FSU REDCap: Protecting High-Risk Data

Overview
While people may only think of clinical data that is available in EHR (electronic health records) as high risk data, many non-clinical projects contain data that includes high-risk data, such as individually identifiable health information and protected health information (PHI). High-risk data may include such things as health status and provision of healthcare, and can even include non-health related data such as criminal activity or financial information.

This document outlines requirements and recommendations pertaining to protecting high-risk data in REDCap.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), established rules protecting the privacy and security of individually identifiable health information. For example, HIPAA set national standards requiring organizations and individuals to implement certain administrative, physical, and technical safeguards to maintain the confidentiality, integrity, and availability of PHI.

FSU REDCap is *HIPAA-capable*.

This means that it contains the necessary components for HIPAA compliancy, but it is the environment into which the software is installed that makes it compliant.

Therefore, HIPAA compliancy requires that certain practices, such as limiting access to high-risk data and restricting export of high-risk data, are thoroughly document and communicated to users. As such, **part of what makes FSU REDCap HIPAA compliant is YOU**.

More information about HIPAA compliance in research can be found on the Office of Human Subjects Protection (OHSP) website.

What is High-Risk Data?
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)

The HIPAA Privacy Rule requires that investigators take the reasonable steps to limit the use or disclosure of, and requests for, high-risk data to the “minimum necessary” to accomplish the intended purpose. FSU REDCap users are expected to always operate according to the “minimum necessary” standard (e.g., limit data access to necessary team members; do not export, share, or transfer data unless absolutely necessary; etc.).

Health information, individually identifiable Health Information, and Protected Health Information (PHI) are defined as follows:

1. **Health Information**

   a. Any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a Health Care Provider, Health Plan, public health authority, employer, life insurer, school or 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 to an individual; or the past, present, or future payment for the provision of health care to an individual (45 CFR § 160.103).

2. **Individually Identifiable Health Information**
   a. Information that is a subset of Health Information, including demographic information collected from an individual, and that: (1) is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an individual; or the past, present, or future payment fo the provision of health care to an individual; and (3) a. identifies the Individual, or b. with respect to which there is a reasonable basis to believe the information can be used to identify the individual (45 CFR § 160.103).
3. **Protected Health Information**
   a. A subset of Individually Identifiable Health Information that is (a) transmitted by electronic media; (b) maintained in any medium constituting electronic media; or (c) transmitted or maintained in any other form or medium (45 CFR § 160.103).
      i. Note: Information pertaining to a patient who has been deceased for more than 50 years is no longer Protected Health Information. Protected Health Information does not include Individually Identifiable Health Information in education records under FERPA or employment records held by a Covered Entity as an employer.

FSU REDCap users are expected to treat ALL health-related data (unless de-identified) as covered by HIPAA requirements—with the highest levels of privacy and security possible—***regardless of the source of the data.***

Which units must follow the HIPAA privacy and security roles?
Florida State University is hybrid entity under HIPAA, meaning that only certain units are considered covered components, also called healthcare components (HCCs).

However, since HCCs are limited in how they can share high-risk data with non-HCCs, all units (“covered” or not) are expected to store and transmit health-related information as if they were covered by HIPAA. Further, HCC’s are not permitted to disclose high-risk data to non-HCC’s without a Business Associate Agreement (BAA).

Requirements for Accessing & Using FSU REDCap. It is the responsibility of the Principal Investigator (PI) and each authorized research team member to complete the requirements for access to REDCap. These requirements include:

- Reviewing and adhering to the Florida State University (FSU) policies and procedures outlined in this User Agreement and the Protecting High-Risk Data document (found online).

