Terms of Use

The University of Florida (UF) requires that all data collected or stored in REDCap follow the processes and procedures outlined in this document.

- All human research studies must have Institutional Review Board (IRB) approval before the research study can be moved to production and data collection can commence.
- The name of the Principal Investigator (PI) must be provided.
- If the research study will include other collaborative personnel such as co-investigators, technicians and students, the principal investigator must assure that the personnel are listed on the approved IRB form.
- If data is collected that is considered either sensitive, protected health information, or HIPAA information, then prior to using the system the user must complete all necessary training including but not limited to required HIPAA training. http://privacy.ufl.edu/privacy-training/hipaa-training/
- Social Security Number training is required annually for all UF personnel who use SSNs in their work or research. The "Protecting Social Security Numbers" training module is available only through myTraining. http://mytraining.hr.ufl.edu/
- It is the responsibility of the principal investigator to ensure that collaborative personnel have the appropriate study-specific and related training and have reviewed the required safeguards according to UF policies and procedures.
- Users of REDCap must adhere to all UF computer policies, regulations, rules and standards. It is the responsibility of the principal investigator and the administrator of each account to routinely monitor their REDCap projects.
- Users of Application Programming Interface (API) must understand the risks when using the API Token.
- If a project or collection is identified as not having an owner because the primary owner has left the university, the department head and secondary owner (if available) will be contacted to locate a new owner. If no new owner is approved, the project or collection will be removed from REDCap.

REDCap Support and Contingency Policies

The Clinical and Translational Science Institute (CTSI) at the University of Florida provides free of charge the use of REDCap™ (Research Electronic Data Capture) software as a service for UF investigators and their teams to collect study data. This service includes the REDCap application software hosted in a web server, server space for data storage, regular system backups, software patches and upgrades.

In the event of a system shut-down, a 24 hour recovery time objective is achievable. UF Health IT has a Disaster Avoidance and Recovery Plan that covers responsibilities, communication, and escalation. The recovery point objective for the REDCap database is 1 hour (no more than 1 hour of data loss). The recovery point objective for the web server is 24 hours (no more than 24 hours of data loss).

- PIs should maintain printed copies of REDCap forms to enable offline data collection and subsequent data entry if there is a need to collect data during an outage.

In the event of an expected catastrophic disaster, such as loss of a data center due to a hurricane, the REDCap Support Team (Administrators) will notify all REDCap users via e-mail of the potential threat.

- PI's are advised to move/export data to a disk and to a storage area approved for sensitive data.

In the event of scheduled System maintenance the REDCap Support Team (Administrators) will notify all REDCap users via e-mail one week prior, one day before and on the day of the scheduled maintenance. All users are notified via e-mail when the system is available again.

Data is not available for export from REDCap during a REDCap outage.

User Responsibilities for IRB studies:

- Complete all necessary training including but not limited to Human Research Studies training (CITI) and required HIPAA training.
- Safeguard all data in compliance with all applicable university policies and standards, federal regulations and state laws.
- Do not to release or share data except as described in the approved IRB application.

Additional Principal Investigator Specific Responsibilities for IRB studies:

- Assure that all requested collaborators have completed all necessary training including but not limited to Human Research Studies training (CITI) and required HIPAA training.
- Acknowledge sole responsible for all who have access to the study data.
- Agree to monitor the activity and users who have access to the data, and promptly remove users who no longer need access.
- Agree to only use the minimum necessary PHI identifiers linked to sensitive data.

Best Practices

When the REDCap project is in “development” stage:

- Test/QC project with sham (fake) data. Do not enter real data into the project.

When the REDCap project is moved to “production” stage:

- Erase all sham data.
- Mark all fields containing protected health information (PHI).
- Set up User Rights.
- Create PDF files of all forms to use in case the system goes down.
- Export data (back up) to File Repository on a regular basis.
- Assure all who are on the project are also on IRB schedule A (if applicable).
- Check Project Dashboard regularly. Do not delete users from Project but rather “expire” access as needed.

When the REDCap project is moved to “archive”:

- Lock all data.
- Create PDF file of all data and burn to disk. Maintain this disk in a storage area approved for sensitive data.
- Export data to disk and maintain in a storage area approved for sensitive data.
- Assure PI is on the project with full user rights.
- Expire all users from the project except PI and primary administrator (if applicable).