Recommendations for IRB Applications

Due to the security of the system, Illinois REDCap is a great resource to use to assure the Institutional Review Board (IRB) that you are doing everything possible to protect the interests of human research participants. Below are recommendations for how to write about REDCap in your Illinois IRB applications.

Completing the New Study Application Form

(Version Date January 9, 2023)

Section 8: STUDY INFORMATION

Section 8.10 ("Describe all procedures chronologically, from screening/enrollment through study closeout, which will be completed in the research project.") -- If using surveys, specify that survey data will be collected using REDCap. If building a database from paper surveys or secondary data, specify that the database will be built using REDCap.

Section 9: DATA MONITORING

- **Section 9.1.2** ("Other or additional subject privacy-related details (specify)") -- Specify that your data will be stored in REDCap, which has the ability to limit user rights for viewing and exporting identifiable data.
- **Section 9.2.1** ("What precautions will be used to maintain the confidentiality of identifiable information?") -- Select the boxes that are accurate to how your survey is set up.
- **Section 9.2.3** (Where will electronic and/or hard copy research data be stored?")
    - Specify that your data will be stored in REDCap, which is HIPAA-capable and has the following abilities:
        - Limiting user rights to who can view and export identifiable data.
        - Providing an audit trail of who has exported data.
        - Signing into REDCap requires 2FA.
    - Remember: REDCap is only for storing data during active data collection, so make sure you specify where else data will be stored once it is moved from REDCap (e.g., Box Health Data Folder).

Section 11: RESOURCES AND RESPONSIBILITIES

Section 11.2 ("Describe the training that study staff and investigators will receive in order to be informed about the protocol and understand their research-related duties and functions.") -- Describe how user rights to viewing and exporting identifiable data will be set.

Section 10: RISKS AND BENEFITS

Section 10.1 ("Describe the reasonable foreseeable risks or discomforts to the subjects.") -- Since there is almost always a risk of a breach of confidentiality, it should be mentioned here. You can also discuss how the use of REDCap minimizes this risk and further protects the privacy interests of participants through limiting user rights, being built in a HIPAA-capable environment, and having an audit trail to track any unnecessary exports.

Section 12: Additional Information

12.1.4 ("Creating or sending data and/or samples to a repository or database to be saved for future research uses?") -- If you choose "Yes" for this question, you will need to describe how you intend to export REDCap data without identifiers in the Databases and Repositories Form.

Submitting a REDCap Survey or Questionnaire to the IRB

Once instruments are built in REDCap, it's easy to download a PDF of the survey or instruments to submit with an IRB application. To do this, follow the following steps:

1. In REDCap, select "My Projects."
2. Select the project you want to download the survey or instruments for.
3. Under "Project Home" select "Online Designer and Data Dictionary Upload" (found under "Quick Tasks") or under "Project Setup" select "Online Designer."
4. Next to the instruments you want to download, select the small PDF icon, which will automatically download a PDF copy of the instrument to your computer.

Completing the Databases and Repositories Form

- **Section 4.2.1** ("If you selected Option 2 or 3 above (in question 4.1), describe the process for de-identifying the data/samples.")
  - Explain how data will be exported from REDCap without identifiers.
  - Additionally, mention if the date-shifting feature in REDCap's data export tools will be used. (Date shifting is a method of de-identification in REDCap. During data export, dates in the project may be shifted up to 364 days back in time so as not to reflect actual dates. When date shifting is enabled, dates are shifted by a consistent length of time for each record, thus preserving the interval between dates.) For more about de-identification, see Protecting High Risk Data.