**Data Security - REDCap**

Study data will be collected using the Boston University Medical Campus’ installation of REDCap data collection system, a software tool developed at Vanderbilt University and made available through the Clinical and Translational Science Awards network (CTSAs). To help protect and secure the data stored in REDCap’s database, the software application employs several methods to protect against malicious users who may attempt to identify and exploit any security vulnerabilities in the system. Access to the REDCap data entry website will be based on permissions granted by username and password which will be managed by the Boston University Clinical and Translational Sciences Institute for the Medical Campus Office of Information Technology. Only authorized study members will be able to enter or view data. The login information (username) of the person submitting the information, the date and time submitted, and other navigational information will be automatically obtained and stored in the database.

Boston University’s installation of REDCap is HIPAA compliant. Information posted on forms will be electronically encrypted using secure socket layering (SSL) encryption technology so that only the intended recipient can decode the data. Data will reside on a secure, password protected server at Boston University Medical Center (BUMC) to which only designated individuals have access, thus providing a secure environment for all project data. The database will be automatically backed up on a nightly basis. Files stored on BUMC servers will be protected by electronic ‘firewalls’ that restrict access to designated users. Restrictions and permissions to update the database will be controlled through the REDCap web application.

Because the server will be part of the BUMC network NT domain, only connections from users authenticated from the domain controller are accepted, thus providing a secure environment for all Center data. Specifically, the policy for computer systems security implemented at BUMC:

* Provide physical security of data. All central systems are physically secured behind locked doors with access restricted to key personnel in the OIT. Access through the primary door is also protected by an alarm system that is tied directly into the on-site central emergency response security control center. Written policies exist for contingencies to provide access to the room to those not explicitly authorized.
* Provide virtual security via connectivity. Internal access to all systems is done via Microsoft Challenge Handshake Authentication Protocol. With the exception of internet provider-based services, external client access must first gain access to the internal network before connecting to the systems. This connection is initiated via a Virtual Private Network connection using Point-to-Point Tunneling Protocol or through the University's modem pool which require Kerberos authentication.

All data are protected with disaster recovery via several methods:

* Hardware redundancy: Several stages of redundancy exist at the hardware level to minimize failure: dual-redundant power supplies exist on each disk array; hot-spare disk is configured to automatically self-heal in the event of a disk failure in the array; emergency power generators ensure a 100% electrical uptime; and uninterrupted power supplies present the systems with conditioned steady-state power.
* Data backup: The data are backed up on a regular schedule. All tapes are moved off-site on a daily basis and are stored in a fire-proof safe. Cycle-time of backups is approximately two months with the exception of a yearly archive which is retained for a one-year period.
* Data Security: All data are stored on NT File Systems with password-protected files and directories.

REDCap has been disseminated for use locally at other institutions and currently supports 240+ academic/non-profit consortium partners on six continents and over 26,000 research end-users ([www.project-redcap.org](http://www.project-redcap.org)).