FSU REDCap User Agreement Form- Updated 2-5-23

FSU REDCap User Agreement

Revised: 2/5/23

All FSU REDCap users must agree to the terms and requirements outlined in this User Agreement, the REDCap User Rights & Roles document (*found online*), and the Protecting High-Risk Data document (*found online*) before using FSU REDCap.

By signing this document, all users acknowledge that they have read through, understand, and completed the training requirements needed to authorize access to REDCap.

There are 5 acknowledgement sections in this agreement form prior to the account request. You will be asked to read and acknowledge each section as you proceed through the form.

Requirements for Accessing and 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.

I agree to abide by the requirements outlined in the **Requirements for Accessing and Using FSU REDCap** section above.

REDCap Security Requirements. FSU Researchers must adhere to the following data security guidelines while using REDCap:

Only using their own login credentials to access REDCap. Logging out of REDCap when stepping away from their device. Exporting and securing data from REDCap for analysis in a secure environment, such as the HDSI's Virtual Desktop Interface (VDI), or a local computer/drive that is strongly encrypted (see this definition of strong computer encryption) such as with a Yubikey or another method outlined in the Protecting High-Risk Data document (*found online*), the HIPAA-Approved Tools/Strategies section. Only providing project access to research team members who have completed all requirements and are part of the project, and removing any research team members who are no longer part of the project. It is strongly recommended that PIs review and follow the guidance of the REDCap User Rights & Roles document (*found online*) when delineating user access and privileges in the REDCap system.

Adhering to appropriate data-sharing practices as stated in the Protecting High-Risk Data document. *Note: never email sensitive, medium- or high-risk datasets to other individuals (this includes HIPAA-protected data). Email is not a secure method of communication, including FSU's Outlook email exchange. It is strongly recommended (and for some granting agencies, required) that PIs submit a Data Management Plan (DMP). FSU Libraries can assist researchers with developing DMPs. Only using REDCap in a way that is compliant with REDCap's authorization statement (***below***) and that is compliant with any Data Usage Agreement (DUA) or Business Associate's Agreement (BAA) the researcher is beholden to.

*FSU REDCap can only be used for authorized university research, operations, and educational purposes. This research may be funded by external entities, including commercial or for-profit organizations, but shall not include the use of REDCap as the basis for providing a contract or other services to any entity (as per*REDCap License Term 1.6*).*

I agree to abide by the requirements outlined in the **REDCap Security Requirements** section above.

External Research Partner Requirements. Research partners external to FSU needing access to FSU's REDCap must (1) obtain a courtesy appointment and (2) complete this user agreement form. It is the PI's responsibility to:

Sponsor the external research partner for their FSU Courtesy Appointment. Ensure the external researcher has met institutional requirements to conduct collaborative research (i.e. obtained and provided a copy of their CITI training certificate in RAMP). Ensure the external researcher complies with any FSU College or Departmental requirements for research. Ensure the external researcher has completed appropriate HIPAA training and complies with FSU's OHSP HIPAA requirements. Add the researcher to the REDCap project once they have received their FSU and FSU REDCap credentials. It is also the responsibility of the PI to delineate the external researcher's role in REDCap (see the User Rights & Roles document, *found online*).

I agree to abide by the requirements outlined in the **External Research Partner Requirements** section above.

When Can a Researcher Access REDCap? REDCap users may access REDCap upon receipt of their REDCap login credentials. Users may access REDCap's development environment as they are building their research instrument. After the PI gains theirIRB approval letter for their research project, the designated researcher for that team will submit a request to the REDCap administrator to review their instrument and move their project from development to production (*note: you should never begin collecting data while your instrument is in development as this can affect the reliability and validation of your data upon a move to production). Once the project is in production, the research team can begin data collection.

I agree to **submit a request to the REDCap administrator** to move my REDCap project from development to production prior to collecting any data.

Institutional Review Board (IRB) Application Language Recommendation. The PI may enter the REDCap environment prior to submitting an IRB protocol to develop the instrument, as stated above. However, before any research involving human subjects may be conducted, including the collection of any data, documentation of IRB approval is required. Researchers may consider using the following boilerplate language in section 7.0 Data and Specimen Banking (describing how data may be banked and used or shared for future research) and/or section 17 Data Management and Confidentiality (describing how data may be managed and protected) of the IRB protocol application (HRP-503; HRP-503a; HRP-503r) if using REDCap:

"Data from this project is being collected and stored in FSU's REDCap, the Research Electronic Database Capture technology system. REDCap is an environment designed to securely store and manage medium- to high-risk data, such as Protected Health Information, and is compliant with HIPAA requirements.

