - Send and collect signed REDCap User Agreements.
  - Add approved users to the authenticated REDCap user group (edc-redcap).
  - Provide login instructions and confirm system registration.

External REDCap – Application Access

External users are collaborators from institutions outside City of Hope and are governed by their home institution's training requirements and are not required to complete COH training. These users will access the external instance of REDCap, but they will work within the same project where City of Hope data is also collected. Through the use of Data Access Groups (DAGs), their access is restricted to data from their own site only, ensuring separation and confidentiality across collaborating centers.

- **Sponsoring PI (COH PI) Responsibilities:**
  - Submit access requests for external collaborators via AccessNet/SailPoint.
  - Ensure appropriate IRB approvals, Data Use Agreements (DUAs), or data sharing agreements are in place.
  - Define the external user's role and scope of access.
- **REDCap Administrator Responsibilities:**
  - Review and process external access requests.
  - Send and collect REDCap User Agreements.
  - Grant access only to the specific project(s) authorized.
  - Confirm external users are placed in the correct REDCap instance and role.

4.7.2 Individual Project Access

Once users have REDCap accounts, they may be added to specific projects based on their role and project type.

Internal REDCap – Project Access

- **PI/Project Owner Responsibilities:**
  - Ensure IRB approval is in place before collecting human subjects data.
  - Confirm all users are listed on the IRB protocol (for research projects).
  - Assign user roles based on the principle of least privilege.
  - Build and test the project in Development mode.
  - Submit the project for Production status after testing.
  - Maintain oversight of user access and project configuration.
- **REDCap Administration Responsibilities:**
  - Verify project type (research, operational, or quality improvement).
  - Review IRB documentation or departmental approval as applicable.
  - Approve project transition to Production mode.
  - Provide support for project setup and access issues.

External REDCap – Project Access

- **Sponsoring (COH) PI Responsibilities:**
  - Define external user roles and ensure they align with IRB or DUA terms.
  - Confirm external users are only accessing data from their own site.
  - Ensure the external project is thoroughly tested before requesting Production status.
- **REDCap Administration Responsibilities:**
  - Assign external users to appropriate Data Access Groups (DAGs) to restrict access to their site's data.
  - Review and approve requests to move external projects to Production after testing is complete.

5. ACCESS and USE CONTROL

This section defines the policies and procedures for managing user access and controlling data use within REDCap at City of Hope. It ensures that access is granted appropriately, roles are assigned based on responsibilities, and data visibility is restricted according to project needs and regulatory requirements.

5.1 Role-Based Access Framework

REDCap uses a role-based access control (RBAC) model to ensure users only have access to the data and functions necessary for their responsibilities per project and it's IRB approval

- **Who Gets What Access and Why**:
  - **Principal Investigators (PIs)** and **Project Managers** are responsible for assigning

roles based on each user's function within the project.

- Common roles include:
  - **Project Designer**: Full access to design and configuration tools.
  - **Data Entry**: Access to enter and view data.
  - **Read-Only**: View-only access to project data.
  - **Data Export**: Permission to export data, with or without identifiers depending on IRB approval.

- **Access Expiration**: PIs and Project Managers must assign expiration dates for each user's access, aligned with IRB approval periods or project timelines.
- **Separation of Access**:
  External users are collaborators from institutions outside City of Hope.
  These users will access the external instance of REDCap, but they will work within the same project where City of Hope data is also collected. Through the use of Data Access Groups (DAGs), their access is restricted to data from their own site only, ensuring separation and confidentiality across collaborating centers.

5.2 REDCap Access Role Matrix – City of Hope

Role	Access Level	Responsibilities	Approval Path	Access Expiration
Principal Investigator (PI)	Full Access	- Submit access requests via AccessNet/SailPoint - Ensure training completion - Confirm project affiliation - Assign roles per least privilege - Can sponsor internal and external users	- IRB approval - REDCap Admin approval via AccessNet/ SailPoint	Aligned with IRB approval period
Project Owner / Manager	Full or Partial Access	- User access management - Project setup - Compliance monitoring - Liaison with REDCap Admin	PI or Department Head - REDCap Admin approval	Aligned with project timeline

