REDCap: Identifiers

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*](#)

Complying with HIPAA's requirements is a shared responsibility. Users sharing and storing PII/PHI in REDCap are responsible for complying with HIPAA safeguards, including:

- Using and disclosing only the minimum necessary PHI for the intended purpose
- Ensuring that PHI is seen only by those who are authorized to see it
- Obtaining all necessary authorizations, data-sharing agreements, and Business Associate Agreements for using and disclosing PHI
- Following any additional steps required by your unit to comply with HIPAA, IRB, and UConn Health Policies and Procedures

The following potential identifiers are allowed in UCH REDCap:

- Dates (all elements of dates (except year) related to an individual. This includes dates of admission, discharge, birth, and death.)
- Names (this includes parts of names, such as initials)
- Signatures
- Any Geographic information (town, city, state, and zip code)
- Phone numbers
- Fax numbers
- Email addresses

The following potential identifiers are considered restricted sensitive data and are **NOT** allowed to be used or stored in the UCH REDCap system:

- Account numbers
- Social security numbers (includes parts of SSNs, e.g. last 4 digits, and scrambled SSNs)*
- Medical Record number
- Mother's Maiden names
- Health Plan number
- Certificate/license numbers
- IP address
- Financial/PCI data
- Vehicle identifiers
- Biometric ID
- Full face/identifying photo
- Audio & Video Files
- HIPAA data not approved by the IRB protocol.
- Data related to International Traffic in Arms Regulations (ITAR). ITAR control the export and import of defense-related articles and services on the United States Munitions List (USML).

*Please Note: Your study materials dictate what data can be collected and how that data will be stored; this information can be found in the protocol, consent forms, IRB application, HIPAA authorization/waiver, etc. If your IRB-approved data collection and storage plan indicates that identifiers will be kept separate from the data collected (i.e. will not be stored with study data) to ensure that data cannot be linked, then identifiers should not be collected/stored in the same project along with the data. It is the responsibility of the PI (as well as the study team) to ensure the collection and storage of identifiers, this includes signed consent documents, is consistent with the confidentiality plans described to the IRB in the application, protocol, consent, etc. Changes to the data collected and how it is stored are to be approved by the IRB prior to implementation. If the IRB determined the research was **Exempt**, the PI should consult the IRB before making changes to ensure those changes do not invalidate the exemption.*
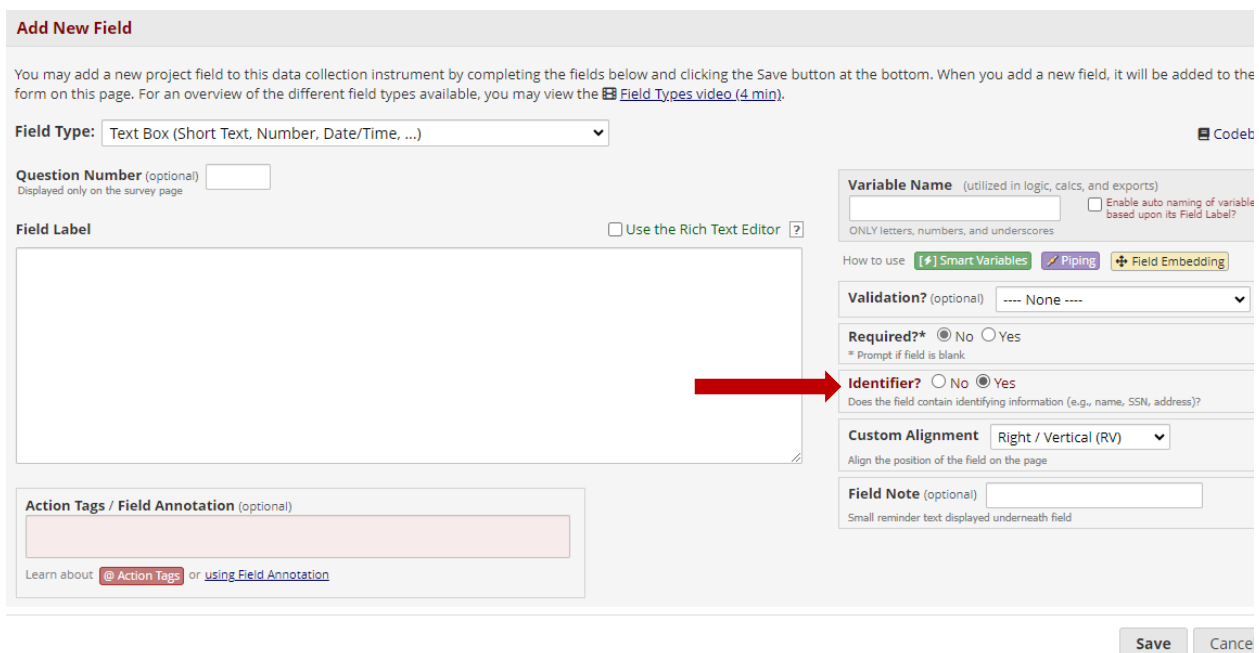
What Fields Should Be Marked as Identifiers in REDCap?

Each data field that *could* be considered an identifier should be marked as an identifier in REDCap. *This may differ from what is considered identifying or sensitive information for other aspects of your project (such as IRB approval.)*

IMPORTANT: *Identifiers should <u>NOT</u> be used as Subject ID or Record ID numbers. And Subject ID or Record ID numbers should not be checked as identifiers. These numbers might be the only way to distinguish a record for users that export data and/or don't have access to identifiers (per project-specific permissions)*

How to Mark a Field as an Identifier in REDCap

If you are building an instrument using the Online Designer, you can mark a field as an identifier when you add it. Select that the field is an identifier on the left side of the "Add New Field" pop-up window when you are adding or editing a field.

Using the "Check for Identifiers" Tool

You can use this tool when your project is in development mode, or while it is in draft mode before you submit changes for approval. This tool automatically checks the names and descriptions of your data fields to look for common keywords that indicate an identifier.

To use this tool, make sure your project is in Development mode or draft mode (for projects that are already in Production.) Navigate to "Project Setup" and the "Design your data collection instruments" box. There will be a small link under the buttons for Online Designer and Data Dictionary.

The Check for Identifiers tool will bring up a checklist of all the fields it has found that may contain identifiers. If the checkbox is already checked, the field has been marked as an identifier. You can edit the identifier designation from this page by checking or unchecking the boxes. Make sure to save your changes with the "Update Identifiers" button at the bottom of the page.

Using the data dictionary

You can mark identifiers when setting up or editing your project using the data dictionary. Your project's data dictionary will have a column labeled 'Identifier.' Mark fields as identifiers by changing the value to "K" in this column.

What is the impact of marking fields as identifiers in REDCap?

Important! When a field is marked as an identifier in REDCap, this only restricts access when data is *exported!*

Users who have "Read" or "View & Edit" access to an instrument will still be able to see data entered into fields marked as an identifier. This is true even if their export privileges only allow them to export de-identified data. For most projects, simply marking a field as an identifier in REDCap should not have significant impacts on how users interact with data in your REDCap project.

How to restrict user access to identifiers in REDCap

If you would like to restrict users from viewing (and not just exporting) identifiers that have been entered into your REDCap project, then you will need to segregate identifier fields within one or more instruments that have their access restricted.