ADMINISTRATIVE POLICY AND PROCEDURE

SUBJECT:	APPROPRIATE USE OF REDCap and REDCap Survey
DOCUMENT MANAGER:	BIOMEDICAL and BEHAVIORAL METHODOLOGY CORE OUHSC
EFFECTIVE DATE:	xx/xx/2014
REVISED DATE:	3/14/2014 by BBMC
SUPERSEDES:	N/A

Scope:

All researchers wishing to use REDCap for managing clinical research data or REDCap Survey for collecting study participants' responses on-line.

Purpose:

To protect patient/participant privacy and confidentiality while assisting researchers in conducting biomedical and behavioral research.

Preamble:

REDCap (Research Electronic Data Capture) and REDCap Survey are powerful software programs created by Vanderbilt University and supported by the REDCap Consortium to facilitate Institutional Review Board (IRB)-approved clinical research and basic research. Data collected in the course of research are managed by local REDCap systems (hosted in the OUHSC IT Data Center), and can be analyzed by commonly used statistical packages, including SAS, Stata, SPSS, and R.

REDCap has a flexible and fine-grained authorization matrix, allowing different members of the study team to have different levels of access (none, read-only, or edit) to data entry forms, and access to database management and data export tools. There are provisions to restrict access to data export to allow export of de-identified data only.

REDCap enforces authorization granted to each user by providing and/or enabling certain functions, tabs, links, and buttons according to granted privileges.

REDCap includes a full audit trail, recording all operations on the data, including viewing and exporting. The audit log records operation, date and time, and the user performing the operation, permitting review of the audit trail as necessary.

REDCap enforces data integrity protection by design; all "databases" created by users are logical data sets on top of a relational database with built-in integrity protection controls. Additionally, REDCap can help to ensure data quality through use of Double Data Entry mode, forms, and records locking and electronic signatures.

Definition of Terms:

Authentication/Authenticated User

A confirmation from the authoritative source (Active Directory, LDAP, etc.) that the user credentials (user name and password) are valid.

Authorization

A set of rights to access specific objects (forms, tabs, controls) in specific mode (read-only, read-write or edit, full data set, de-identified data set) granted to a research team user. The Project Owner will determine and authorize the users for their respective projects. Individual user's access levels will be set by the Project Owner. Authorized access by users will be audited routinely by the BBMC administrators.

BBMC

Biomedical and Behavioral Research Core of OUHSC. This group of biostatisticians and data systems experts was selected by OUHSC IT and a REDCap Governance Body to be responsible for the general administration and maintenance of all REDCap instances, management and organization of the REDCap governance body, user education, and management of databases (moving to production, approving changes when in production, restoring from backup, etc.) in the BBMC customization box.

BERD

Biostatistics, Epidemiology, and Research Design (BERD) Core of the Oklahoma Shared Clinical and Translational Resources (OSCTR) of OUHSC. The BERD includes biostatisticians and data systems experts who develop and implement data collection processes in REDCap; educate end-users; and manage databases (updating software versions, moving to production, approving changes when in production, restoring from backup, etc.). The REDCap Governance Body has granted BERD primary responsibility for implementing and managing studies utilizing the OUHSC Enterprise instance of REDCap.

Database

A research database implemented in REDCap. A set of data entry forms, schedules, and other REDCap instruments pertaining to a specific study or research project.

Development Mode

A state of database that allows authorized Research Team members to add, modify, or delete data entry forms and other elements of the study design. In the development mode, the database is temporary and is not backed up. No data is guaranteed to be preserved in the database in this mode.

PI

Principal Investigator. A person responsible for the conduct of the research study, including the appropriate use of the REDCap research database by all members of the Research Team.

PO

Project Owner. A person designated by the PI to be responsible for the conduct of study data collection, including assignment of the roles and authorizations to use specific forms and functions of the REDCap project to the members of the Research Team.

Production Mode

A state of database that allows authorized Research Team members to add, modify, or delete clinical research data. All data stored in the production database is on a virtual server that resides in a high availability cluster. If there is a hardware related problem, the server will simply move to another server

in the cluster. The database server is configured for nightly exports that are then backed up using an enterprise backup solution. Backups are retained for 15 days. Any modification to the data collection design in this mode will need to be approved by the BBMC or the OSCTR BERD cores (see descriptions below). BBMC and BERD cores offer to review proposed changes before approval to ensure data integrity (note: this may or may not require fee-for-service charges, depending on institutional funding of REDCap support and project qualification status), but this review is not a requirement of approval.

REDCap Governance Body
An oversight committee composed of key stakeholders throughout OUHSC with a mission to facilitate access to and guide proper use of REDCap on campus. Members include administrators of the College of Medicine, Office of Research Administration, University Institutional Review Board, OUHSC IT, BBMC, and BERD.

Research Team

PI, PO, Research assistants, nurses, data entry persons and other personnel granted access to the REDCap research database. These *REDCap users* can be OUHSC personnel or personnel from another institution working on or in collaboration with an OU research project. Non-OUHSC personnel must have an authorized OUHSC login ID before being granted access to REDCap. Access to a REDCap project is granted, first, to the PO by one of the REDCap administrators (BBMC or BERD personnel). Future access to the project for the other Research Team members is managed by the PO.