Data processing (compute and/or analysis) will occur [STATE YOUR METHODS FOR PROCESSING DATA IN A SECURE ENVIRONMENT HERE (I.E. *"…by exporting data to a local desktop, analyzing data in a protected virtual desktop environment, and storing data on a local hard drive using appropriate encryption methods via a Yubikey."* OR *"…by exporting data to a local desktop, analyzing data in a protected virtual desktop environment, and storing data in FSU's Azure Cloud, which is compliant with HIPAA requirements for data processing and storage.")*].

Researcher access to REDCap must include secure on-premises and remote access components. On-premises access will require connectivity to the FSU enterprise network and a current FSU ID and password. Remote access for internal or external collaborators will require multifactor authentication and a current FSU ID and password. Through access management controls in REDCap, only users with permission from the PI can access the project data.

Data retention requirements indicate research data must be stored/retained for seven (7) years

beyond the end of data collection associated with this project. Data will be stored [STATE WHERE YOU WILL STORE DATA AND HOW YOU'LL KEEP IT SECURE (I.E. THROUGH STRONG ENCRYPTION, CLOUD STORAGE, ETC.)]."

IF YOU'RE PLANNING ON (or if the IRB requires) DEIDENTIFYING DATA: "*Participants' data will be deidentified* [INSERT METHOD FOR DEIDENTIFICATION HERE. IF COLLECTING PHI, REFER TO THE PROTECTING HIGH-RISK DATA DOCUMENT TO DETERMINE HOW YOU WILL DEIDENTIFY DATA]."

Research Citation Recommendation. When using REDCap for research it is recommended the researcher use the following boilerplate language (keep in mind you may need to edit citations based on your publication formatting requirements):

"Study data were collected and managed using REDCap electronic data capture tools hosted at [YOUR INSTITUTION].1,2 REDCap (Research Electronic Data Capture) is a secure, web-based software platform designed to support data capture for research studies, providing 1) an intuitive interface for validated data capture; 2) audit trails for tracking data manipulation and export procedures; 3) automated export procedures for seamless data downloads to common statistical packages; and 4) procedures for data integration and interoperability with external sources."

1PA Harris, R Taylor, R Thielke, J Payne, N Gonzalez, JG. Conde, Research electronic data capture (REDCap) – A metadata-driven methodology and workflow process for providing translational research informatics support, J Biomed Inform. 2009 Apr;42(2):377-81.

2PA Harris, R Taylor, BL Minor, V Elliott, M Fernandez, L O'Neal, L McLeod, G Delacqua, F Delacqua, J Kirby, SN Duda, REDCap Consortium, The REDCap consortium: Building an international community of software partners, J Biomed Inform. 2019 May 9 [doi: 10.1016/j.jbi.2019.103208]

Additional Terms & Conditions. Any updates made to FSU's REDCap User Agreement will be sent to current users via email. Continued use of REDCap after the agreement has been sent implies consent to the agreement changes. Any user found in violation of the FSU REDCap User Agreement may have their account suspended until issues have been resolved. The FSU REDCap administrator will handle any issues on a case-by-case basis and will communicate violations and steps to restore the user account via email. The FSU REDCap administrative email is only monitored for system emergencies during evenings and weekends. General requests will be addressed M-F from 8a-5p.

I understand the **Additional Terms & Conditions** outlined for FSU REDCap.

Requester Information

First & Last Name

_____

Your Title

_____

Institution (Higher Ed Researchers) / Organization (Non-Higher Ed Researchers)

_____

College/Department (Faculty Researchers)

_____

Affiliation:

- ○ FSU Faculty (1)
- ○ FSU Post-Doc (2)
- ○ FSU Staff (3)
- ○ FSU Graduate Student (4)
- ○ FSU Undergraduate Student (5)
- ○ External Higher Ed Research Partner (6)
- ○ External Healthcare Research Partner (7)

○ Other External Affiliate (8)

_____

FSU Email Address (external partners need to complete the courtesy appointment process to receive an FSU ID)

_____

Phone Number

_____