Supplemental Information

1. Data safety monitoring plan
2. Privacy and confidentiality
3. Data management

1. Data Safety and Monitoring Plan

The interventions in the study have minimal risk, but any adverse events will be documented. The PI reviews study conduct such as accrual, drop-outs, protocol deviations on a monthly basis. The PI reviews AEs individually real-time and in aggregate on a weekly basis. The PI reviews serious adverse events (SAEs) in real-time. The PI ensures all protocol deviations, AEs, and SAEs are reported to the IRB according to the applicable regulatory requirements.

An internal data quality inspection will be performed. The PI will do a random 10% data audit 1-2x/year. If necessary, re-training of data collectors will be conducted.

2. Privacy and Confidentiality

All study forms including consents, HIPAAs, and case report forms (CRFs), which will include elements from the present and past history, patient demographics, including age, current medications and lab draws, will be stored in in a locked cabinet in Dr. Taub's office in the ACTRI building. Only approved study personnel will have access to this information. To minimize the potential loss of confidentiality, patients will be assigned a unique number as their subject identifier code. The unique subject code will be used to label all study documents.

3. Data management

Data will be collected using standardized paper forms and will be identified with the study's ID of the participant. The codes that link the name of the participant and the study ID will be kept confidential by the Principal Investigator in a secured cabinet. Data will be entered in the computer independently by UCSD certificated and trained data entry staff, and discrepancies corrected by a supervisor based on source documents.

Specimens: Some portions of the specimens collected may be sent to a central laboratory outside of UCSD for testing. All samples will be labeled with a unique specimen code and the only way to link the specimens with the subject code and any personal health identifiers will be on a physical sheet of paper locked in a cabinet in Dr. Taub's office in the ACTRI building.

mCC app data: The mCC app is designed uses HIPAA compliant Amazon Web Server (AWS) for server-side operations. Two large capacity Linux servers (main server and backup) with load balancing are used to capture the data that the smartphone users transmit. The data will be stored on AWS S3 (Simple Storage Service). These two servers will remain online 24h a day, 7 days a week.