- Confirming an up-to-date copy of their CITI training certificate is uploaded to the FSU RAMP portal. For FSU IRB applications regarding human subject research, the CITI Human Subjects Research training and the Good Clinical Practice training are required.
- Ensuring all individuals on the research team comply with their own College or Department policies for research handling medium- or high-risk data (including Protected Health Information [PHI]).
- Ensuring researchers handling PHI comply with the Office for Human Subjects Protection HIPAA requirements found on the HIPPA in Research webpage.
- Completing the appropriate project-specific REDCap training. PIs and Research System Administrators working on the project in REDCap should complete the tutorial videos in sections 1, 2, and 3 on the REDCap resources webpage (cumulatively, approximately 1 hour and 20 minutes) prior to using REDCap for the first time.
- Completing an annual user access review for each in-production project they manage. It is the responsibility of the PI to let the REDCap team know if any research team members who are no longer affiliated need to be removed from the project; the PI may designate a research project administrator to provide this information, but the responsibility remains with the PI.

Compliance Documentation

- If an FSU REDCap project is collecting research data involving human or animal subjects, the PI or designated Project Administrator (e.g. lab manager, research coordinator) must acquire the appropriate compliance documents prior to collecting data (e.g. IRB letter). The FSU REDCap team may request this documentation from you at any time.
- If the project is conducted at more than one institution, the project owner attests that appropriate regulatory approvals (non-FSU) have been obtained prior to data collection.
- A Data Use Agreement (DUA) may be required when working with a limited data set in which high-risk data has been obtained from a clinical partner. Since a limited data set contains identifiers, the HIPAA Privacy Rule states that covered entities (e.g. clinical partners) must enter into data use agreements with recipients (e.g. researchers). Some third parties also require a DUA regardless of whether the data is considered a limited data set.

HIPAA-Approved Tools/Strategies at FSU

The following systems/services meet certain requirements established by the HIPAA Security Rule and therefore are approved to process, store, or collect high-risk data:

1. **FSU HDSI Microsoft Azure VDI**
   a. This service is a Virtual Desktop Interface (VDI) that replicates the look and feel of a typical FSU desktop. However, this desktop is secured for the collection and processing of high-risk data including PHI. Tools available on the VDI include most Microsoft Office suite products, SPSS, SAS, MatLab, and others. If you have a commonly used application or software, you can work with the ITS team to establish a customized environment for your needs. **Note: electronic mail (email) is not provided as a service in the FSU HDSI Azure VDI.*
   b. Accounts must be requested through FSU ITS.
   c. Generally requires additional IT support and resources
2. **Personal Desktop/Laptop and/or hard-drive storage**

   a. Researchers may choose to use their own equipment to process and store PHI. In doing so, researchers must take certain steps to ensure security and privacy controls for their dataset.
   b. Strong encryption practices are necessary to protect data. Some options include:
      i. Microsoft Bitlocker can be used to encrypt on Windows Desktops/Servers running a current and supported version of the Windows operating system. This tool utilizes strong encryption protoco9ls (e.g., AES-256), to encrypt a physical hard drive.
      ii. SecureZip (PKWARE). This product is focused on file-level encryption (e.g. a PDF, Word document, etc.) and also can be configured to use strong encryption methods such as AES-256. A desktop version can be purchased for approximately $50 or less from https://www.pkware.com.
      iii. Yubikey is a low-cost USB key (less than $50) that hangs on a keychain and is plugged into a USB port on a desktop/laptop. Windows would be configured so that researchers who need access to the data would need to plug in the Yubikey: https://support.yubico.com/hc/en-us/articles/360013708460-Yubico-Login-for-Windows-Configuration-Guide
      *iv. *Note: there are other open-source version of encryption solutions. While FSU does not endorse any specific solutions, the tools listed above are user-friendly and effective.*

3. **FSU REDCap**
   a. REDCap is a HIPAA-capable data collection and storage (database-style) tool that exports data into multiple formats for analysis.
   b. Access must be requested here.
   c. FSU HIPAA training must be completed.
   d. REDCap training should be completed prior to access to establish baseline familiarity with the application.
   e. Project consultations are available with our REDCap experts.
4. **De-Identify Your Data (see section below)**

De-Identification
There are two methods to de-identify Personal Health Information (PHI): the Safe Harbor method (§164.514(b)(2)) and Expert Determination (§164.514(b)(1)).

