Security in the REDCap Mobile App

Secure Data Transmission

SSL/HTTPS: All data in the REDCap Mobile App that is downloaded from or uploaded to a REDCap server is transmitted using the REDCap API, which is a RESTful web service API. Therefore, as with all REDCap API requests, data transmitted to/from the app is done using a secure, encrypted transmission (SSL/HTTPS). For increased security, the app additionally verifies the SSL certificate of the REDCap server that it is communicating with in order to validate the server's identity. By verifying the SSL certificate of the REDCap server, this precludes the possibility of a so-called "Man in the Middle" attack during data transfer. If the REDCap server does not have a signed certificate from a Certificate Authority (CA) – either it is not using SSL or instead has a self-signed SSL certificate - then a warning popup will appear to the user in the REDCap Mobile App whenever sending data to/from the REDCap server. This will ultimately not prevent the user from proceeding with an insecure data download/upload, but it will strongly encourage them to wait and try to find a safer connection at a later time before proceeding. Note: Users connecting to a REDCap server with a self-signed SSL certificate will receive this warning every time.

Secure Data Storage

Encryption: The REDCap Mobile App employs encryption-at-rest on the mobile device's hard drive so that all important data and information stored on the device is properly protected from unauthorized or malicious users. Encrypting the REDCap 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). All user PINs are ciphered using SHA cryptography, and all stored REDCap data values (potential PHI or PII), API tokens, and REDCap app logs are encrypted using AES encryption standard on the mobile device's hard drive. The 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. Note about external/detachable drives: The REDCap Mobile App does not allow any data to be stored on external hard drives (e.g., USB Flash drives) connected to the mobile device. To maintain the greatest level of security, the app only allows the device's internal hard drive to be used for data storage.

Built-in Safeguards to Prevent Unauthorized Access

Username and PIN: Each user on the REDCap Mobile App has a username and four-digit PIN that is used to authenticate the user before accessing their REDCap projects and data in the app. User PINs are ciphered using SHA cryptography and stored in the app's local database on the mobile device. For additional security purposes, the app only allows five login attempts within a fifteen minute window (across all users), after which the user gets temporarily locked out. This severely restricts any unauthorized user from gaining access to someone's account in the app.

Remote Lockout: In certain situations it may be necessary to remotely lock out a person so that they cannot (or no longer) access the data stored in the app or to prevent them from downloading or uploading data to the REDCap server from the app. Such situations would assume that 1) they have direct physical access to the mobile device, and 2) they know the PIN for accessing a user's account on the app. If this occurs, the person whose REDCap account is connected to the device will need to go to the REDCap server to have their API token revoked for each project that has been initialized in the app. This can be done by the users themselves on the REDCap Mobile App page in the project (on the REDCap server). Once their API token has been deleted or regenerated, the person with unauthorized access to the app will no longer be able to download data from or upload data to the REDCap server for that project in the app. Furthermore, if the app is "online" (detects that it has WiFi or cellular connectivity), then the app will check if the API token for the project is still valid. And if not, it will additionally prevent the unauthorized user from even accessing the project in the app, thus preventing them from viewing or accessing the REDCap data currently stored in the app. In this way, the remote lockout feature provides yet another way for users to protect their data, both on the REDCap server and in the app.