REDCap

Research Electronic Data Capture

Mobile App User's Guide

INTRODUCTION

About the App

REDCap software provides its online users with the ability to create and manage surveys and databases quickly and securely to facilitate data collection. The REDCap Mobile App adds a new dimension to the software's versatility by providing users with a tool for **offline data collection**, particularly in environments with poor internet connectivity. REDCap users can now collect their REDCap data in a mobile app on an iPhone, iPad, or Android phone or tablet. With REDCap and the REDCap Mobile App, users have new options for electronic data capture for studies that under previous circumstances would have dictated pen and paper**. The app cannot be used on its own but is a companion app that must be used alongside REDCap itself. All users of the app must already be a REDCap user before using the app.** To activate the Mobile App in your project, there is a **$1,000 fee (per project)**. User support for the Mobile App is **$85/hour**. The $1,000 fee will be billed to the PI before activation of the App.

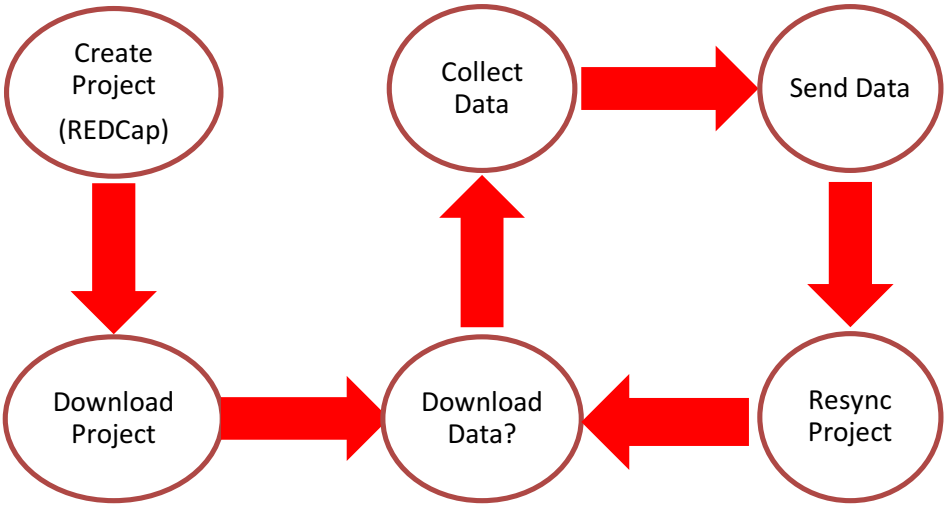
App Videos

Click on the following video links for an app overview and installation and setup instructions.

- REDCap Mobile App – Overview
- REDCap Mobile App – Installation & Setup

App Workflow

The REDCap mobile app is an app that can be installed on a tablet or mobile device so that data may then be collected in an offline fashion on that device, after which it may then be synced back to this project on the REDCap server. The app is most useful when data collection will be performed where there is **no internet service** (e.g., no Wi-Fi or cellular service) or where there is unreliable internet service. Once a user in the project is given 'REDCap Mobile App' privileges, they can navigate to the mobile app page on the project's left-hand menu and set up the project inside the mobile app on their device. Once the mobile project is set up on the device, the user can collect data (which is stored locally on the device), and then at some point sync that data back to this project on the REDCap server.



App Concept

These are the steps for a high level view of how the Mobile App works:

1. **Create** and design project on your REDCap installation.
2. **Contact** the REDCap Team to activate the Mobile App and get token. **Note: There is a $1000 turn-on fee per project. User support is $85/hour.**
3. **Set Up** project. While online, set up the project on the app using a code provided in REDCap.
4. **Collect** data from participants. This can be done offline, or online (if internet access becomes available).
5. **Send** affected data to the REDCap server securely. New records are sent as a package; modified records have their values adjudicated against existing server values. The app user will then be given a chance to refresh the project. This step must be done online.
6. **View and Analyze** data. Once the data is uploaded to REDCap, it is a living part of the project.

REDCap vs. the App

You DO NOT need to use the Mobile App to enter data into REDCap from a device. If you have an internet connection, you can simply use a browser to collect data through surveys or data entry forms.

The two options for collecting data from a device are compared below:

REDCap Online Browser	REDCap Mobile App
Use if there is a reliable and secure and internet connection	Use if there is no, or an unreliable, internet connection
Data is directly entered into the REDCap project once a form is saved on the device. No data is stored on the device.	Data is saved on the device once a form is saved, and will not be entered in the main REDCap project until data is synced (via an internet connection).
Data is always up-to-date in the REDCap project.	Data might be out of sync if the data stored on the device is not regularly synced to the main REDCap project.
No additional security measures required on the device.	Further security measures must be taken to ensure data security.
The REDCap interface is exactly the same as it is on desktop.	The interface is adjusted to fit uniquely for a mobile device, and looks slightly different.
User accounts and rights set in REDCap are applicable.	Separate user accounts and user rights are needed to be created in the App and API tokens are required to link back to user accounts in the main REDCap project.

Downloading a Project

New project creation is not possible in the REDCap Mobile App itself. The app's purpose is to collect data offline that will later be added to an existing project in the web based REDCap application. In order to do so, a copy of the project's data collection instruments must be reconfigured in the REDCap Mobile App.

