Version date August 15, 2019

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.

Exempt Form (version date December 3, 2018)

Research Procedures

- Section 8G ("Narratively describe the research procedures in the order in which they will be conducted.") – 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.

Confidentiality and Privacy

- Section 9A ("How are participant data, records, or specimens identified when received or collected by researchers?") – Check that this is accurate with how your survey is set up. Are you collecting identifiers, even if you do not intend to export them? If so, make sure "Direct identifiers are collected" is selected.
- Section 9B ("Select all methods used to safeguard research records during storage.") –
    - Mark "Electronic data is stored in a secure, UIUC-approved location" and specify that it will be stored in REDCap. 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).
    - Mark "Other" and specify that REDCap is a system that 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
- Section 9C ("How long will identifiable data be kept?") – If you will be utilizing REDCap's ability to export data completely de-identified, specify this here.
- Section 9D ("Describe provisions to protect the privacy interests of subjects.") – Here, you can reiterate various things related to user rights, 2FA, exporting of de-identified data, etc., as it's suited to your specific project.
- Section 9E ("Describe the training and experience of all persons who will collect or have access to the data.") – Describe how user rights to viewing and exporting identifiable data will be set.

Dissemination of Results

- Section 11C ("Do you intend to put de-identified data in a data repository?") – If yes, 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.

Protocol Form (version date December 3, 2018)

Research Procedures

- Section 14F ("Narratively describe the research procedures in the order in which they will be conducted.") – 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.

Confidentiality and Privacy

- Section 17A ("How are participant data, records, or specimens identified when received or collected by researchers?") – Check that this is accurate with how your survey is set up. Are you collecting identifiers, even if you do not intend to export them? If so, make sure "Direct identifiers are collected" is selected.
- Section 17B ("Select all methods used to safeguard research records during storage.") –
    - Mark "Electronic data is stored in a secure, UIUC-approved location" and specify that it will be stored in REDCap. Remember: Illinois REDCap is only for storing data during active data collection, so make sure you specify where data will be stored once it is moved from REDCap (e.g. Box Health Data Folder).
    - Mark "Other" and specify that REDCap is a system that 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 Illinois REDCap requires 2FA
- Section 17C ("How long will identifiable data be kept?") – If you will be utilizing REDCap's ability to export data completely de-identified, specify this here.
- Section 17D ("Describe provisions to protect the privacy interests of subjects.") – Here, you can reiterate various things related to user rights, 2FA, exporting of de-identified data, etc., as it's suited to your specific project.
- Section 17E ("Describe the training and experience of all persons who will collect or have access to the data.") – Describe how user rights to viewing and exporting identifiable data will be set.

Dissemination of Results

- Section 19C ("Do you intend to put de-identified data in a data repository?") – If yes, 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.

Risks & Benefits

- Section 20B ("Describe the steps that will be taken to minimize the risks listed above.") – Since there is almost always a risk of a breach of confidentiality, which would be mentioned in Section 20A, you can 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.

Additionally, 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.

*__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 example, if a participant, Mary, had three sequential appointments with actual dates of April 2, April 15 and April 26, when the dates are shifted, Mary's appointment dates may appear as November 16, November 29, and December 10.

Date shifting, if enabled, leaves the record intact and will not affect the actual saved dates in the project. It merely alters the dates in their resulting format when performing a data export in REDCap.

Date shifting is important for de-identification because dates, like name and social security number, are identifiers that can be used for identifying an individual and thus possibly exposing confidential personal information. Date shifting prevents any dates from being used as identifiers for each project record while preserving the interval between dates. For more about de-identification, see Protecting High Risk Data.