Study Coordinator (Internal)	Limited Access	- Enter/edit data - Run reports	PI or Co-Investigator	Aligned with project timeline
Data Entry Personnel / Research Staff	Limited Access (Data Entry)	- Enter/edit data per protocol and PHI handling rules - No export rights (unless approved)	- PI/PM assignment - IRB listing (for research) - REDCap Admin approval	Aligned with project duration
Data Analyst/ Statistician	Limited Access (Data Export)	- Export data (de-identified data or PHI data with IRB approval) - Run statistical reports	- PI/PM assignment - IRB listing (for research) - REDCap Admin approval	Requires justification and IRB alignment
IRB / Compliance Office	Limited Access (Read-only or audit-level access)	- Review protocols - Ensure regulatory compliance - Provide guidance	- Institutional Authority	N/A
System Administrator (REDCap Admin)	Admin Access (Manages system-wide access and compliance)	- Manage user groups - Approve project transitions - Review access requests - Collect User Agreements - Add users to edc-redcap - Approve Production status	Institutional Authority	N/A
Study Coordinator (External Projects)	Limited Access for external projects	- Liaison for external users - Communicate with REDCap Admin - Manage DAGs	- COH PI sponsorship - REDCap Admin approval	Aligned with 4 6 months (renewable with

	(No internal project access)			coordinator approval)
External Collaborator	Limited Access for external projects (No internal project access)	- Participate in external projects - Access only their site’s data	- COH PI sponsorship - REDCap Admin approval	6; months (renewable with coordinator approval)

Key Internal Access Policies

- **Training Requirements**: HIPAA, CITI, and data security training must be completed before access is granted.
- **IRB Protocol Alignment**: All users must be listed on the IRB protocol for research projects.
- **Access Expiration**: Must align with IRB approval periods or project timelines.
- **Role Assignment**: Based on the principle of least privilege.
- **Project Lifecycle**:
  - Development → Testing → Submit for Production
  - REDCap Admin verifies IRB/departmental approvals before Production status

5.3 Data Access Approval Process

All users must complete a formal access approval process before being granted access to REDCap. This process ensures that access is granted only to individuals who are authorized and appropriately documented.

5.3.1 Internal Users

Internal users include City of Hope employees, faculty, and affiliated research staff.

- **Access Request**: The PI or designated project builder submits a request via AccessNet (to be replaced by SailPoint. The request goes through manager approval followed by System owner approval
- **User Agreement**: The REDCap Administrator sends the REDCap User Agreement to the requester. Access is granted only after the signed agreement is returned.
- **Account Provisioning**: Once the agreement is received, the user is added to the authenticated REDCap user group (edc-redcap) and receives login instructions.
- **IRB Alignment**: For research projects, the PI must ensure that all users are listed on the IRB

application and have appropriate IRB clearance.

- **Access Expiration**: The PI or Project Manager must assign an access expiration date that aligns with the IRB approval period or project duration.
- **Optional Orientation**: Users may view a brief (approximately 4-minute) REDCap overview video to familiarize themselves with the system.

5.3.2 External Users

External users are collaborators from institutions outside City of Hope and must be managed In a separate instance of REDCap
External REDCap is open to users from other institutions who will be collaborating with a COH researcher – with COH as the primary site for the collaboration.
User accounts will only be granted to external users who have an official email address from their institution of employment. The accounts of external users will expire after four months but can be extended for another four months with the authorization of the study coordinator.

External users are governed by the training requirements of their institution of affiliation and are not required to complete City of Hope's internal training modules.

All communication regarding study and participant needs should be funneled through the study coordinator, who will then reach out to the REDCap Admins (RI) via our help request ticketing system: CRIC_Help@coh.org.
*CRIC_Help and the REDCap Admin team are available for COH employees only.

- **Sponsorship**: External users must be sponsored by a City of Hope's PI.
- **Access Request**: The COH sponsoring PI submits a request to Research Informatics (RI) on behalf of the external user via AccessNet/SailPoint (see 4.7.1)
- **User Agreement**: External users must sign and return the REDCap User Agreement before access is granted. See link under resources for a copy of the agreement.
- **Project Separation**: External users are granted access only to separate, designated projects and are not added to internal City of Hope projects. They are restricted to viewing and interacting with data from their own center only and do not have access to data from other collaborating centers.
- **Access Limitations**: Access is limited to the minimum necessary data and functions required for their role. For external projects, only REDCap project administrator can create REDCap projects.