If using the Safe Harbor Method, there are 18 pieces of information, or “identifiers,” linked to data that must be removed to consider the data de-identified:

1. Names
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. Dates (other than year) directly related to the individual
4. Phone numbers

5. Fax numbers
6. Email addresses
7. Social Security Numbers (SSN)
8. Medical Record Numbers (MRN)
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal, and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code *except the unique code assigned by the investigator to code the data.*

Data is considered de-identified according to this method once these 18 specific identifiers linked to an individual have been removed. In essence, de-identifying the data removes all information that could reasonably be used to re-identify an individual. Attention must be given to check that all 18 specific identifiers are removed, wherever those identifiers appear.

If using the Expert Determination Method, you may use an expert with "appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" to determine that there is a "very small" risk that the information, alone or in combination with other reasonably available information, could be used by the rese4archer to identify the individual who is the subject of the information. The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination. The University must keep such certification, in written or electronic format, for at least six years from the data of its creation or the data when it was last in effect, whichever is later.

Anonymous Code Systems and Re-Identification
After de-identification of high-risk data, data managers are permitted to use an anonymous code system, which assigns a code or other means of record identification to allow the information to be re-identified or linked to the dataset.

The mechanism for assigning codes and re-identifying records (the "key") **must not be:**

- Derived from any identifiers (e.g., using a participant's initials in lieu of their name)
- Used for any purpose other than re-identification
- Disclosed to others outside your group
- Stored on any machines, including those used for data collection/analysis

If you are working with high-risk data, you must keep your code stored with high-risk data, such as in a HIPAA-approved Microsoft Azure account, or FSU REDCap. If you are working with high-risk data in FSU REDCap, you must store your identity key(s) on a separate form and limit access. See "Entering data" section under **Required Strategies to Maintain Security of Data in FSU REDCap** (*p. 6 of this document*).

Details about this process should be listed in your Institutional Review Board (IRB) protocol.

Limited Data Sets

A "Limited Data Set" contains identifiers. A limited data set pertaining to health information is therefore always high-risk data. A Data Usage Agreement (DUA) (see Compliance Documentation) may be required if the limited data set originates with a clinical partner or other third party.

Identifiers that may remain in the information disclosed in a limited data set include:

- Dates such as admission, discharge, service, DOB, DOD
- City, state, five digit or more zip code
- Ages in years, months, days, or hours

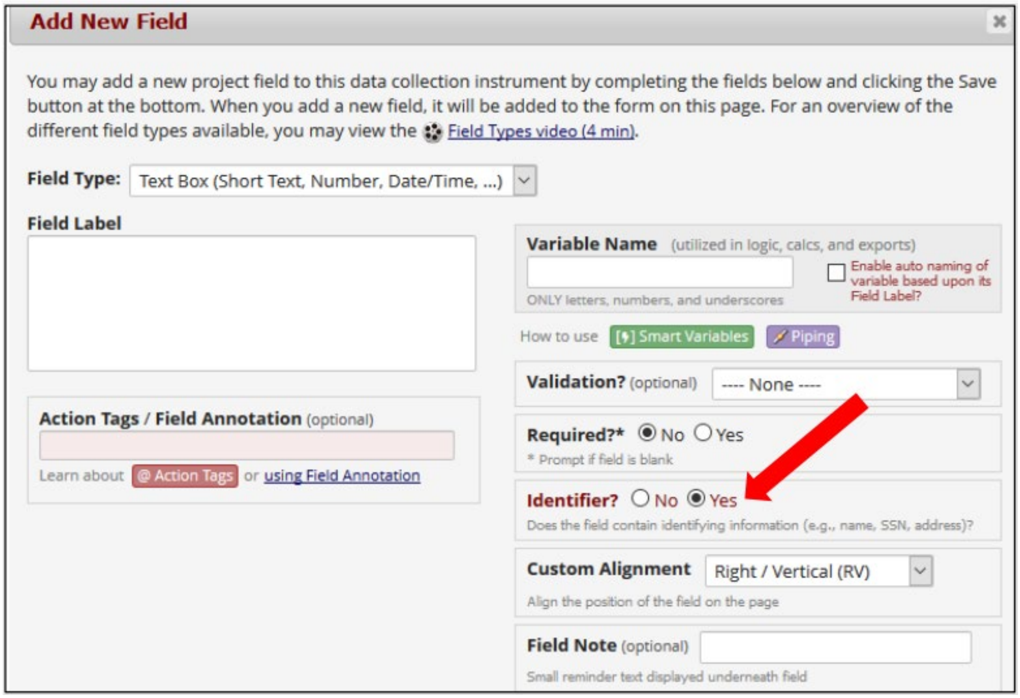
Required Strategies to Maintain Security of Data in FSU REDCap

