CFRI REDCap Mobile App Request

Please complete the following survey to the best of your ability. Details in this survey will assist the CRSU team to understand your project and approve the project's eligibility.

The REDCap Mobile App is a data collection tool that allows users to collect data without internet on a mobile device and to synchronizes data with an active project on the CFRI REDCap server.

The REDCap mobile app uses API (Application Programmer Interface) tokens to allow an existing REDCap project to be copied from the server onto the mobile device.

Please provide the information below regarding the device(s) and the CFRI REDCap project you would like to use with the Mobile App.

For information on how the REDCap Mobile App works, how best to use it and relevant defintions, please refer to the CFRI REDCap Mobile App Manual

Username _____
(@DISABLED)

Device Information

What type of mobile device will you use?

- ☐ Mobile phone
- ☐ Tablet
- ☐ Desktop computer

Which operating system will you use for your device?

- ☐ iOS
- ☐ Android

How many devices will you use? _____

How many users will use the app? _____

Who will be responsible for maintaining the device(s)?

- ☐ Project Administrator
- ☐ Other (PI, Research Assistant...)

Ex. Updating the app and device software, keeping track of the device...

If other, please provide the name, email, and phone number.

_____

Mobile App Project Details

Please describe how the mobile app will be used.

Why is the mobile app necessary or desired compared to using a web browser on a mobile device?

- ☐ Lack of reliable internet access
- ☐ Want to save money on cell-based Internet access
- ☐ Prefer mobile app interface
- ☐ Other

If other, please describe

The following criteria are concerned with managing the data collection device and the individual API tokens granted to users.

Please contact redcap@cfri.ca with any questions.

By submitting this request, you agree to follow the practices listed below:

The device will be protected by a password/pin, available to REDCap Mobile users only.
◯ Yes
◯ No

The device will be used solely for data collection and not for personal use.

◯ Yes ◯ No

Each user of the mobile app will use their own API token to access REDCap.

The API tokens used by the mobile app to authenticate to REDCap will not be shared with anyone nor stored anywhere besides in REDCap and in the mobile app.

◯ Yes ◯ No

Users will not share accounts in the mobile app and/or share the password for their mobile app account.

◯ Yes ◯ No

The QR code (or alternative code) used by the mobile app to transfer the API token from REDCap to the mobile app will not be copied or shared in any way, except by the QR reader in the mobile app.

◯ Yes ◯ No

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.

◯ Yes ◯ No

Each user of the mobile app will be trained to protect their API token, to protect their QR code, to use only their own app account, to use the Secure Instrument feature when allowing patients to self enter data, and to follow any further institutional and/or department guidelines on protecting the security and privacy of data on mobile devices.

◯ Yes ◯ No

The following criteria is concerned with security and privacy on the device. PHSA and UBC policies require certain security measures be taken with the device, such as technical updates, encryption, and API token management.

A device can either be supported by CFRI IT or by the Project Administrator. If the Project Administrator decides to support the device, they are responsible to adhere to and implement the security measures. Please contact redcap@cfri.ca for more information, or if you have any questions.

By submitting this request, you attest to the following criteria:

Mobile device security will be managed and maintained by the CFRI IT Team

◯ Yes ◯ No

If you have already submitted a ticket to the CFRI IT team to request Device Management, please provide your CFRI IT ticket number: _____

If not, please submit a ticket at https://support.cfri.ca/sdp/r3/services.php.

The maintainers of the devices have read and will abide by the mobile IT Policies for UBC and PHSA listed below.

◯ Yes ◯ No

UBC IT Policies

[Attachment: "Std 07 Securing Computing and Mobile Storage Devices or Media.pdf"]

[Attachment: "Std 05 Encryption Requirements.pdf"]

PHSA IT policies

Click Here (internal link - contact redcap@cfri.ca if you cannot access this link)

In accordance with UBC & PHSA IT Policies for devices storing critical data, devices will be protected with whole-device encryption.

◯ Yes ◯ No

In accordance with UBC & PHSA IT Policies for devices storing critical data, backups are not allowed to use cloud services, such as iCloud, so backups will be turned off or directed at institutional services.

◯ Yes ◯ No

Microsoft Office applications (Word, Excel,..) will not be used on devices to read, edit, or store clinical or study data because files are automatically stored on the Microsoft OneDrive cloud, located in the United States.

◯ Yes ◯ No

All security incidents involving the mobile device will be communicated to CFRI Data Management Team (redcap@cfri.ca).

This includes compromised, unsecured, lost and/or stolen devices, API tokens, and QR codes.

◯ Yes ◯ No

Technical problems with devices will be escalated to CFRI IT (https://support.cfri.ca/sdp/r3/services.php). Problems with the REDCap Mobile app will be escalated to CFRI Data Management Team (redcap@cfri.ca).

◯ Yes ◯ No

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.

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.

◯ Yes ◯ No