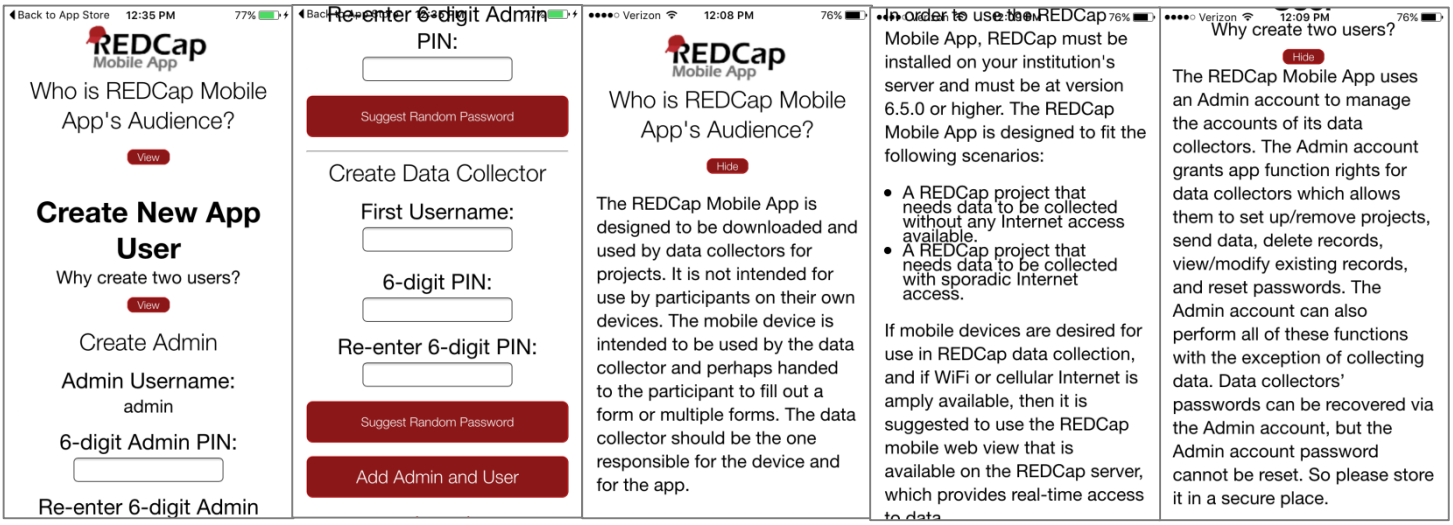
APP USERS

Admin Interface

With the specially-created password, the admin user can log in. This will result in accessing a special interface that enables the admin to do just about everything in the app but collect data. This allows projects the ability to separate data collection from app administration through user rights management. Or if full access is desired for users, then full rights can be given, and the admin interface need not be used - which is the default.

An admin can add users and customize user rights. User passwords can be reset here. When a user is created, full rights are automatically given. The admin (and only the admin) can revoke rights. If all rights are revoked, the user can only collect data for new records. This allows a sort of user management for projects depending on the trust and the ability of the data collector.

Projects can be managed by the admin interface for each user. One can set up a mobile app project. One can also send any data for a project. Data can be dumped to the Mobile App File Repository on REDCap, logs can be sent, and projects can be refreshed. Everything but data collection is possible through this interface.



User Responsibilities

REDCap Project Creator:

- Create and design the REDCap project.
- Grant mobile rights access to the appropriate REDCap users.

REDCap User:

- Create a token for the project so that it can be distributed to the App User.
- Coordinate data reception from the app(s). No action is required other than monitoring the project.

App (Device) User:

- Download the project onto the app.

- Collect data on the app.
- Send data from the app to the server at an appropriate time.
- Keep the project up-to-date by reinitializing the project after data is sent.

User Management

You can add multiple users to the device in the Add & Manage Users section. Each user will have a unique PIN that you assign to provide access. Each app user, however, maintains unique project copies on the device and cannot share the same REDCap Mobile App projects. An app user downloads the main project from a REDCap user on the server with the opportunity to download all data that has been entered or uploaded. This app user collects data separately from anyone else (i.e., the data is siloed to each app user and then again, to each REDCap Mobile App project). When the app user sends data to the server, the process handles duplicate record ID's and conflicting data, and conflicts are presented to the app user. (This is described in the Sending Data section.) After the data is sent, the REDCap user can view the data.

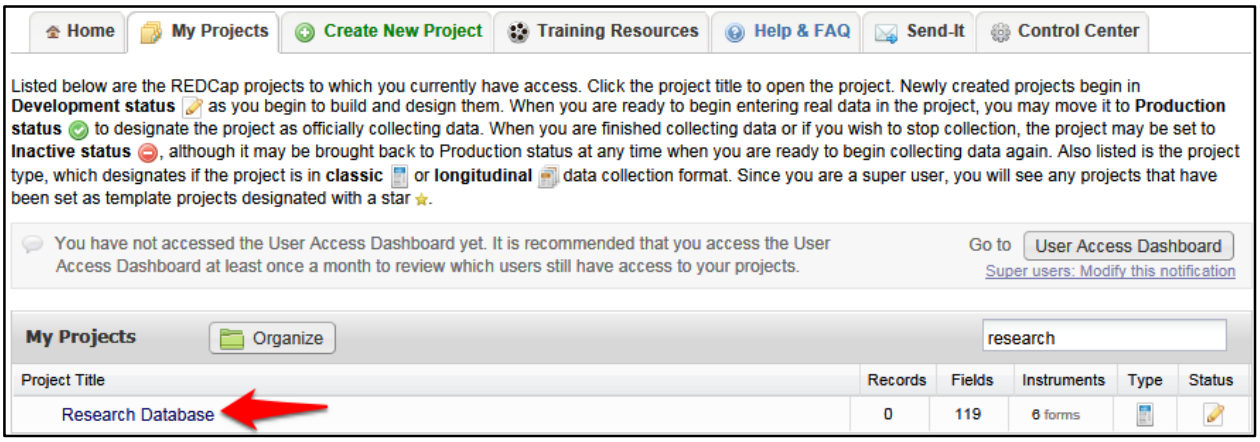
User Rights

It is important to note that the user privileges inside the REDCap Mobile App mimic a user's privileges in the project on the REDCap server with regard to data collection. For instance, if a user has 'No Access' Data Entry Rights for a specific data collection instrument, then the user will also not have access to that instrument in the app. There is an additional user privilege associated with the app that allows you to choose whether or not the user is able to download data (i.e., records in this project) to the mobile app on their device. For example, you may choose not to allow them to download record data to the app if this project contains very sensitive data (e.g., PHI).