Minimum Necessary User Rights

- Customize user rights/roles according to the "minimum necessary" standard defined on page 1 of this document. These user rights/roles should be reviewed regularly by the PI/owner of the REDCap project.
- Learn more about user rights and roles on our User Rights and Roles document.

Flag Identifiers

- When creating new fields, if your field label calls for identifying information (i.e. any of the 18 HIPAA identifiers), you must choose "Yes" next to the Identifier



Add New Field

You may add a new project field to this data collection instrument by completing the fields below and clicking the Save button at the bottom. When you add a new field, it will be added to the form on this page. For an overview of the different field types available, you may view the Field Types video (4 min).

Field Type: Text Box (Short Text, Number, Date/Time, ...)

Field Label

Variable Name (utilized in logic, calcs, and exports)

ONLY letters, numbers, and underscores

□ Enable auto naming of variable based upon its Field Label?

How to use [$] Smart Variables Piping

Action Tags / Field Annotation (optional)

Learn about @ Action Tags or using Field Annotation

Validation? (optional) ---- None ----

Required?* ● No ○ Yes

* Prompt if field is blank

Identifier? ○ No ● Yes

Does the field contain identifying information (e.g., name, SSN, address)?

Custom Alignment Right / Vertical (RV)

Align the position of the field on the page

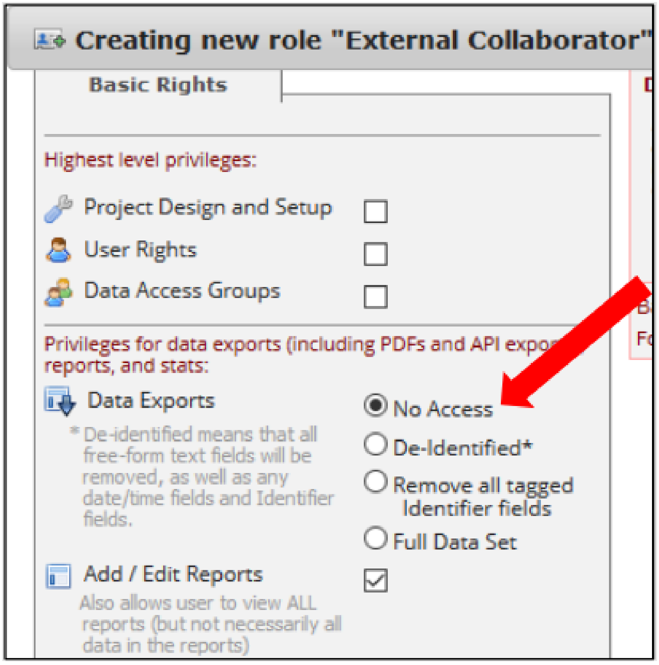
Field Note (optional)

Small reminder text displayed underneath field

Restrict data export rights and ensure safe data export

- Restrict/limit Data Export user rights according to "minimum necessary" standard
    - For example, non-Illinois (i.e., external) collaborators **should not have** Data Export rights

Adapted from Illinois Interdisciplinary Health Sciences Institute REDCap documentation



Creating new role "External Collaborator"

Basic Rights

Highest level privileges:

