Protecting High Risk Data in Illinois REDCap

- Background
- What is High Risk Data?
- Which Units Must Follow the HIPAA Privacy and Security Rules?
- U of I System HIPAA Training
- Compliance Documentation
- De-Identification
- Anonymous Code Systems and Re-Identification
- Limited Data Sets
- HIPAA-Approved Tools at Illinois
- Required Strategies to Maintain Security of Research Data in Illinois REDCap
- Additional Resources

Background

While people may only think of clinical data that is available from electronic medical 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). There is a wealth of information about an individual that could be considered high risk data, such as information about health status and provision of health care. There is also non-health related data that should be protected as high risk data, such as criminal activity or financial information.

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

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, the HIPAA Privacy Rule and Security Rule set national standards requiring organizations and individuals to implement certain administrative, physical, and technical safeguards to maintain the confidentiality, integrity, and availability of PHI.

Illinois REDCap is *HIPAA-capable*. 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 documented and communicated to users. As such, part of what makes Illinois REDCap *HIPAA-compliant* is YOU.

More information about HIPAA and HIPAA compliance at the University of Illinois, including the Privacy Directive, can be found at https://hipaa.uillinois.edu.

What is High Risk Data?

According to University Counsel and the University's Information Security Controls, ALL the following are designated *high risk data* and must be stored and transmitted in accordance with HIPAA standards:

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

This effectively means that Illinois 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*.

Further, the HIPAA Privacy Rule requires that investigators take reasonable steps to limit the use or disclosure of, and requests for, high risk data to the **"minimum necessary"** to accomplish the intended purpose. Illinois 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 absolute necessary; etc.). See Required Strategies to Maintain the Security of Research Data in Illinois REDCap.

Health Information, Individually Identifiable Health Information, and Protected Health Information (PHI) are defined as follows:

1. Health Information
    - 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
    - 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 for 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 (PHI)
    - 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)
        - 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.

Again, Illinois 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 Rules?
The University of Illinois at Urbana-Champaign is a "hybrid entity" under HIPAA, meaning that only certain units are considered "covered components," also called healthcare components (HCCs).

A list of current HCCs on our campus is available here.

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 are covered by HIPAA. Further, HCCs are not permitted to disclose high risk data to non-HCCs without a Business Associate Agreement (BAA). For more information about these requirements, please refer to https://hipaa.uillinois.edu/.

U of I System HIPAA Training
Because Illinois REDCap is housed in a HIPAA-provisioned Amazon Web Services (AWS) space, all users who will be accessing Illinois REDCap must complete U of I System HIPAA training, regardless of whether they reside in a "covered component," and regardless of whether they will be working with high risk data.

HIPAA training is administered by the U of I System. Training is coordinated so that most people are only required to complete HIPAA training once per year. However, some users may be required to complete HIPAA training more than once in a year if their access requirements change. Annual HIPAA training is required. Failure to complete the annual training may result in suspension of Illinois REDCap access until training is completed.

To obtain access to HIPAA training, users must first complete the Illinois REDCap User Request Form. If you have already completed U of I System HIPAA training, you will have the option to upload your HIPAA training completion certificate to your Illinois REDCap User Request Form.

Within an hour of submitting your user request form, you will receive instructions via email to access the U of I System HIPAA training. Please follow these steps:

1. Follow the instructions to access and complete the U of I System HIPAA training (approx. 1.5 hours)
2. Save and email your HIPAA training completion certificate to redcap-admin@illinois.edu
    - Note: The IHSI REDCap team is not automatically notified when training has been completed. Therefore, it is essential that you save and email the PDF of your certificate directly to redcap-admin@illinois.edu.

Upon receipt of your HIPAA training completion certificate, the IHSI REDCap team will grant you Illinois REDCap access (may take up to 2 business days).