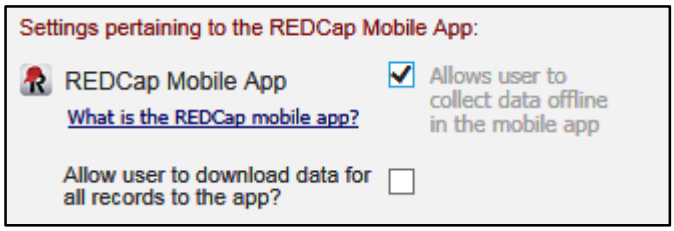
USING THE APP

Getting Started

1. **Log into REDCap** and select your correlating project from your "My Projects" page.



2. **Contact the REDCap Team to turn on the Mobile App and grant mobile apps user rights**. Locate the Applications features on the left sidebar. Choose the User Rights application and add REDCap Mobile App rights for yourself or another appropriate user. By rule, you will now be able to download the full data set and request an API token regardless of previous permissions levels.



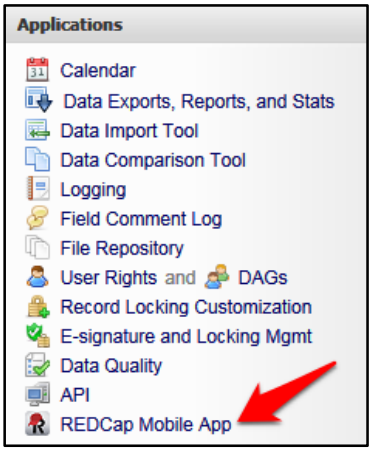
The 'REDCap Mobile App' user right allows users to:

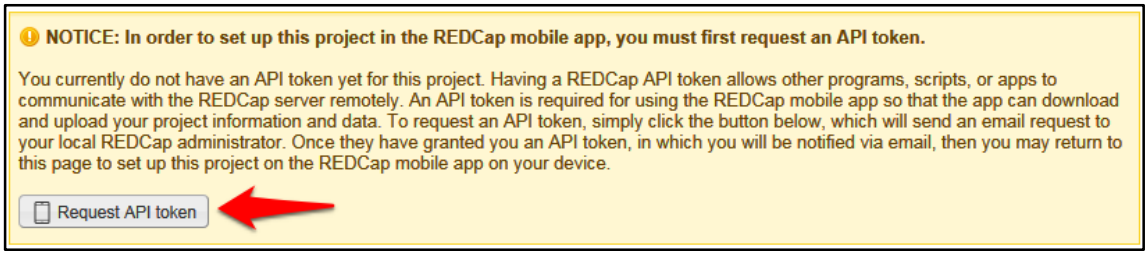
- Set up the project inside the Mobile App on your device.
- Collect data which is stored locally on the device.
- Sync that data back to this project on the REDCap server.
- The REDCap Mobile App section is where users can view the App log and file archive.

The 'Allow user to download data for all records to the app?' user right allows users to:

- Download records from the server to the app.
- Unchecking this privilege prevents users from unwittingly (or wittingly) downloading lots of sensitive data to their mobile device.
- If a user is given this privilege, then when they initialize the project in the App and the project contains at least one record, then the App will prompt the user to choose if they wish to download all the records to the App or not.

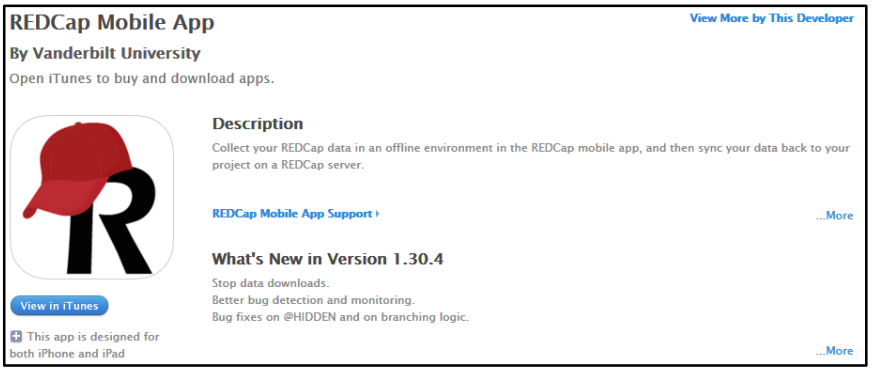
3. **Request token and get app access code**. Click the REDCap Mobile App link on the sidebar and request an API token. Once the token is created, return to that page (or refresh the page). A QR code is now available under the Initialize Project in Mobile App tab. If you have trouble with the QR code, click the "Can't get the QR code to work?" link to access a 10-character access code that can be entered manually.



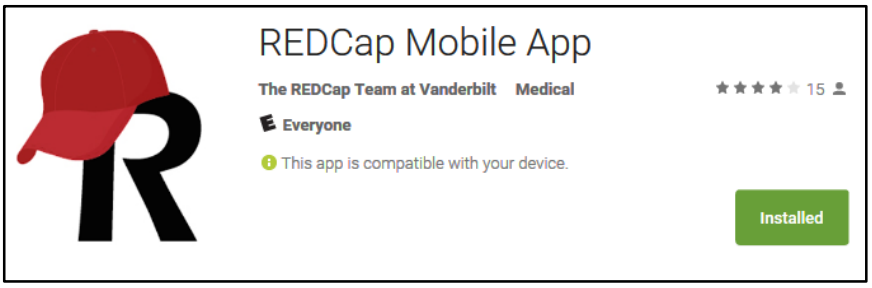


4. **Download and open the app on your device**. Download the Mobile App on your iOS or Android device by searching the App Store or Google Play Store for 'REDCap' on your mobile device to find the app there to download. The app is available for the following platforms: iOS 6.0 or later (iPhone 4 and up, iPad 2 and up) and Android 4.3 or later (phones and tablets). Below are the links for downloading the app from the Apple App Store or from the Google Play Store (depending on what type of mobile device you have).

