REDCap Mobile App Best Practice Recommendations

Devices

- Device must be protected by a password lock/pin, available to REDCap Mobile App users only.
- Device usage should be restricted to data collection through the REDCap Mobile App, and not for personal use.
- On iPads, disable 'iCloud Drive' and 'Backup' under the iCloud settings.
- Microsoft Office applications (Word, Excel,…) should not be used on devices to read, edit, or store clinical or study data because the files are automatically stored on the Microsoft OneDrive cloud, located in the United States.
- In accordance with UBC & PHSA IT Policies for devices storing critical data, devices will be protected with whole-device encryption.
- If a device has failed such that the REDCap app can no longer be opened in order to dispose of data, the device will be remotely wiped, if possible, or the device will be destroyed, using institutional services for device destruction, if available.
- If destroying a device would void a desired warranty, the manufacturer of the device will be contacted to request that the device is destroyed after being returned or exchanged.
- Mobile Device Upgrade: Please check with REDCap support team before upgrading the operating system of your mobile device to ensure compatibility with the REDCap App.
- If your device is lost or stolen, or if your credentials or API token have been compromised, please contact REDCap support team immediately at ***redcap@cfri.ca*** or call ***604-875-2000 ext.: 4888 or 3477***.

REDCap Mobile App

- Don't reveal your REDCap credentials (PINs or passwords) and API token to any third party.
- Send data from device to server as often as possible when device is connected to internet.
- Erase data from device as soon as data is successfully transferred to server.
- Send the mobile device logs to REDCap server every 24 hours when possible.
- If you make changes to the project structure (Creating new forms/Events, adding new fields) in main Redcap project, reset the project on the Mobile App to reflect the changes.
- Always upgrade your REDCap App on mobile device to the latest version; CFRI REDCap Support Team will you send you a notification whenever new versions are available in any App store.
- When asking participants to self-enter data, the "Secure Instrument" feature of the REDCap mobile app will be used so that participants cannot see other data.
- When a user stops being associated with a project or when a device is disposed of in any way (sold, given, returned, exchanged), all REDCap data will be cleared from the device and the user's API token will be deleted from the REDCap project.
- Problems with the REDCap Mobile app should be reported to CFRI Data Management (redcap@cfri.ca).
- For more information about the App, please refer to the CFRI DM REDCap Mobile App Manual, the FAQ section in the App, or the following link: http://projectredcap.org/app/faq.pdf

Security and Privacy Policies

Below are the PHSA and UBC IT Polices will be followed with using the mobile app to collect data.

PHSA IT Polices:
http://pod/policies/Information%20ManagementInformation%20Technology/Forms/public.aspx

UBC IT Polices:
UBC Policy- Securing Computing and Mobile Storage Devices/Media

UBC Policy- Encryption Requirements