- Project Design and Setup □
- User Rights □
- Data Access Groups □

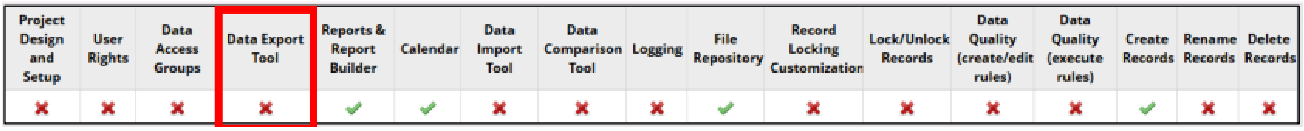
Privileges for data exports (including PDFs and API expo reports, and stats:

Data Exports
● No Access
○ De-Identified*
○ Remove all tagged Identifier fields
○ Full Data Set

* De-identified means that all free-form text fields will be removed, as well as any date/time fields and Identifier fields.

Add / Edit Reports ☑
Also allows user to view ALL reports (but not necessarily all data in the reports)

User rights table looks like this when “No Access” to Data Export is selected:



Project Design and Setup	User Rights	Data Access Groups	Data Export Tool	Reports & Report Builder	Calendar	Data Import Tool	Data Comparison Tool	Logging	File Repository	Record Locking Customization	Lock/Unlock Records	Data Quality (create/edit rules)	Data Quality (execute rules)	Create Records	Rename Records	Delete Records
✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗

- Export and/or transfer data according to “minimum necessary” standard
  - Ensure that “Remove all tagged identifier fields is checked prior to exporting and/or transferring data

If you must export and/or transfer data with identifiers for the purpose of analysis, the technology environment you are exporting/transferring the data to must meet one of the **HIPAA-Approved Tools/Strategies at FSU** on pages 3 & 4 of this document.

Utilizing Surveys in FSU REDCap

REDCap has two online survey options, a private survey and a public survey.

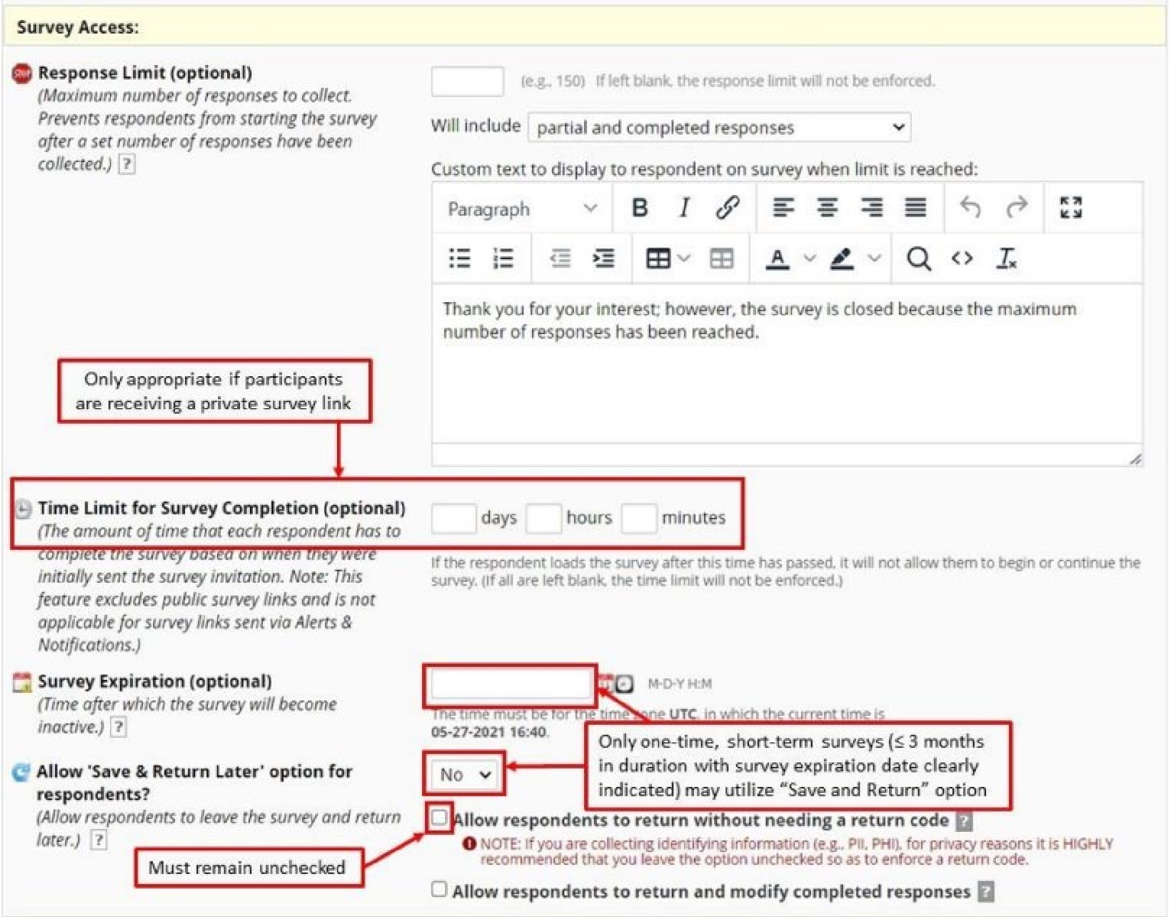
- The **private survey** utilizes a participant’s email address and REDCap sends a unique survey URL to each individual participant. Participants may only take the survey one time.
- The **public survey** option involves a REDCap survey URL that can be posted on a website, emailed to a mailing list, etc.