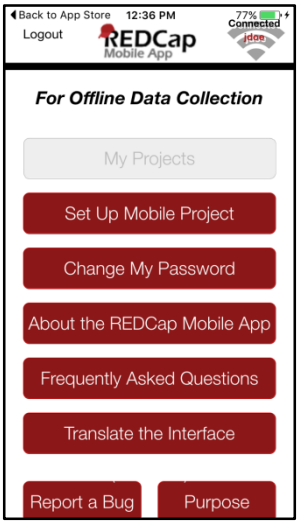
iOS app on App Store:
https://itunes.apple.com/us/app/redcap-mobile-app/id972760478



Android app on Google Play:
https://play.google.com/store/apps/details?id=edu.vanderbilt.redcap

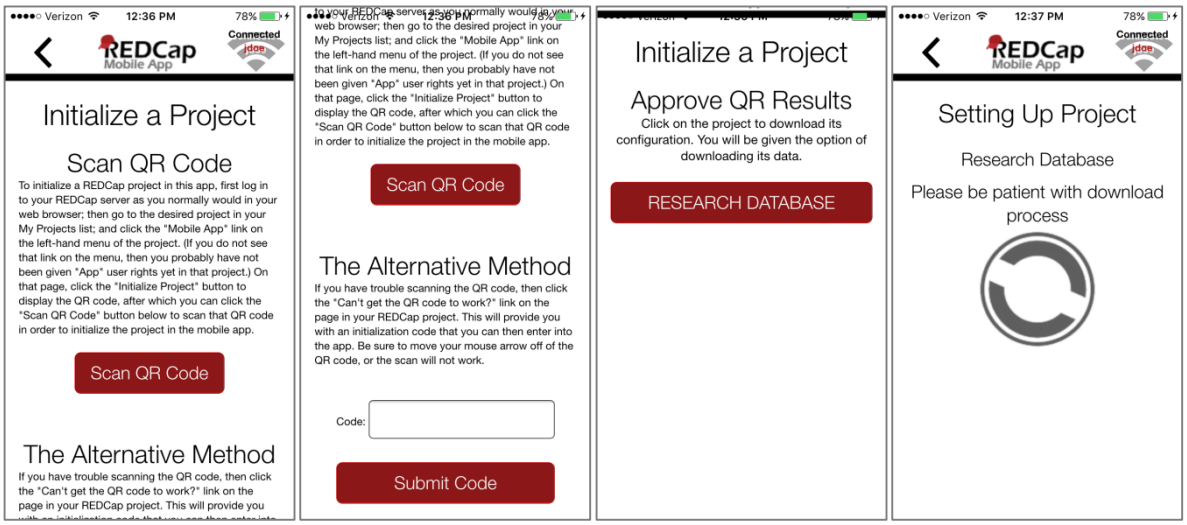


5. **Set up the project**. Click the 'Set Up Mobile Project' button.



Optionally downloading data: In addition to the data collection instruments, you can choose whether you want to download data from the project or not. This process happens while online immediately after adding or resynchronizing the mobile project. When resynchronizing a mobile project on the REDCap Mobile App, all existing data for that project on the app will be deleted. (This will not affect any other projects that you have added in the app.)

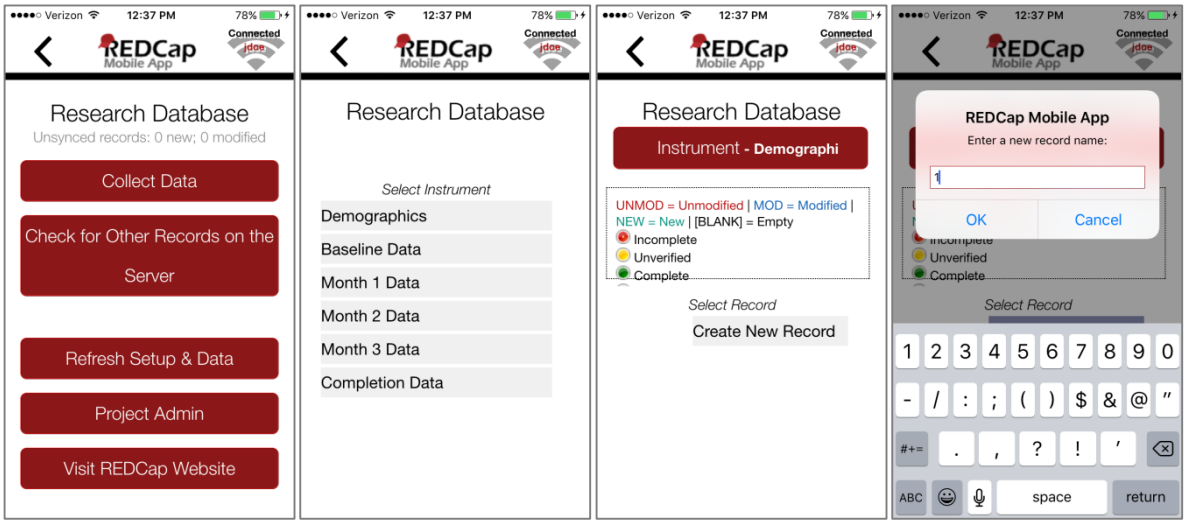
6. **Provide the code**. Click the Scan QR Code and Initialize button. Scan the QR code that you see displayed or enter the 10-character access code here. If correct, either will grant you access to the project which has now been replicated on your device for offline data collection.

