**Boilerplate REDCap Language**

The boilerplate language below is intended as a guide and may be edited as needed for your research protocol. Please be sure to state how you intend to use REDCap (Research Electronic Data Capture) in your IRB approved study documents. Keep in mind that OHSU’s instance of REDCap should be mentioned in your protocol (and other study documents as needed) as the location where you will be storing data for this project.

For all REDCap specific questions, including information about training requirements, and getting help using the software and help setting up your project in REDCap, contact OCTRI Informatics Research Support at octrihlp@ohsu.edu.

**BOILERPLATE REDCap language:**

*Data for this project will be stored in OCTRI's installation of REDCap, a highly secure and robust web-based research data collection and management system.*

*Features of REDCap that protect participants' privacy and data security include:*

*·        Physical Security: OCTRI's REDCap software is housed on servers located in ITG's Advanced Computing Center providing locked physical security*

*·        Electronic Security: The REDCap servers are housed behind both the OHSU firewall and a second ACC firewall.  All web-based data transmissions are encrypted with industry-standard SSL methods.*

*·        Controlled User Access: REDCap is employs a robust multi-level security system that enables researchers to easily implement "minimum necessary" data access for their research staff, including specification of data fields that are identifiers. This feature includes “single click” ability to provide completely deidentified (removing all identified data fields and shifting dates) for analysis or other purposes.  User activities are logged to enable auditing of all data access.   Access is integrated with OHSU's network such that users who are also OHSU employees are authenticated against their OHSU network credentials.*

*·        Data Integrity: REDCap is jointly managed in accordance with OHSU Information Security Directives by ACC staff and members of OCTRI's Biomedical Informatics Program, ensuring fidelity of database configuration and back-ups.  User activities are logged to enable auditing of all data changes.*