Compliance Documentation

- If an Illinois REDCap project is collecting research data involving human or animal subjects, the Principal Investigator or designated Project Administrator (e.g., lab manager, research coordinator) must acquire the appropriate compliance documents *prior* to collecting data. The IHSI REDCap may request this documentation at any time.
- If the project is conducted at more than one institution, the project owner attests that appropriate regulatory approvals (non-Illinois) 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.

De-Identification

There are two methods to de-identify Personal Health Information: 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 data to be 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 the 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 an individual
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers (SSNs)
8. Medical record numbers (MRNs)
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 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 researcher 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 date of its creation or the date when it was last in effect, whichever is later.

If you have questions about de-identifying your data, please consult with the IHSI REDCap Team at redcap-admin@illinois.edu or the Office for the Protection of Research Subjects (OPRS) at irb@illinois.edu.

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 that 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 other purpose other than for 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 Box Health Data Folder, HIPAA-approved Amazon Web Services account, or Illinois REDCap. If you are working with high risk data in Illinois 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 Illinois REDCap.

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

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 Use 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

HIPAA-Approved Tools at Illinois
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:

- Amazon Web Services (AWS)
    - **HIPAA accounts must be requested** at https://aws.illinois.edu
    - Requires systems deployed to meet "high risk" standard of the Illini Secure security controls found at https://cybersecurity.uillinois.edu/controls
    - Generally requires additional IT support and resources
    - Ideal for processing high risk data (e.g., running scripts)
- Box Health Data Folder (BDHF) via U of I Box
    - **BHDFs must be requested** at https://hipaa.uillinois.edu/protecting-phi-with-box-health-data-folders/
    - "Syncing" and unsupported third-party Box integrations are not permitted
    - Ideal for storage of high risk data, including protected health information
- Illinois REDCap
    - **Access must be requested** at https://healthinstitute.illinois.edu/research-support/redcap
    - U of I System HIPAA training (instructions provided after submission of Illinois User Request Form) must be completed
    - REDCap training (https://projectredcap.org/resources/videos/) should be completed prior to access to establish baseline familiarity with the application
    - Ideal for collection of high risk data

Additional administrative, physical, and technical safeguards have been instituted to meet the remaining requirements, including mandatory de-identification to export, share, or transfer data.