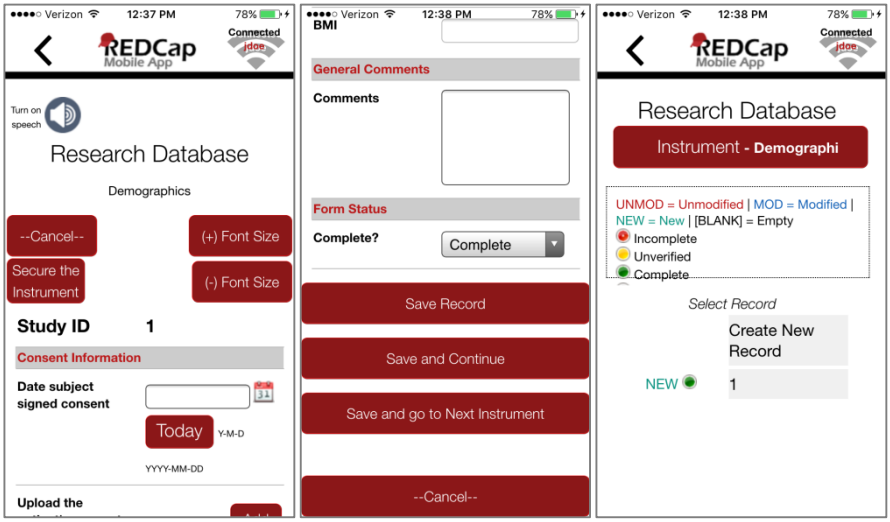


Data Collection

With the project in place, you can begin data collection for both new and existing records.

- Tap the Collect Data button and choose an instrument and a record. (This selection order is slightly different for classical projects, one-armed longitudinal projects, and multi-armed longitudinal projects.)
- If this is a new record, you must choose the first instrument. If this is a new record on a project without auto-numbering enabled, you will also have to choose a record name.
- Enter data and set the form status at the bottom as needed.
- Save your data in one of three ways:
  - Save Record (to save data entered and return to the records list)
  - Save and Continue (to save data entered and remain on the same screen)
  - Save and go to Next Instrument (to save data entered and move on to the next instrument in sequence)





Data collection features:

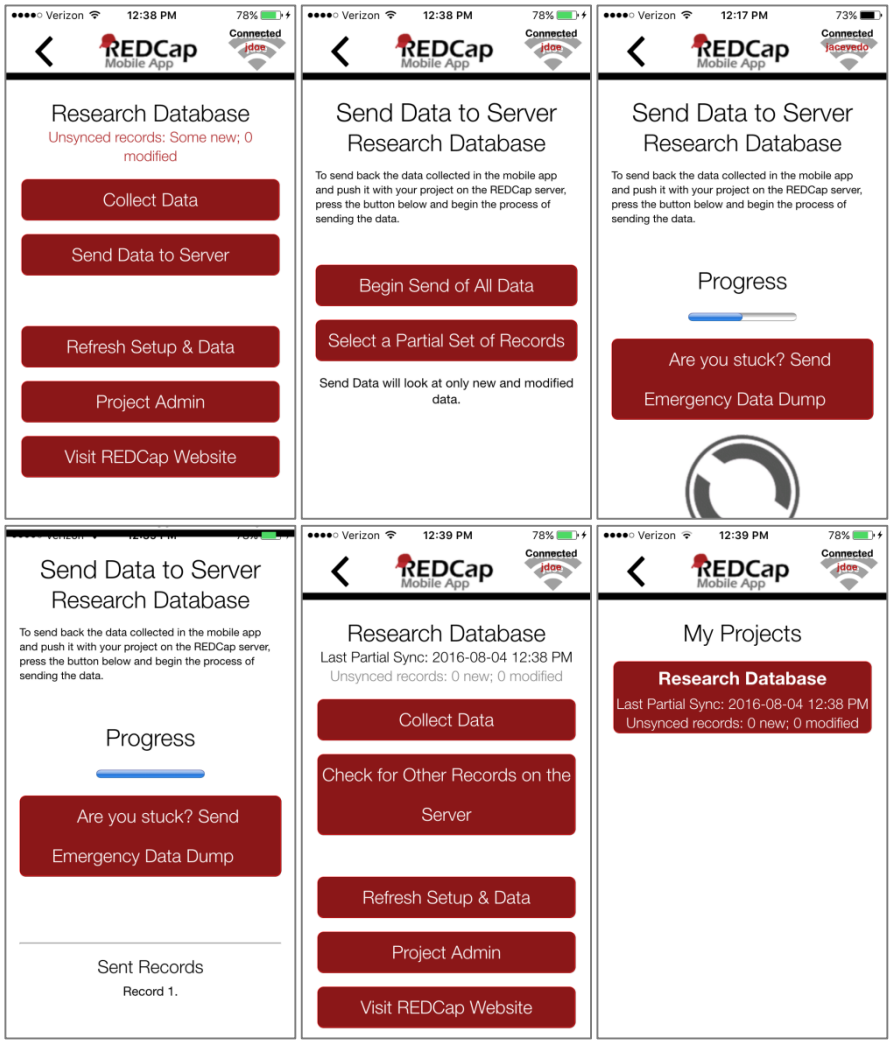
- Besides free text and structured data entry, pictures, videos, and audio can be uploaded into designated file fields. Signatures can be captured as well.
- Records can be renamed on the first form. Note that renamed records will appear as new records when uploaded to the main database, so you will need to delete the original record there to complete the replacement process.
- Instruments can be secured so that participants/users will only have the option of entering data (and not traversing the rest of the app, which can jeopardize confidentiality). They can be unlocked via the primary user's pin.
- The amount of data collection is only restricted by what your device's hard drive will allow.
- All data collection can be offline – without Internet access.

