REDCap Technical Overview

Introduction

There is a fairly short list of infrastructure requirements and dependencies for installing REDCap. REDCap can run on a number of different operating systems (Linux, Unix, Windows, Mac). The only requirements that REDCap has are that the hardware and software listed below be installed. (Note: All required software is open source.)

REDCap Infrastructure Requirements and Dependencies

1) **Web server** (e.g. Microsoft IIS or Apache)
    a. PHP – version 5.1.2 and up (download and install PHP)
    b. PHP frameworks and extensions needed
        i. cURL extension is required for some optional components (how to install cURL)
        ii. MySQLi extension is required in PHP
2) **Database server**
    a. MySQL database – version 5.0.0 and up (how to install MySQL)
    b. MySQL client – required for installation/upgrades (e.g. phpMyAdmin, MySQL Workbench)
3) **SMTP email server** – In order to send emails from REDCap, an SMTP server must be configured with PHP on your web server. It can be installed on the same web server or on a separate server (preferred), such as an existing institutional SMTP server, if available.
4) **File server** (per[illegible]

for them. The table-based authentication, which utilizes the storage of username/password pairs in a database table, is often the easiest to set up because it is built-in and requires no setup and no configuration with external services in order to operate. For security reasons, the password in the database table is not stored as plain text but as an encrypted one-way hash of the password.

REDCap contains an auto-logout setting, which is customizable (default auto-logout time is 30 minutes), and will automatically log a user out of the system if they have not had any activity (e.g. Rtn y

will have the data de-identification methods imposed as a means of preventing them from exporting sensitive data, either mistakenly or intentionally.

REDCap Data Storage

REDCap stores its data and all system and project information in various relational database tables (i.e. utilizing foreign keys and indexes) within a single MySQL database, which is an open source RDBMS (relational database management system). The front end of REDCap is written in PHP, which is a widely used, robust, open source scripting language for web applications. Setting up the web server and database server and securing the communication of the servers to each other and to the end-user are the responsibilities of the partner institution that is installing REDCap, and thus they must be completed prior to installing REDCap. The institution installing REDCap will store all data captured in REDCap on its own servers. Therefore all project data is stored and hosted there at the local institution, and no project data is ever transmitted at any time by REDCap from that institution to another institution or organization.

REDCap's native webpage encoding and database storage collation is UTF-8, which allows for non-English languages to be utilized in user-defined text that gets stored in REDCap. This includes data entered for a project or the text defined for a survey question or database field label, among many other types of user-defined text. REDCap's database tables implement MySQL's Innodb storage engine, which allows for the use of foreign keys for referential integrity, transactions, and row-level locking (as opposed to table-level locking), all of which are needed in REDCap for consistency, performance, and scalability.

REDCap does not employ any kind of encryption of data (i.e. encryption "at rest") on its database server. (This is not to be confused with encryption of data "in transit" (i.e. via SSL) to the database, which should always be done and must be set up by the partner institution.) The encryption of database data is not necessary if the database server is properly secured. However, some institutions or compliance offices impose requirements such that encryption is required. In those cases, partner institutions are encouraged to seek either filesystem-level encryption solutions or database-level encryption solutions,
sl3(e)a5l(t)yTc 0 1.5-4 8iS1(5)-5(r)8(y)-8(-1S1(5)o8Tw 0.304 0 Td7.587t)-3(ab)2(a.)]TJ0 Tc ver.2(er)1.-wee1(6(5(er)3(l)3(y)9s)2