Required Strategies to Maintain Security of Data in Illinois REDCap

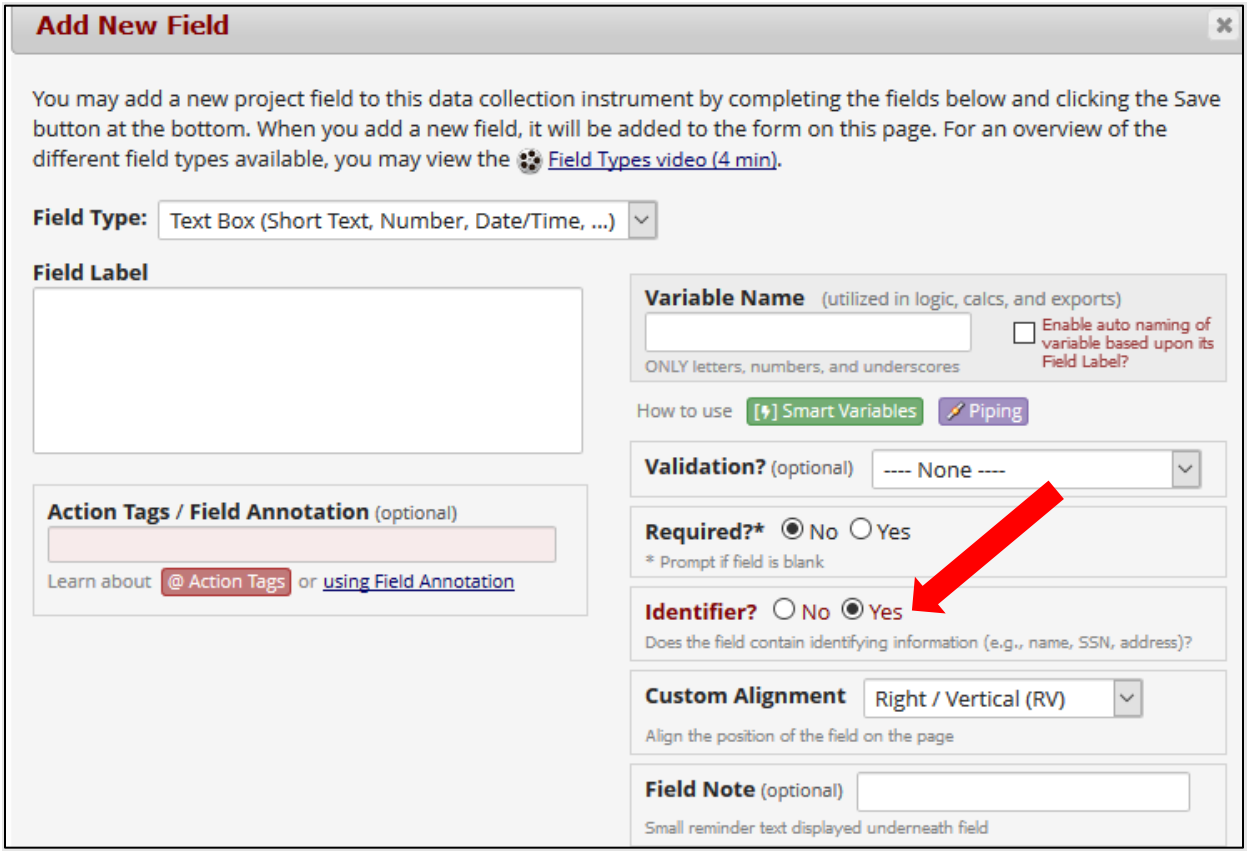
Minimum Necessary User Rights

- Customize user rights/roles according to the "minimum necessary" standard defined on page 2 of this document. These user rights/roles should be reviewed regularly.

- Learn more about user rights and roles on our User Rights and Roles document

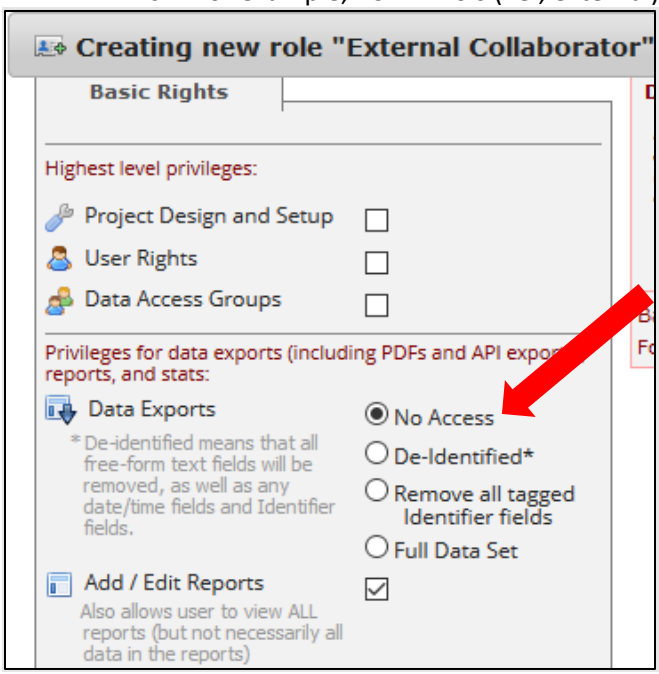
Flag identifiers

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



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



User rights table 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 de-identified 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, please contact the IHSI REDCap team and your unit IT professional(s) for assistance *prior to export/transfer* with secure data transfer and local requirements.