Sending Data

When back online, you can send data to the project's REDCap server. This will coordinate the mobile device's data with the main REDCap project. If record names or data values conflict, you will be given the opportunity to make adjustments before completing the upload. If the instruments themselves have been modified

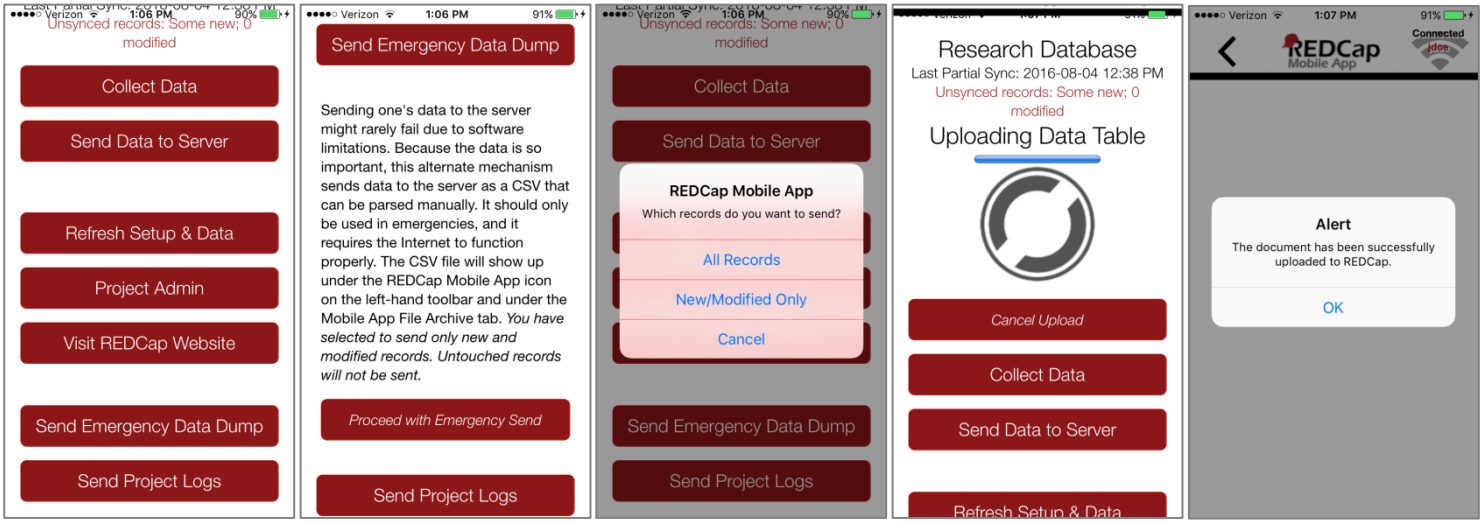
significantly in the main REDCap project since REDCap Mobile App project setup, you will not be able to complete the upload.

- In the app, click on Send Data to Server.
- Click the Begin Send button.
- New records will be added to the main REDCap project immediately if no conflicts exist or if conflicts exist but are automatically resolved by the app.
  - If there are no duplicate record names/numbers, records will upload with the names/numbers assigned at the app.
  - If auto-numbering is enabled and there is a record name conflict, REDCap will automatically update the record numbers to the next numerical series of numbers before uploading and provide details on the app page.
  - If auto-numbering is not enabled, a new ID number is suggested but can be modified unless its name conflicts with a new record on the server.
- Existing records that have been modified on the app will have modifications detailed on the app page.
  - An option to send the data to the server for each modified record appears, as well as the opportunity to view details of the differences between server data and app data for that record. Individual field values can be selected from the details (i.e., server vs. mobile device).
  - Each record that has been modified is usually auto-filled with a "Yes" response to the "Send data to the server?" question. If after reviewing the scheduled changes for that record, you decide not to make the update, change the response to "No" to remove it from the upload queue.
  - To choose field-level changes, click on the cells that have the information you want to enter for the record. You can choose from either the app side or the server side of the table.
  - Special scenarios to note:
    - If a record is deleted from the main project after it has been replicated in the app and a change was not made to the app record, the record will not upload from the app to the project as a replacement. You will not receive a notification from the app or server that the original record has been deleted.
    - If a record is deleted from the main project after it has been replicated in the app and a change was made to the app record, you will receive a notification and option to change the ID number and upload as a new record, or not to upload the record at all.
    - If a record is deleted from the app, it will not be deleted from the server after data syncing. You may only delete records from the main project on the server.
    - For cases where auto-numbering is disabled, if a new record was entered on the server with the same ID as a new record entered on the app, you are given the options to merge the data, to upload the app data with a new ID, or not to upload the data.
    - Click Send Records with Changes to complete data upload when ready.
    - Click Clean & Reset Mobile Project (recommended) to remove old mobile data and replace with the most current project information from the main REDCap project, or choose Back to Project to continue working with the same data. If you choose Back to Project, uploaded data will no longer be marked as new or modified; that is, it will no longer be queued for upload.

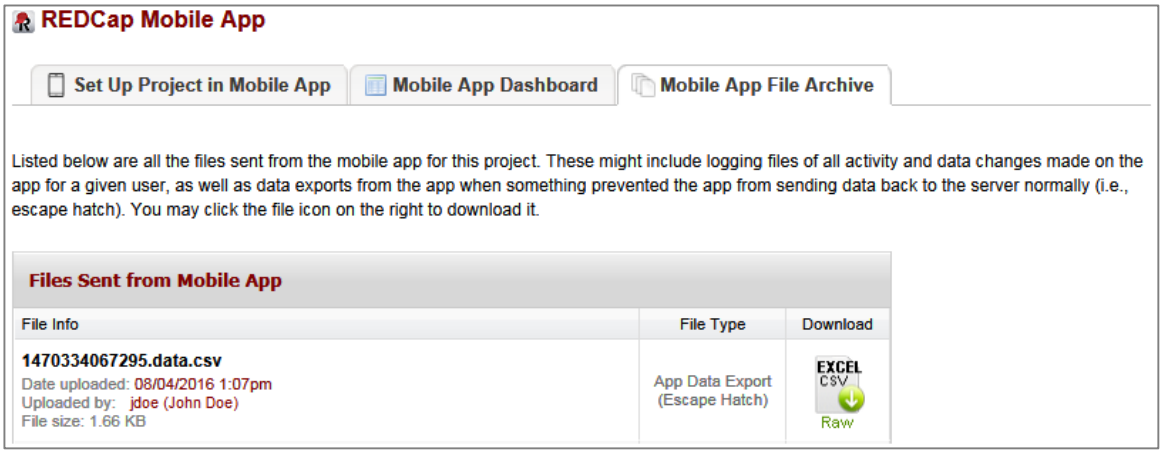


Emergency Data Dump

When something prevents the app from sending data back to the server normally, use the "Send Emergency Data Dump" option to send data to the server as a CSV file.