Policy

Any Authenticated User has a right to access REDCap, review public databases (e.g., demo databases), and create a new database or modify a database for which corresponding authorization has been granted (e.g., his/her own). Currently, the University of Oklahoma Health Sciences Center Directory serves as the Authentication source.   There are three REDCap installations available: https://rcapdev.ouhsc.edu (development only), https://bbmc.ouhsc.edu (BBMC customized version for internal development and production), and https://redcapweb1/redcap (an enterprise version for general development and production).

Any new user is strongly encouraged to make an appointment with the BBMC or BERD Core for an introduction to REDCap (about 1 hour) before attempting to create a new database in REDCap. A REDCap project request form is available online (https://bbmc.ouhsc.edu/redcap/redcap_v4.11.2/Miechv/Informatics3.html). Project requests should be accompanied with an uploaded study design proposal (protocol or grant submission) at least 1 full working day before the appointment.

Any new Database will be created in Development Mode. When a Database is in Development Mode, the user cannot enter any identified patient information. For testing purposes, fictional identifiers must be used. BBMC will periodically review contents of all databases in Development Mode to ensure compliance and report violations to the Privacy Officer of the institution whose data is being used. In the case of data regarding patients or participants of OUHSC and its affiliates, all users must comply with Health Insurance Portability and Accountability Act (HIPAA) Privacy (http://www.ouhsc.edu/hipaa/) and Security (http://it.ouhsc.edu/policies/) Policies and Procedures for "Protected Health Information" (PHI), Family Educational Rights and Privacy Act (FERPA; http://www.ouhsc.edu/admissions/FERPA_Notice.htm) Policies and Procedures for protection of educational records, and all other human subjects information privacy and security protections (for more information, please contact the Office of Human Research Participant Protection (HRPP) Program at 405-271-2045 or irb@ouhsc.edu or the University Privacy Official at 405-271-2511 or compliance@ouhsc.edu).

It is the responsibility of the PI to:

- Obtain IRB approval prior to using REDCap for studies involving human participant research
- Build the REDCap database (entry forms) in such a way that it corresponds to the study design that will be submitted to the IRB and provides proper data collection tool for all the data necessary for testing the study hypothesis (hypotheses)
- Collect all the data necessary for testing study hypothesis (hypotheses)
- Limit REDCap storage of PHI to the minimum that is reasonably necessary to conduct the research

Alternatively, the PI may request that BBMC or BERD share the above responsibilities and directly participate in the development of the REDCap database for the study, via separate agreement between the PI and one of the two Cores (BBMC or BERD).

To move a database into production, the study PI or authorized PI representative needs to request a review by BBMC or BERD, providing the following information:

- IRB-approved research protocol or final version of the research protocol (for studies not requiring IRB approval)
- IRB approval letter (or letters, if multiple IRBs and/or regulatory bodies; e.g., VA Research & Development Committee are involved) or an IRB exemption notice
- A signed copy of the REDCap Use Agreement.

After review and approval, BBMC or BERD will move the database into production and the study team will be able to collect research information. Please note the distinction between a REDCap Use Agreement, which enables access to a REDCap project for authorized members of the Research Team, and an IRB data use agreement for sharing data (perhaps within REDCap) with members outside the research team. Permission for the latter will require a separate IRB-approved Research Privacy Form (http://www.ouhsc.edu/irb/IRB_Forms_HIPAA_MainPg.asp). Users are encouraged to contact the IRB should questions arise about which privacy forms are required for each specific data sharing instance.

REDCap and REDCap Survey are being supported by BBMC, BERD, and OUHSC Information Technology. BBMC, BERD, and OUHSC IT bear responsibility for maintenance of the software, Database deployment (moving to production) and data security and integrity.

The PI is responsible for managing access to the PI's database(s) to ensure compliance with HIPAA, FERPA, and other state and federal regulations protecting patient/participant privacy and confidentiality.

Aside from regularly scheduled audits for the IRB, audit trails of any user over any period of time will be produced at the request of the Decision Support Group, OUHSC IT Leadership Team, HIPAA Privacy Official or Security Officer, or Chair of the Institutional Review Board.

IRB-approved research protocols utilizing REDCap or REDCap survey will be tracked by the BBMC in a database which will keep the name of the PI, the title of the protocol, the IRB protocol number, the date of access provision, and date of access deactivation.

IRB Auditing

- The BBMC will perform nightly audits of user access for each REDCap instance. When an unauthorized user has been identified by the auditing system, the user and PO will be immediately notified by email and encouraged to resolve the issue. Should a problem persist, weekly reminders will be sent to the user and PO. If a resolution has not occurred after 90 days, a REDCap administrator will notify the IRB of a possible protocol violation. The IRB will then determine if and what corrective actions should occur.
- Upon request, the IRB will have access to an audit report of IRB approved use, and any research/study documents maintained by BBMC.