



Handling Confidential Data in REDCap Guide

Confidential Data: Identifiers & Protected Health Information (PHI)

REDCap may be used to collect and store research data that includes identifiers or Protected Health Information (PHI). Before collecting identifiable data, study teams must understand institutional requirements, IRB expectations, and applicable HIPAA regulations.

Important: The collection and storage of identifiable data in REDCap must be explicitly approved in your IRB protocol and supported by appropriate safeguards.

[Recommended Reading:](#) A beginner's guide to avoiding Protected Health Information (PHI) issues in clinical research – with how-to's in REDCap: [View Here](#)

HIPAA Responsibilities

Compliance with HIPAA is a shared responsibility. Users collecting, storing, or sharing PHI in REDCap are responsible for:

- Using and disclosing only the **minimum necessary** PHI
- Ensuring PHI is accessible only to **authorized individuals**
- Obtaining required **authorizations, data use agreements, and BAAs**
- Following all applicable **institutional, IRB, and regulatory policies**

Participant ID Best Practices

- Avoid using names, initials, MRNs, or identifiable data in record IDs
- Use **non-identifiable, coded IDs**
- Ensure IDs support longitudinal tracking without exposing identity

Best practice: Record IDs should never contain PHI or directly identifiable information.

Permitted Identifiers (With IRB Approval)

The following identifiers may be collected **only if explicitly approved by the IRB** and must be marked as Identifier fields in REDCap:

- Dates (except year)
- Names (including initials)

- Geographic subdivisions smaller than a state
- Phone numbers
- Fax numbers
- Email addresses

Important: Fields not marked as identifiers will not be excluded from exports.

Restricted Data (Not Permitted)

The following confidential data types must **not** be stored in UConn Health REDCap:

DATA ELEMENTS PROHIBITED IN REDCAP	
Medical Record Numbers (MRNs)	Social Security Numbers
Account Numbers	IP Addresses
Health Plan Beneficiary Numbers	Biometric Identifiers
Full-face Photographs	Audio/Video Recordings
Financial / PCI Data	ITAR-restricted Data
Mother's Maiden Name	Vehicle Identifiers

Important: These data types are prohibited regardless of study design or IRB approval.

Follow Your IRB-Approved Plan

- All REDCap data collection must align with IRB-approved materials
- Do not collect data not explicitly approved
- Ensure access and storage align with confidentiality requirements

If it is not in your IRB protocol, it should not be in your REDCap project.

Email Use & Identifier Linkage

Using email addresses for survey distribution (Survey Invitations or ASIs) creates a direct linkage between participant identity and study data.

- Email use must be explicitly described in the IRB protocol
- Consent materials must disclose this use
- Survey responses are linked to identifiable participants

Important: If email is used for survey distribution, you cannot state that identifiers are fully separated from study data.

Changes Require IRB Approval

- All changes must be IRB-approved **before implementation**
- Consult IRB for Exempt studies before making changes

Important: Unauthorized changes may invalidate your study approval.

Best Practice Recommendations

- Restrict access using User Rights and DAGs
- Exclude identifiers from unnecessary forms/exports
- Consider a separate contact project if separation is required
- When Identifiers Must Be Stored Separately
 - Use a **separate REDCap project** for identifiers
 - Avoid direct linkage unless IRB-approved
- If Storing Identifiers Is Required confirm IRB approval, apply appropriate safeguards, and limit access to authorized personnel only