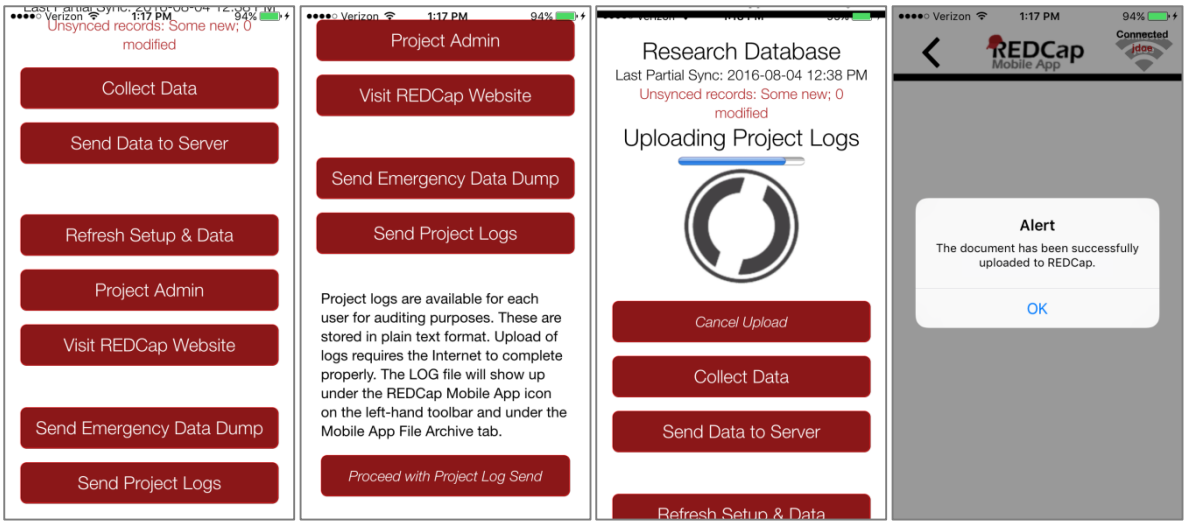


The file will show up under Mobile App File Archive tab, ready for import.

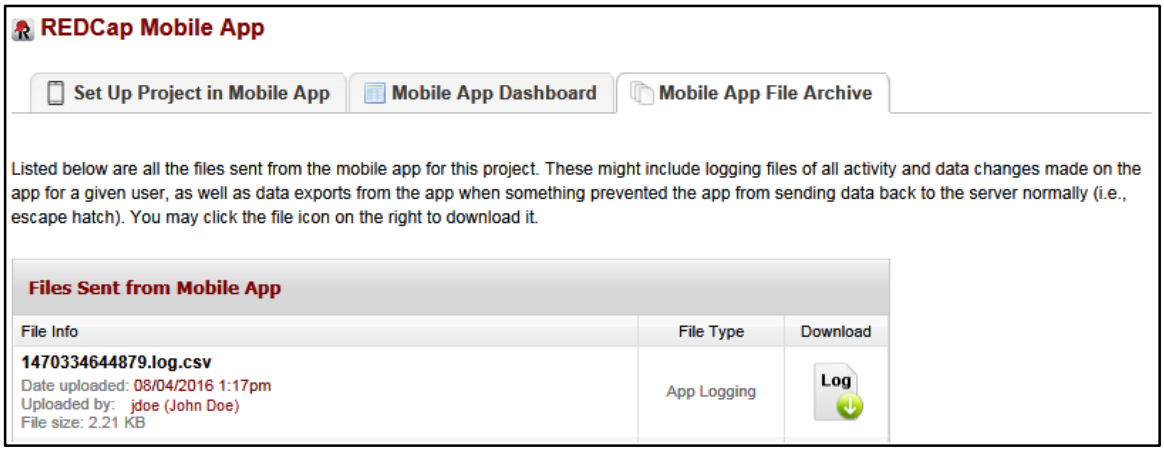


Activity Logs

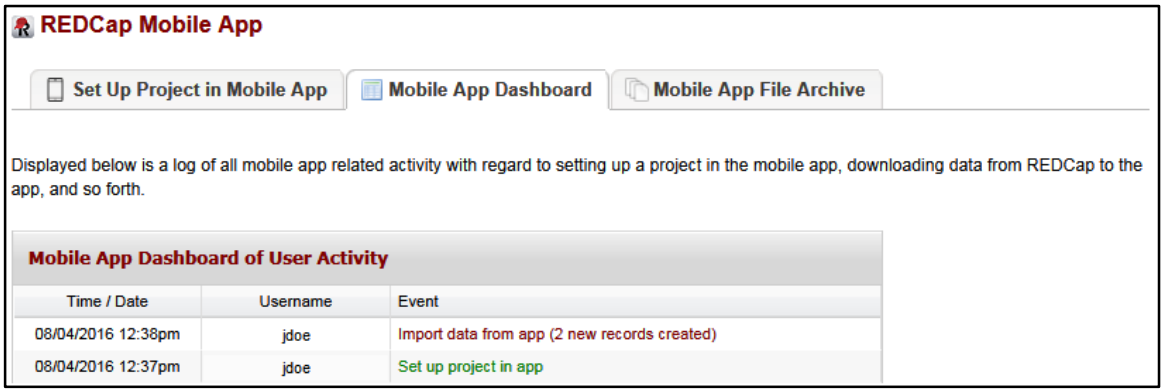
Mobile App Log: Project log for activity on the REDCap Mobile App is stored in the main project Mobile App File Archive. These can be transmitted to the server (for one given project) via the Send Project Logs button on the Project menu.



The file will show up under Mobile App File Archive tab.



REDCap Mobile App Dashboard tab displays a log of all mobile app related activity.