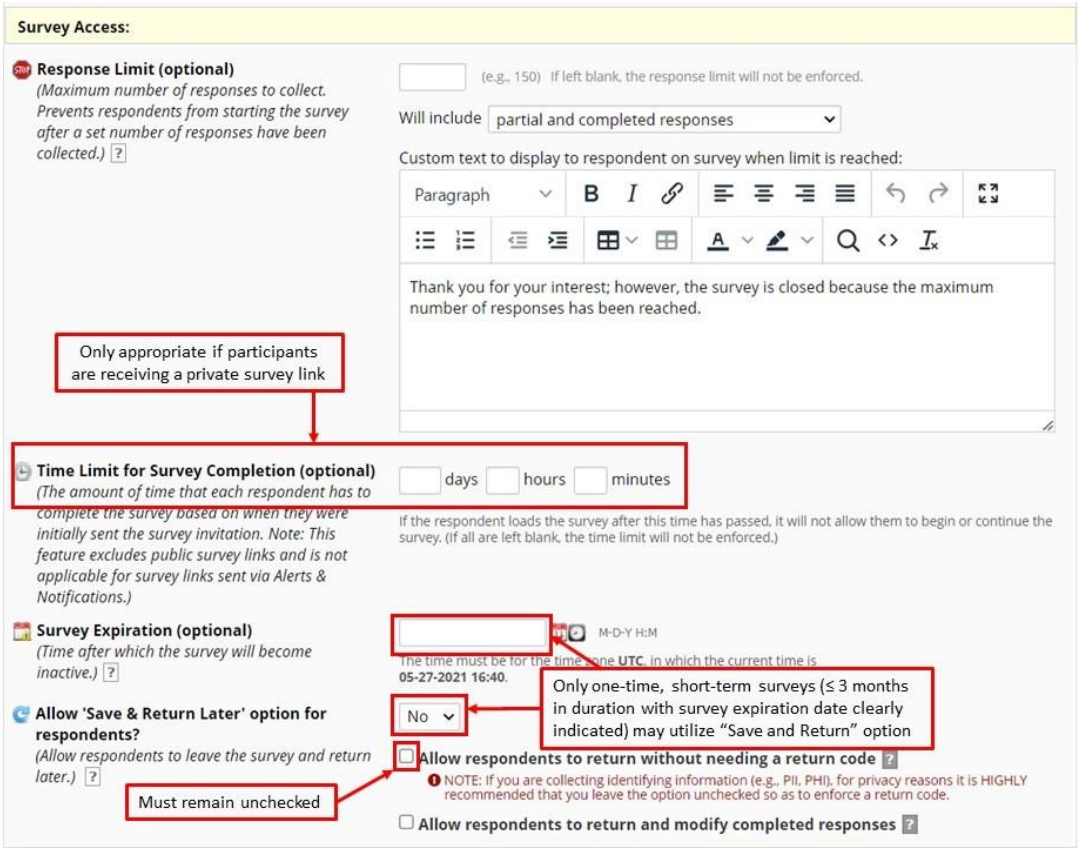
Utilizing Surveys in Illinois REDCap

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 private 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 surveys **may not use** this function.
- "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 IHSI REDCap Team prior to moving projects to production.



Additional Resources

- Illinois REDCap Homepage: https://healthinstitute.illinois.edu/redcap
- U of I Amazon Web Services Info: https://aws.illinois.edu
- U of I Box Health Data Folders Info: https://hipaa.uillinois.edu/protecting-phi-with-box-health-data-folders/
- U of I Cybersecurity Controls and Data Classification Info: https://go.illinois.edu/dataprivacy
- U of I HIPAA Homepage: https://hipaa.uillinois.edu/
- U of I HIPAA Privacy and Security Directive: https://hipaa.uillinois.edu/policies/
- U of I Office for the Protection of Research Subjects: https://oprs.research.illinois.edu/
- U of I Office of the Vice Chancellor for Research – Animal Care and Use: http://research.illinois.edu/regulatory-compliance-safety/animal-care-and-use
- U.S. Dept. of Health and Human Services De-Identification Info: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
- Vanderbilt University's REDCap Homepage: https://projectredcap.org/