5.4 User Policy Acknowledgement and Tracking

All REDCap users are required to acknowledge and accept the REDCap User Policies.

- For **new projects**, acknowledgment is captured through the updated REDCap User Agreement form.
- For **existing projects**, REDCap Administration will contact users directly to obtain acknowledgment via email or a designated form.

- All acknowledgments will be logged and tracked by the REDCap Administration team to ensure compliance.

5.5 Minimum Necessary Principle

City of Hope enforces the Minimum Necessary Principle to protect sensitive data and ensure compliance with HIPAA (45 CFR § 46.115(b).

- Data exports and PHI access are restricted based on IRB approval and user role. To verify IRB approval, users must submit documentation such as the IRB approval letter or protocol that clearly outlines the approved roles and data access permissions. This documentation should be included when submitting a ticket to the REDCap Admin team to request access.
- PIs and Project Managers must regularly evaluate whether users' access levels remain appropriate.

5.6 Periodic Access Reviews

To maintain data security and compliance, REDCap access is subject to regular review.

Semi-Annual Review: Project Owners are required to review the user list for each project at least once every six months. During this review, they must remove any users who are no longer active and revoke their access accordingly.

6. DATA CLASSIFICATION

This section defines the categories of data managed within REDCap at City of Hope and outlines the corresponding security and compliance requirements. Proper classification ensures that sensitive data is handled in accordance with institutional policies, HIPAA regulations, and ethical standards.

6.1. High Risk Data

High-risk data includes both clinical and non-clinical information that requires heightened security due to privacy, regulatory, or ethical concerns. This includes:

- **Individually Identifiable Health Information**
- **Protected Health Information (PHI)** under HIPAA
- **Sensitive non-health data** such as criminal records and financial information

City of Hope REDCap users must adhere to the HIPAA "minimum necessary" standard (45 CFR § 46.115(b), limiting access to essential team members and avoiding the export, sharing, or transfer of data unless absolutely necessary and with proper approval.

All of the following are designated as high-risk data and must be stored and transmitted in accordance with HIPAA standards:

- Health Information

- Individually Identifiable Health Information
- Protected Health Information (PHI)

6.2. Health Information

Defined under 45 CFR § 160.103, health information includes any information, including genetic data, that:
1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school, university, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care; or payment for health care.

6.2.1 Individually Identifiable Health Information

A subset of health information that includes demographic or clinical data which:

- Identifies the individual, or
- Can reasonably be used to identify the individual

This includes data created or received by a health care provider, health plan, employer, or clearinghouse that relates to health status, care, or payment.

6.2.2 Personally Identifiable Information (PII)

PII refers to any data that can be used to directly or indirectly identify an individual. Examples include:

- - Full name, email address, phone numbers
  - Date and place of birth, gender, race/ethnicity
  - Social Security number, driver's license, passport number
  - Financial account details, biometric data, IP address
  - Photos, videos, voice recordings, and other unique identifiers

6.3. Protected Health Information

PHI is a subset of Individually Identifiable Health Information that is:

- - Transmitted by electronic media
  - Maintained in any medium constituting electronic media
  - Transmitted or maintained in any other form or medium

Note: PHI does not include education records covered by FERPA or employment records held by a covered entity in its role as an employer. Information about deceased individuals is no longer considered PHI.

6.3.1 The 18 HIPAA PHI Identifiers

These are specific data elements that, if disclosed, could identify an individual:

1. Names
2. Geographic subdivisions smaller than a state
3. All elements of dates (except year) related to an individual
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web URLs
15. IP addresses
16. Biometric identifiers (e.g., fingerprints, voiceprints)
17. Full-face photographic images
18. Any other unique identifying number, characteristic, or code

7. STORAGE AND RETENTION

This section outlines the policies and procedures for the secure storage and retention of data collected and managed within REDCap at City of Hope. These practices support compliance with institutional policies, regulatory requirements, and data integrity standards.

