MyCap Security Overview

Terms

- *App*: MyCap mobile app (iOS or Android)
- *Module*: MyCap external module for REDCap
- *Participant*: Person using the *App*

Secure Data Transmission

SSL/HTTPS + HMAC

All data in the *app* that is downloaded from or uploaded to a REDCap server is transmitted using the *module* API. Data transmitted to/from the *app* is done using a secure, encrypted transmission (SSL/HTTPS). For increased security, the app additionally uses a hash-based message authentication code (HMAC-SHA246) to verify the integrity of the data and to authenticate the sender. Each *app* request to the *module* is valid for 15 minutes after which it will expire and be discarded.

Secure Data Storage

Encryption

The *app* employs AES-256+SHA2 encryption-at-rest on the mobile device's hard drive so that all *app* and *participant* data on the device is properly protected from unauthorized or malicious users. Encrypting the data on the device prevents any unauthorized users from accessing data in the app, even if they were to gain access to the device's file system in some way (whether using a direct hardware connection or via other software on the device). Encryption keys are stored in iOS's Keychain and Android's KeyStore, which is standard practice for achieving the highest level of security for encrypted data stored in iOS and Android.

Project Data Isolation

Participants may participate in multiple MyCap-enabled projects on a single device. Project data is isolated. Thus, project "A" and project "B" data cannot be intermingled.

Data Retention

Participants complete tasks and results are stored in the project's encrypted database on the device. Results are transmitted immediately to the REDCap server if an internet connection is

available. Once transmitted, results in the project's encrypted database are erased. Note that some types of tasks allow the *participant* to see his or her results. In this case results are not erased after transmission. If an internet connection is not available then results will remain on the device until transmission is possible. A synchronization attempt is made every time a *participant* completes a task.