Resource – Boilerplate Language

Below you will find the current boilerplate language for REDCap across the Enterprise

REDCap General

This initiative will be utilizing the REDCap (Research Electronic Data Capture) platform for data collection and management. Vanderbilt University, with collaboration from a consortium of institutional partners, has developed a software toolset and workflow methodology for electronic collection and management of research and clinical trial data. REDCap data collection projects rely on a thorough study-specific data dictionary defined in an iterative self-documenting process by all members of the research team with planning assistance from the Atrium Health team. The iterative development and testing process results in a well-planned data collection strategy for individual studies. The REDCap system provides a secure, web-based platform for building and managing online surveys and databases that is flexible enough to be used for a variety of types of research, provide an intuitive interface for users to enter data, and have real time validation rules (with automated data type and range checks) at the time of entry. These systems offer easy data manipulation with audit trails and reporting for reporting, monitoring and querying patient records, and an automated export mechanism to common statistical packages (SPSS, SAS, Stata, R/S-Plus). While REDCap can be used to collect virtually any type of data in any environment (including compliance with 21 CFR Part 11, FISMA, HIPAA, and GDPR), it is specifically geared to support online and offline data capture for research studies and operations. REDCap was developed specifically around HIPAA-Security guidelines and is recommended to researchers by both our Research Administration (including the Office of Clinical and Translational Research, Clinical and Translational Sciences Institute, and Institutional Review Board). REDCap has been disseminated for use locally at other institutions and currently supports over 5000 academic/non-profit consortium partners across six continents and over 2 million research end-users worldwide (www.projectredcap.org). It was developed and continues to be supported in part by the National Institutes of Health (NIH/NCATS UL1 TR000445).

REDCap Platform and Server Security

Data for this initiative will be entered into a REDCap database, which uses a MySQL database via a secure web interface with data checks used during data entry to ensure data quality. REDCap includes a complete suite of features to support HIPAA compliance, including a full audit trail, user-based privileges, and integration with the institutional LDAP server. The MySQL database and the web server are both housed on secure virtual servers operated by the Atrium Health's Information Application Systems group (AH-IAS). The virtual servers are hosted in a physically secure location on-site and are backed up nightly, with the backups stored in accordance with the AH-IAS retention schedule of daily, weekly, and monthly tapes retained for 1 month, 3 months, and 6 months, respectively. Weekly backup tapes are stored offsite. The AH-IAS servers provide a stable, secure, well-maintained, and high-capacity data storage environment, and both REDCap and MySQL are widely-used, powerful, reliable, well-supported systems. Access to the initiative's data in REDCap will be restricted to members of the initiative team by username and password and multi-factor authentication (MFA) where required.

REDCap Update and Maintenance

REDCap platforms in the Atrium-Wake Enterprise follow an LTS (Long Term Support) update paradigm. Necessary patch upgrades are performed regularly throughout a calendar year, while larger and more comprehensive upgrades that introduce new features, functionality, and broader system improvements occur 1-2 times per calendar year (roughly every 6 months). All upgrades, regardless of size and scope, are test in development environments first before being committed to any production REDCap platform. They are performed by the REDCap administrative team, and users are notified at least 2 weeks in advance of minor patch upgrades and 30 days in advance of major comprehensive upgrades.

REDCap Surveying

REDCap allows for external data collection (such as PROs, questionnaires, surveys, etc.) via its robust surveying functionality. Data can be collected and submitted by participants directly into REDCap in a compliant and secure manner using REDCap's surveying features, omitting the need for the use of third-party or external services. Additional secure and compliant features include the eConsent Framework which allows for the collection of electronic consent through REDCap, Survey Login options, automated survey invitations, and anonymous survey data collection.

REDCap for Multi-Site Studies

In multi-site studies records can be segmented by group/institution such that users are only able to view/edit the records assigned to their group/institution, known as DAGs (Data Access Groups). Whether serving as a coordinating site or the central data coordinating center (DCC) for a study, both roles can be supported by REDCap in a manner compliant with any study protocol.

