Recommendations from OUHSC IT, 9/10/13

**

*ADMINISTRATIVE POLICY AND PROCEDURE*

SUBJECT: APPROPRIATE USE OF REDCap and REDCap Survey

OWNER: BIOMEDICAL and BEHAVIORAL METHODOLOGY CORE OUHSC

EFFECTIVE DATE: x/xx/2013 REVISED DATE: 8/26/13 by OUHSC IT 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 the research are managed by the program, 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:**

**PI**

Principal Investigator. A person responsible for the conduct of the research study, including assignment of the roles and authorizations to use specific forms and functions of the REDCap research database to the members of the research team.

**Research Team**

PI, Research assistants, nurses, data entry persons and other personnel granted access to the REDCap research database.

**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.

**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 (by REDCap design). As a fee-for-service option, BBMC offers to review proposed changes before approval to ensure data integrity; should PI opt out by requesting that BBMC automatically approve any changes, it will be PI's responsibility should the changes violate data integrity or consistency.

**BBMC**

Biomedical and Behavioral Research Core of OUHSC. A group responsible for the implementation and maintenance of REDCap, for user education, and for management of databases (moving to production, approving changes when in production, restoring from backup etc.).

**Authentication**

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 user.

**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://miechvprojects.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 for an introduction to REDCap (about 1 hour) before attempting to create a new database in REDCap. Please fill out the REDCap project request form that is available online (<https://miechvprojects.ouhsc.edu/redcap/redcap_v4.11.2/Miechv/Informatics3.html>) and upload a proposed study design (protocol or grant submission) to this BBMC web-form at least 1 full working day before the appointment.

Any new database will be created in development mode. When in development mode the user cannot enter any identified patient information. For testing purposes use fictional identifiers. 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 her 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](mailto:irb@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 study hypothesis (hypotheses)

• Collect all the data necessary for testing study hypothesis (hypotheses)

• Collect only minimally-necessary set of PHI, in addition to those required by study design or operational requirements, to positively identify study subjects during data entry phase

Alternatively, the PI may request that BBMC share the above responsibilities and directly participate in the development of the REDCap database for the study.

To move a database into production, the study PI or authorized PI representative needs to request a review by BBMC, 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 Data Use Agreement.

After review and approval, BBMC will move the database into production and the study team will be able to collect research information.

REDCap and REDCap Survey are being supported by BBMC and OUHSC Information Technology. BBMC 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.

Review of audit trails of any user over any period of time will be undertaken at the request of the Decision Support Group, OUHSC IT Leadership Team, HIPAA Privacy or Security Official 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 IRB will be regularly sent an auditing report on the activity and authorized users of all human research projects. The report will allow IRB to monitor protocol compliance.

• Upon request, the IRB will have access to an audit report of IRB approved use, and any research/study documents maintained by BBMC.