CHEO REDCap Data Management:

The Clinical Research Unit (CRU) will be used as a central location for data processing and management. The CRU will house the data in a dedicated, locked server room within the CHEO Hospital main site, which is secured with 24-hour on-site security guards. The CRU coordinates its network infrastructure and security with CHEO Information Systems (CHEO IS). This provides the CRU with segregated and redundant firewalls and switches, HVAC, malware and anti-virus support, data backup and recovery support, and server hardware and software support within CHEO IS. Network equipment includes two servers connected to redundant gigabit switches. Administrative user authentication to the servers is centralized to CHEO IS Active Directory while the application authentication uses an internal table-based authentication method. Communication over public networks and between the web application is encrypted using secure socket layer (SSL) with 256-bit encryption or higher. Access between the web application and database is protected by a firewall.

Direct access to CHEO computers is only available while physically located inside the facility, or via Citrix remote access. All servers and desktops are scanned for malware and antivirus threats, and our IS staff is notified of alerts. Security is maintained using active directory security. Users are required to change their passwords every 180 days, and workstations time out after 10 minutes of inactivity. All files are protected at group and user levels; database security is handled in a similar manner with group level access to databases, tables, and views in MySQL Server.

The REDCap data collection application will be used for study data management. REDCap, developed by an NIH-funded consortium of institutional partners, provides a secure, web-based application for users to enter data and have real time validation rules (with automated data type and range checks) at the time of entry. The system offers data manipulation with audit trails for reporting, monitoring and querying patient records, and an automated export mechanism to statistical applications. REDCap was developed specifically around HIPAA security guidelines and has a proven track record with over 400 academic clinical research centres hosting the application.

The investigators and CRU staff are fully committed to the security and confidentiality of all research data. All CRU personnel have signed confidentiality agreements concerning all data encountered in the center. Violation of these agreements may result in termination from employment at the CHEO Research Institute. In addition, all personnel involved with CRU data systems have completed GCP training and are governed by CRU standard operating procedures that address data management, privacy and security.