

Mobile App Request

Please complete the survey below to request use of the REDCap Mobile App. Please contact fom.redcap@ubc.ca if you have any questions.

The REDCap Mobile App is a data collection tool that allows users to collect data without the internet on a mobile device and to synchronize data with an active project on the Faculty of Medicine (FoM) 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 FoM 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 definitions, please refer to the REDCap Mobile App Manual, attached.

[Attachment: "Vanderbilt REDCap Mobile App Manual 1.1.pdf"]

For best practice guidelines and the Data Management team recommendations, please see the Mobile App Best Practice Guidelines, attached.

[Attachment: "FoM DM REDCap Mobile App Best Practice Guidelines.pdf"]

Requester Name

Requester Email Address

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

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

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.fom@ubc.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 App 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 research team is responsible for maintaining their mobile devices. Maintainers of the devices have read and will abide by the mobile IT Policies for UBC 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"]

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

Yes No

In accordance with UBC 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

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