Data Protection Checklist

Data protection and security is a process that begins in the early stages of research planning and development. While a project is in development, the research team should begin planning how they will protect data at every stage.

Below are suggestions for how to ensure data is being appropriately protected throughout the research lifecycle when Illinois REDCap is used during the data collection process. Researchers should also consult with their unit's IT professionals for localized recommendations and best practices.

Project Planning

1. □ Identify what data will be collected and what level of protection it needs.
    a. Remember, any health data should be treated as high-risk data, no matter the source!
    b. Only plan to collect identifiable data when it is absolutely necessary. For example, if you will not be using participant phone numbers for anything, do not collect participant phone numbers.
2. □ If receiving data from a secondary source accompanied by a Data Use Agreement, make sure you thoroughly read and understand any terms, conditions, and restrictions set forth in the agreement.
3. □ Clearly establish the responsibilities of research team members during the research project, including responsibilities for data collection and security.
    a. If data needs to be shared with external collaborators, plan for how that will be done securely and at what stages.
    b. Set expiration dates for researchers who will have an established, finite amount of time on the project, such as graduate students or research assistants who will only be working on a project for a semester.
1. □ If it is a project that needs approval from a compliance unit (e.g. IRB approval), incorporate their requirements and suggestions.
2. □ Check that all identifiers are marked as identifiable information in REDCap, even if you do not plan on exporting that data from REDCap.
    a. This can be done in "Online Designer" when creating a new field or editing an existing one. To mark a field as an identifier, select the "Yes" radio button on the right-hand side of the "Add New/Edit Field" pop up.
    b. In REDCap, a quick way to check if identifiers have been marked is to select the "Check for Identifiers" hyperlink on the "Project Setup" page. This link will be in the box titled "Design your data collection instruments & enable your surveys." This feature scans the fields, looking for keywords for pieces of data that are commonly identifiers (e.g. name, email, etc.). Identifiers can be updated from this page. However, this module may not capture all identifiers, so conscientiousness is recommended when building the project.
    c. "Checkmate" is a macro developed by the REDCap team at the University of Colorado Anschutz Medical Campus that is available to all Illinois REDCap users moving projects from development to production. "Checkmate" scans data dictionaries for keywords, such as birth or address, and marks them as potential identifiers. Running the macro generates a report that can be used to verify that identifiers are marked and validation and coding best practices are followed. This macro does not automatically update

information in REDCap and changes must be made manually. For more information, see Checkmate.

Active Data Collection

1. □ Ensure user rights are assigned based on the minimum necessary standard.
    a. Conduct periodic reviews of user rights to ensure they are still appropriate and limited to people who are currently on the research team.
    b. Set expiration dates for user access for users you know will have a finite amount of time working on the project.
    c. REDCap allows researchers to set pre-defined user roles, to which individual users can be assigned. This is a good way to add members for large labs or long-standing projects.
2. □ Follow the data collection and privacy and confidentiality measures that were approved by relevant compliance units.
3. □ Store collected data securely.
4. □ Check the logs on a regular basis to see who has altered or exported data.
5. □ Limit how often you export data, and only do so when you must run reports or analyses outside of REDCap. Utilize the report features in REDCap whenever possible.

End of Active Data Collection

1. □ Close surveys or forms by moving them offline as soon as possible to ensure no additional data is entered. If you know when you would like a survey to end, or how many people you would like to take a survey, you can define those parameters in the "Survey settings."
2. □ Illinois REDCap can be used for long-term data storage. However, if an alternative storage solution is more appropriate, be sure to use a secure, Illinois-approved service such as a U of I Box Health Data Folder (BDHF) or Amazon Web Services (AWS). See Protecting High Risk Data for more details.
3. □ Utilize data export features in REDCap that remove identifiers data during the export process, such as date-shifting and removing data marked as identifiable.
4. □ De-identify other data as necessary, such as removing or re-coding location data.
5. □ Practice secure transfer, such as by utilizing encrypted connections and/or encrypting data prior to transfer. Consult with your unit's IT professionals to discuss what options are best for you.
6. □ If retaining an identity key, ensure it is stored securely and separately from other data.

API Tokens (if applicable)

1. □ Ensure access to any API token is limited to the user who requested the token and is secured within an encrypted script rather than plain text.
2. □ Regenerate tokens every 90 days.
3. □ Report all security incidents (e.g., compromised, unsecured, lost and/or stolen tokens) involving API tokens to REDCap administrators (redcap-admin@illinois.edu) and the IRB and/or HIPAA liaison, as necessary.