Important:

- Only one-time, short-term surveys (≤ 3 months in duration with survey expiration date clearly indicated) may utilize the “Save & Return Later” option; all other survey **may not use** this function.

Adapted from Illinois Interdisciplinary Health Sciences Institute REDCap documentation

- “Time Limit for Survey Completion” is **only an option** if the participant is receiving a private survey link. It is not an option when public survey links will be utilized. Researchers are responsible for ensuring they are using private survey links when this setting is used.
- Further, the following option should **never** be checked: “Allow respondents to return without needing a return code.”
- In accordance with our security protocol, this will be reviewed by the HDSI REDCap team prior to moving projects to production.



Survey Access:

Response Limit (optional)
(Maximum number of responses to collect. Prevents respondents from starting the survey after a set number of responses have been collected.) ?

(e.g., 150) If left blank, the response limit will not be enforced.

Will include: partial and completed responses

Custom text to display to respondent on survey when limit is reached:

Thank you for your interest; however, the survey is closed because the maximum number of responses has been reached.

Only appropriate if participants are receiving a private survey link

Time Limit for Survey Completion (optional)
(The amount of time that each respondent has to complete the survey based on when they were initially sent the survey invitation. Note: This feature excludes public survey links and is not applicable for survey links sent via Alerts & Notifications.)

days hours minutes

If the respondent loads the survey after this time has passed, it will not allow them to begin or continue the survey. (If all are left blank, the time limit will not be enforced.)

Survey Expiration (optional)
(Time after which the survey will become inactive.) ?

M-D-Y H:M

The time must be for the time zone **UTC**, in which the current time is **05-27-2021 16:40**.

Only one-time, short-term surveys (≤ 3 months in duration with survey expiration date clearly indicated) may utilize “Save and Return” option

Allow 'Save & Return Later' option for respondents?
(Allow respondents to leave the survey and return later.) ?

No

□ **Allow respondents to return without needing a return code** ?

NOTE: If you are collecting identifying information (e.g., PII, PHI), for privacy reasons it is HIGHLY recommended that you leave the option unchecked so as to enforce a return code.

Must remain unchecked

□ **Allow respondents to return and modify completed responses** ?

Additional Resources

- FSU REDCap Webpage:
- FSU Data Security & Privacy Document:
- FSU HIPAA Research Webpage:
- FSU ACUA Research Webpage:
- FSU IRB Webpage:
- U.S. Department of Health & Human Services De-Identification Information
- Vanderbilt University REDCap Homepage

Adapted from Illinois Interdisciplinary Health Sciences Institute REDCap documentation