REDCap Randomized Clinical Trials

REDCap can provide a secure and compliant environment for data collection and management for a randomized clinical trial (RCT). When properly designed, it can serve as the trial's CTMS, accommodating the randomization of participants, maintaining multiple arms and cohorts, document management, compliant user privileges, and preliminary data analysis throughout all phases of the trial. This allows for all trial data and documentation to be captured, managed, and stored centrally and securely on the Atrium-Wake Enterprise network servers.

REDCap and SMS / Text Messaging

SMS messaging and IVR (interactive voice response) in REDCap utilizes the third-party service, Twilio. All voice calls and SMS messages are routed through Twilio's servers via HIPAA-compliant accounts hosted and managed by Wake Health's internal DCOMM team. In turn, REDCap utilizes several functions to ensure that voice call records and SMS transcriptions do not remain in Twilio's logs but are removed shortly after being completed. This is done to satisfy security and privacy concerns (e.g., HIPAA), in which survey participants' phone numbers and their survey responses do not get permanently logged on Twilio's servers but instead remain securely stored in REDCap.

REDCap for Biorepositories

Accommodating EMR data workflows, bar code tracking, and complex system data management, REDCap can compliantly and securely track and store data and specimens for biorepository purposes.

REDCap for Registries

Accommodating EMR data workflows and system-to-system data management, REDCap can compliantly and securely track and store data for clinical research and patient management registries. Using a strict granular user privilege system, REDCap permits study teams to delegate appropriate levels of access to research data to both internal network and external participating user bases.

Composed DMP with REDCap

The Research Electronic Data Capture (REDCap) system, hosted across the Atrium enterprise, will be used as the web-based data collection and management system for this study. REDCap is a secure, web-based application designed with the flexibility to support data capture for a variety of research projects. It provides:

- a highly granular User Rights management system to appropriately set privileges for all users accessing the project,
- a mechanism for automatically validating and providing additional user review of data uploads from external sources,
- an intuitive user interface for validated data capture through the execution of real-time validation rules, such as univariate data type and range checks,
- an audit trail for tracking transactions within the system, such as study system setup and modifications, data imports, data entry and edits, and data exports, and
- a mechanism for seamless data downloads to common data formats (SAS datasets will be the format of choice for this study).

The Case Report Forms (CRFs) will serve as the basis for the operational and data structure of the REDCap database, which produces a data dictionary with labels for each data field captured and specific validation rules and field metadata associated with each data field as well as a human-readable Codebook and live review of the complete project data structure at any time. Data values that violate these rules are identified at the time of data import or entry and require correction at the entry source before they can be accepted into the database. The REDCap project structure will be designed and built by the Application Specialist or designee and only these individuals can modify the structure. User rights and access to all system data and applications will be assigned and managed by the Application Specialist within the DCC.

All databases and accompanying servers are virtual and maintained on a fully encrypted network. The physical location or the virtual servers are protected in a secured room which is accessible only by a designated security key card. In addition, the secured room is in a secured suite which is also accessible only by security key cards given to Atrium servers' management staff. The building is locked and accessible only by current server management staff.

Non-secure ports of all servers are located behind the DCC network firewall and accessible only under the following conditions: 1) a workstation physically present in the building and physically connected to the network 2) granted system access to the database server 3) a user name and password for that database server 4) a second username and password for database software 5) validation through multifactor authentication 6) granted access to a data project 7) granted access to data items.

All non-essential ports of the database server and web servers are closed. Only one secure (HTTPS) port on the website server is open outside of the firewall.

A network system administrator regularly monitors for occurrences of attempted access to the network by unauthorized users. Automated processes are in place to additionally identify any unwanted access attempts to the system. There is a security administrator for the virtual servers where the application resides and a team of database administrators who monitor and authorize appropriate use of REDCap and the Oracle database servers.