METRC Data Management Procedures

All data management activities for the proposed projects are overseen centrally by the staff of the Data Management and Analysis Core and the Computer Support and Informatics Core within the Coordinating Center. Needs for additional programming, database and server management expertise are met by the Johns Hopkins Bloomberg School of Public Health Biostatistics Center.

In general, data are collected on paper Case Report Forms (CRFs) designed specifically for each study. METRC has standard procedures for developing CRFs. In summary, drafts of the case report forms are developed during the protocol development process by the Principal Investigator (PI), the PI at the METRC Coordinating Center, the Project Director and members of the Computer Support and Informatics Core. Core METRC data elements and CRFs serve as the backbone for this process; additional items and instruments are added based on the needs of the specific protocol. CRF drafts are reviewed and approved by the protocol committee and once finalized, formatted according to a standard template. Survey instruments and clinical assessment items are drawn from the METRC core dataset, which serves as the basis for standardized data collection across all studies and is maintained by the Data Standards and Adjudication Committee.

Data are collected in real time on paper CRFs by the study site investigators or the site Research Coordinator. These CRFs serve as source documents for the study. Source documents, including the CRFs and other medical records (e.g., treatment logs of physical therapists and orthotists), are signed by the site PI, other site investigators, or the Research Coordinator. The Research Coordinator, or an MCC-certified staff member working under the supervision of the Research Coordinator, enters the data from the CRFs into the REDCap database described in detail below.

Data Management Using REDCap

The centerpiece of the METRC data management infrastructure is the NIH-funded Research Electronic Data Capture (REDCap) project. (See https://www.project-redcap.org/)The REDCap distributed data entry system was selected among a number of competitors because it is built using a highly customizable and flexible open source design, is publicly available, has a strong and responsive development community, is actively being used by numerous universities and medical centers, and is specifically designed for multicenter clinical studies. The program was built by a team at Vanderbilt University using non-proprietary technologies (PHP + JavaScript and a MySQL database engine), making it highly customizable. The REDCap application runs from secure, dedicated servers located at the Johns Hopkins Bloomberg School of Public Health (see server description, below) and added functionalities have been programmed into the base configuration to support project-specific requirements.

The REDCap data management functionality allows for a web-based distributed data entry system using most web browsers to access an internet-connected database server. The system permits both the METRC Coordinating Center and participating clinical sites to have access to data as soon as they are entered. This allows for near-real-time recruitment reports, detection of data anomalies, and increased data entry availability and convenience for the clinical sites. The primary functions of the data system include the following existing features of the REDCap application: registration of all candidates for the trial; entry of all study data forms; inventory, management, and editing of study data; maintenance of full audit trails of all data entry and

editing; and real time performance report generation. The REDCap data entry system also includes extensive data validation functionalities, such as field level validation, checking the correct format and range of each entered item; intra-form validation, checking for logic errors, skip pattern violations, etc., across items on a form; and inter-form validation (checking for inconsistencies across forms). In addition, using REDCap's flexible open source design, METRC has modified the software to include clinical site management tools such as participant scheduling, serious adverse event and protocol deviation notifications, eligibility adjudication, and notifications for patient enrollment or withdrawal.

REDCap has a number of built-in data import and export capabilities, including the capacity to upload x-rays and photos which are used for eligibility and outcome adjudication, and to directly produce data files for several common statistical analysis and data management packages (Microsoft Excel, SPSS, SAS, R, Stata).

Data Security

Within METRC, data are historically captured on hard-copy case report forms (CRFs) and then entered into REDCap. Sites maintain hard copy documentation, including crosswalks between patient identifiers and study identifiers locally, while de-identified data are uploaded to REDCap, preventing the electronic transfer and storage of protected health information (PHI). Participating centers certify compliance with the following procedures to protect PHI: (1) hard copy documents containing patient identifiers and contact information are stored in secure document containers in accordance with standard document management practices; (2) consent procedures and forms, and the communication, transmission and storage of patient data follow individual site IRB and DoD requirements for compliance with the Health Insurance Portability and Accountability Act (HIPAA); (3) data collection case report forms (CRFs) are maintained according to FDA and ICH guidelines regarding on and off-site storage; (4) paper forms are shredded within five years after study completion; and (5) sites provide the Coordinating Center with a signed verification that these data have been destroyed. All study forms, reports, and electronic records that are part of the study data collection materials will be identified by a unique study ID to maintain patient confidentiality. Clinical information is not released without written permission of the patient, except as necessary for monitoring by the local IRB, the MCC, the DoD, or Medical Monitor. Results of clinical assessments and physical performance tests are shared with study participants at the time of the study follow-up visits. Study results are made public upon completion of all study-related activities and analyses.

