# Resource Template for REDCap

REDCap (Research Electronic Data Capture) is a secure web based application tool used for building and managing surveys and databases used for research, created by Vanderbilt University. Vanderbilt developed a Consortium of institutions to share this research and data capture tool. The Consortium was launched in 2006 and has Consortium partners including the University of Kentucky. The security of the application is largely dependent on the IT infrastructure and environment in which REDCap is hosted, not the software itself. Vanderbilt has a list of best practices that were utilized when installing and hosting the REDCap instance locally. For more information on Consortium Partners, please view http://www.project-redcap.org/consortium.php.

The University of Kentucky REDCap instance was installed in the Institute for Pharmaceutical Outcomes & Policy in 2008 and is located in 180 BioPharm Complex (BPC). The web server and the database server are located on separate servers behind a firewall with in-house control with UK's campus network. In addition, in order to maintain secure communications, the web server has a secured security license (SSL) and is located on https://redcap.rdmc.org/redcap/. Research data is stored locally and is backed up daily using MySQL Administrator software using the Windows Server 2008 R2 edition.

REDCap implements authentication of users that log into the system. All accounts are set up using the LinkBlue ID and are password protected. Furthermore, the software has an auto logout feature included. Once a REDCap user creates a project, they are the owner and have full rights to the project. Once study personnel/users are added by the owner, user rights or privileges are established. User rights can be for view only, edit only, or view and edit. User rights or access, can be further limited to individual case forms within the project. Custom locking of case report forms or digital signatures are another feature that can be assigned in the user rights section of the project. REDCap maintains a built-in audit trail that logs all user activity and pages viewed. The logging record can be viewed by those with proper user rights.

Data exportation is defined within the user rights section, and can be limited by user as a full data set or as a deidentified data set. Data is exported into comma delimited (CSV) files which can be uploaded into Excel, SAS, SPSS, STATA, or R for analysis. Advanced features of deidentification include removal of free form text, removal of dates, date shifting that keeps the integrity of the date interval, and/or removal of fields tagged as identifiers. REDCap also has an internal email function for large data sets or sensitive data. This feature can be used to send emails to non-REDCap users as well. The file is stored on REDCap and allows non users to log in using a secure password to download the files (password to access email is sent in a separate email to the user).

REDCap stores its system data and project information in various relational database tables within a single MySQL database. All data submitted via the web server by the researcher is encrypted while transmitted. The portable devices do not download the data, it is directly stored into the secure web based connection (https) behind the firewall. This reduces the liability and possibility of researchers losing protected health information. All files are password protected once entered into the system. All project data is stored and hosted locally. No data is ever shared with Vanderbilt or the consortium partners.

REDCap software uses various methods to protect against malicious users that attempt to identify or exploit any security vulnerabilities in the system. In REDCap, all data is intentionally filtered, sanitized, and escaped for every query string data found in the URL while accessing REDCap. Server environment variables that are vulnerable to forgery by users are checked and sanitized. All user submitted data is filtered for any possible harmful mark-up tags (scripts) and then escaped prior to ever being displayed on a web page within the application. SQL queries sent to the database server from REDCap are properly escaped prior to being sent. User defined data used within the SQL query has the data type checked to prevent any mismatching of data types (makes sure a number is really a number). The processes of filtering, sanitation, data type checking, and escaping all help to protect against methods of attacks.

The Consortium has grown to 1997 active institutional partners in 105 countries with 398,000 users since 2006 with 290,000 products currently in production. The University of Kentucky currently has over 2300 users with over 1600 projects in production and another 1200 projects in development. All members of the Consortium are active in the future development of REDCap functionality and software testing. Users are also engaged in a Regulatory and Software Validation Committee which includes compliance with 21 CFR Part 11, HIPAA, and other regulations.