REDCap Security Template- Addresses D105 issued by IRB for Confidentiality and Data Security Guideline for Electronic Data

REDCap is a secure web based application for building and managing online surveys and databases. The application is trademarked by the Vanderbilt CTSA; however, the data is housed on local servers with in house control.

REDCap is implemented as a secure web server (HTTPs) located within IPOP behind a firewall on UK’s network. Accounts are created using the mc/ad domain account generated by UK and is used for authentication purposes. This login process requires individual password protection for investigators.

Investigators can assign additional users of REDCap to their Projects/Surveys and define permissions for each user. User rights issued include the ability to invite participants for survey responses, creation of calendar events, import or export of data-which can be further secured by enabling export of data as a full data set or as deidentified only, ability to build reports, lock or unlock records when entry is completed, create records, rename records, edit records, or delete records, or determine if an electronic signature is required for certain events. In addition, each user can be given an expiration date which will remove access to that individual user.

REDCap survey projects can be configured according to individual IRB approved protocols. Data may be collected with identifiers or anonymously. Respondents are invited via email and REDCap validates and tracks responses through this email. Once a respondent has completed a survey, they cannot reenter the survey again. This prevents duplication; however, if a survey is posted through a web link, less control is given to the investigator on preventing duplication of responses. When recorded into the database, the investigator can only see a unique number generated for that respondent and date and time completed. IP addresses are captured during survey completion, but they are scrubbed from the data viewed by investigators. REDCap does not share IP addresses with other consortiums.

When investigators are logged onto REDCap to enter data into their case report forms, a vulnerability to hacking the account while open is of concern; however, all data is encrypted when transmitted to the REDCap server. Portable devices are not at risk because nothing is downloaded onto the device, a secure web based connection is used for all data collection.

Data storage on portable devices is not a security concern for REDCap administration, but appropriate measures should be taken when exporting data from REDCap. To assist investigators, REDCap has an email function that offers greater security for large attachments that contain sensitive data. Each recipient receives an email containing a unique downloaded URL, along with a second follow up email with the password for downloading the files. The file is stored securely and removed from the server upon the specified expiration date.