Electronic data are collected using the REDCap system, which is accessible by logging into the secure area of the METRC website. Access to the data system is further restricted by an additional level of password protection requiring entry of an "activated" individual PIN ("personal identification number") and unique individual password. Individuals are not granted access to the system until properly trained and certified by the MCC. Each PIN has its own password and staff are trained to recognize the sharing of PINs or passwords as misconduct.

The REDCap Data Access Groups control functionality permits differing levels of system access. Access levels are controlled by the MCC. These include specific permissions to view, edit, and enter data, as well as higher-level permissions to modify table structures, review logs, and assign user privileges. As an example, clinical sites may access, edit, and generate reports

for their site, but cannot access the data entered by other sites. Once data are entered, sites cannot go back and modify data without permission from the MCC.

Detailed change and data entry logs are routinely maintained as part of REDCap. These logs are routinely inspected as part of a Data Quality and Query System, and also serve to identify suspicious activity and provide an audit trail for all data entries and revisions. The change logs make it possible to recover valuable data in the case of malicious or accidental loss.

Dedicated Linux servers for this project are contracted through the ongoing partnership between FireHost Secure Managed Hosting (http://www.FireHost.com) and the Johns Hopkins Biostatistics Center. FireHost provides redundant, HIPAA compliant, dedicated server space. FireHost data centers all have controlled access and physical security (onsite security teams, biometric scanning and video surveillance). FireHost provides operating system upgrades, automatic remote backups, and 24/7 security monitoring and intrusion detection. Daily vulnerability scans and more extensive monthly vulnerability scans are provided automatically by FireHost. Monitoring alerts are immediately forwarded to the MCC, server administrator and FireHost support via email, phone and/or pager.

Based on industry best practices, METRC utilizes a server layout that can parse various types of network traffic and requests, segment server level functions, and maximize security. Server, database, and software configurations are adjusted to enhance overall system security. Appropriate policies, including frequent and regular backups, are established to minimize potential exposure to data loss and ensure research continuity and disaster recovery in the unlikely event of an unforeseen server or software failure. Backup of secure METRC web and database servers is provided by FireHost. Full backups are performed weekly, with incremental backups performed daily. Redundant copies of backups made by FireHost are stored off-site from the data storage facility where METRC servers are located.

Direct access to secure METRC web and database servers is limited a small number of programming staff for development and maintenance purposes. Security is strengthened through strong password policies and two-factor authentication. Password protected, user-level access to all systems residing on secure servers is restricted to individuals certified by the MCC to conduct data collection and data entry for METRC studies.

Requirements for Reporting Sensitive Data

If, during the course of completing the surveys assessing depression (PHQ-9) or PTSD (PCL) via, a participant has a PHQ-9 score indicating major depressive disorder (>=20) or has a PCL score indicating clinically significant PTSD (>=30), the participant will be notified and advised to contact his/her physician or to visit the emergency department.

If on the PHQ-9 item #9, the participant reveals that he/she has thoughts of being better off dead or of hurting him/herself in any way, more often than “not at all,” the coordinator will ask the additional questions of the participant regarding intention for self harm and whether or not a health professional is aware of the participants thoughts. If the participant is under the care of a health professional, the interview proceeds; if not, the interviewer follows a script informing the participant that a clinician (usually the local investigator) will follow up, and urging the participant to call the National Suicide Prevention Hotline or proceed to their local emergency department should they have thoughts of hurting themselves. Once resolved, and if required by

the local IRB, Research Coordinator (RC) document these events as adverse events and report them to the local IRB. While this situation does not constitute a typical adverse event, i.e., one initiated by the study's intervention, the IRB is notified to assist the study team and institution in case of any future legal.