For data retention and destruction, users must follow City of Hope's official Records Retention, Storage, and Destruction Policy (Link to Policy).

7.1. Data Storage

REDCap is hosted on secure, institutionally managed servers maintained by City of Hope's IT and Database Administration (DBA) teams. While standard enterprise backup practices are followed, REDCap is not configured for full disaster recovery across geographically distributed sites, as it is designated mostly for research use. Users should maintain a PDF copy of their REDCap projects and data in a secure location to ensure access to essential information in the event of system downtime or application unavailability.

Projects containing PHI or other high-risk data must follow HIPAA-compliant storage practices and may be subject to additional oversight.

7.2 Data Retention

Data must be retained in accordance with applicable regulatory, IRB, sponsor, or institutional requirements. This may vary depending on the nature of the project (e.g., clinical trial, quality improvement, operational).

The Principal Investigator (PI) is responsible for understanding and adhering to the required retention period for their project data.

It must be noted that REDCap is not intended for long-term archival storage. Upon project completion or closure, data should be exported and stored in an approved long-term repository if required.

7.3 Project Closure and Data Archiving

When a project is complete, the Principal Investigator (PI) or Project Owner must move the project to Archived status. If a project is mistakenly archived, notify Research Informatics immediately, as only REDCap administrators can revert the status.

Requests for data deletion should be handled by the study team, provided the individual performing the deletion is authorized and covered under the IRB protocol. Research Informatics (RI) may assist with bulk deletions or complex scenarios, but this is uncommon. If assistance is needed, contact RI with appropriate documentation and justification.

8. EXTERNAL SHARING AND EXPORT

This section outlines the policies and procedures for exporting data from REDCap and sharing it with individuals or systems outside of City of Hope. These controls are in place to protect sensitive information, ensure compliance with HIPAA and institutional policies listed in this document, and maintain data integrity.

8.1 General Principles

- Data exports must follow the minimum necessary principle, ensuring only the required data elements are shared.
- Exported data must be stored and transmitted securely, using encrypted formats and approved channels.

8.2 Export Permissions in REDCap

- REDCap allows granular control over export permissions:
    - **No Export**: User cannot export any data.
    - **De-Identified Export**: User can export data with identifiers removed.
    - **Full Data Export**: User can export all data, including identifiers (requires IRB approval).
- The PI or Project Manager is responsible for assigning user export rights based on user roles

and IRB determinations.

- No export rights are given to users for EXTRENAL REDCap.

8.3 Sharing with External Collaborators

- External collaborators must have:
  - A valid REDCap account (see Section 4.8.2)
  - A signed REDCap User Agreement
  - IRB approval or a Data Use Agreement (DUA), if applicable
- External users will never be added to internal projects.
- Exporting data for analysis or sharing with other institutions is not permitted.

8.4 Prohibited Practices

- Exporting data to personal devices or unapproved cloud storage platforms (e.g., Google Drive, Dropbox) is strictly prohibited.
- Sharing login credentials or exporting data on behalf of another user is not allowed.
- Data must not be exported or shared with third parties.

9. AUDIT AND MONITORING

City of Hope requires that all REDCap projects be subject to ongoing audit and monitoring to ensure compliance with institutional policies, HIPAA regulations, and IRB requirements. While Research Informatics (RI) maintains system-level audit logs and may conduct periodic reviews, the primary responsibility for monitoring project activity lies with the Principal Investigator (PI) and Project Owner. They are expected to regularly review user access, data exports, and project changes to ensure that only authorized individuals have access and that all activity aligns with approved protocols. Any suspected misuse or irregularities must be reported promptly to the Compliance Office.

COH Institutional Policy References:

1. Records Retention, Storage and Destruction
2. California Code of Regulations, Title 22
3. 21 CFR § 56.11
4. 45 CFR § 46.115(b)
5. Health and Safety Code 123149

Resources:

1. How to Mark PHI data in REDCap
2. How to Delete Data in REDCap
3. REDCapUserAgreementEForm_Internal
4. CityOfHopeREDCapUserAgreement_External