Boilerplate REDCap Language for NIH Data Safety and Monitoring Plans

- What type of physical security is used for the server (e.g., controlled access, secure data networks, service monitoring, environmental management, disaster recovery/business continuity, reliability and scalability)?

The data center in which the REDcap servers are housed has strict access control; only authorized core personnel may access the facility un-escorted. Only authorized users are allowed to connect to the network, and the security of the network is actively monitored. Power and environmental controls have several layers of backups, from interruptible power supplies to alternate and redundant feeds to the local utility company. The REDcap system administrator contributes to the maintenance of institutional disaster recovery and business continuity plans. Load balancers and a highly fault tolerant SAN infrastructure contribute to high availability.

- What type of security is provided for information transmitted/entered (e.g., details of how the data is stored/technical security of server, security of the data in transmission)?

All transactions are securely delivered to the application using SSL (SHA-1 with RSA Encryption; 2048-bits). It is then transmitted internally (behind the firewall) to the database server. All transactions are logged at the server layer (http logging), application layer (REDCap logs activity to a database table), and the database layer (using both query and binary logging).

- How is access managed?

Access to the data is managed by institutionally sponsored login IDs. All personnel must pass an employment background check before being issued an ID. Access to individual REDCap projects (and their data) is managed by the owner of the project.

- What measures are taken regarding password protection (e.g., complexity/construction of passwords, frequency of forced password changes)?

The REDcap system relies upon the institution's identity and access management infrastructure. Password complexity, history and expiration standards are implemented at the institutional level.

- What measures are taken regarding security event monitoring (e.g., monitoring of physical security, monitoring of database and application logs, monitoring of equipment for security events)?

The physical security of the data center is actively monitored 24x7 by security personnel using closed-circuit video. The institution actively logs and monitors all communication to the application server (multiple firewall layers prevent direct external communication to the database server) and the system owner is alerted to any unusual activity. If warranted, the institution will immediately as well as automatically ban offending IP addresses at the perimeter before they reach the application server. The application itself also rejects and bans IP addresses of anything it considers abnormal access.

- Have all other requirements deemed appropriate by the Data Security Officer been met?

Yes