APP SECURITY

Security Features

- **Secure Data Transmission**: Data is transmitted securely to and from the REDCap server via SSL (https) if it is set up on the server. If SSL is not set up on the server, the REDCap Mobile App will alert the user when the project is downloaded.
- **Device's Hard Drive**: The database is encrypted on the mobile device's hard drive using SQLCipher (public key/private key encryption). This prevents someone from breaking into the file in the event of a stolen device.
- **Application**: A login with a 6-digit pin is required to access the application. Five login attempts are allowed before lockout, and a 15-minute lockout period is initiated. When the application is sent to the background or is cloaked with a screen saver, the pin is required again to access the application if a user is logged on. Similar log in attempt rules and lockout rules apply when the user reenters the application.
- **Instrument**: The Secure the Instrument feature restricts access by a participant to a single form. Enabling this feature allows you to hand over the device to a participant to enter information directly, but locks the participant out of the rest of the application as well as other forms. REDCap Mobile App user's 6-digit pin is required to unlock the form. Similarly, the 6-digit pin is required to reenter the form if the participant minimizes the application or if a screen saver interrupts form entry.
- **Logs**: Project logs for activity on the REDCap Mobile App are stored in the database's Mobile App File Archive. These can be transmitted to the server (for one given project) via the Send Project Logs button on the Project menu. These logs record data creation, modifications, and uploads; renaming, deletion, and viewing of records; and downloads of project instruments and records.

Additional Security Information

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.

FREQUENTLY ASKED QUESTIONS

1. When should I use the app?

Use the app when you need **offline data collection**, particularly in environments with poor internet connectivity. With REDCap and the REDCap Mobile App, users have new options for electronic data capture for studies that under previous circumstances would have dictated pen and paper.

2. What devices are supported?

- iOS iPhone 4 and up, iPad 2 and up. Requires iOS 6.0 or later.
- Android - phone or tablet. Requires Android 4.3 and up.

3. What type of device is best for what projects?

Since these devices are supported by the same code, the user experience is almost the same on any device. Users have provided some feedback, however, related to their particular projects that may be helpful. The Android devices have better global reach, so they are better with global health projects. The Android devices also seem slightly better with extremely large projects (1000+ records). Apple delivers better quality of device in their iPads, which is generally recognized as the best device on the market.

4. What features of REDCap are supported?

- Data entry
- DAGS
- GPS
- Pictures, videos, and audio can be uploaded into designated file fields.
- Signatures fields
- Action tags
- Instruments can be secured so that participants/users can enter their own data.

5. What noteworthy features of REDCap aren't supported?

- CATS (Computer Adaptive Test Surveys)
- Double data entry
- Survey specific features
- Survey queue
- Randomization
- Viewing files
- Inline audio/video
- Survey instructions
- Survey stop actions
- Survey thank you text
- Downloadable files in file fields

6. How are surveys and forms handled?

Normal REDCap Survey features are not used for Mobile App data collection. They are treated as entire forms without the pagination. Instruments can be secured with a pin so that participants/users will only have the option of entering data when the device is handed over to them. The instrument can be locked/unlocked via the primary user's pin.

7. What are the weaknesses of the app?

If you have online access, REDCap Mobile is a better platform because it inputs data directly into REDCap. Sending data simultaneously from multiple devices is not supported. Sending data is, at present, a complicated process.

8. What is the workflow of the app?

- Via an admin: Create a user; push projects to them; let them collect data; allow them to send data or send data yourself; clean & refresh the project; repeat; remove project.
- Via a user: Set up a project or multiple projects; collect data; send data; clean & refresh the project; repeat; remove project.

9. Can I limit users of my app so that they cannot do all functions?

User access can be restricted through the administrator interface. An administrator on the app can assign users the appropriate level of data access rights.

10. Can I use data access groups?

Yes, Data Access Groups (DAGs) are supported by the app. Whichever REDCap user supplies the download code – this user's DAG is used.

11. Can I restrict access to data?

Access to data can be restricted by using DAGs. You can also restrict all data via the user rights.

12. What happens if the app crashes (i.e., closes unexpectedly)?

This is a memory problem and probably occurred while sending data. It is probably best to perform an Emergency Data Dump. This will send a CSV to the Mobile App's File Repository. This CSV can then be used to feed the Data Import Tool. This only works while the device is online.

13. What action tags are supported?

@HIDDEN
@HIDDEN-APP
@READONLY
@READONLY-APP
@LATITUDE
@LONGITUDE
@PASSWORDMASK

@NOW
@TODAY
@BARCODE
@BARCODE-APP

14. What types of barcode/QR-code encodings are supported by @BARCODE and @BARCODE-APP?

- Android only
  - CODE_93
  - CODABAR
  - RSS14
  - PDF417
  - RSS_EXPANDED

- Android and iOS
  - QR_CODE
  - DATA_MATRIX
  - UPC_E
  - UPC_A
  - EAN_8
  - EAN_13
  - CODE_128
  - CODE_39
  - ITF

15. What security features are used by the app?

- **Secure Data Transmission:** Data is transmitted securely to and from the REDCap server via SSL (https) if it is set up on the server.
- **Secure Data Storage Encryption:** Encryption 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).
  - 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.
- **Application:** A login with a 6-digit pin is required to access the application. Five login attempts are allowed before lockout, and a 15-minute lockout period is initiated. When the application is sent to the background

or is cloaked with a screen saver, the pin is required again to access the application if a user is logged on. Similar log in attempt rules and lockout rules apply when the user reenters the application.

- **Instrument:** The Secure the Instrument feature restricts access by a participant to a single form. Enabling this feature allows you to hand over the device to a participant to enter information directly, but locks the participant out of the rest of the application as well as other forms. REDCap Mobile App user's 6-digit pin is required to unlock the form. Similarly, the 6-digit pin is required to reenter the form if the participant minimizes the application or if a screen saver interrupts form entry.
- **Logs:** Project logs for activity on the REDCap Mobile App are stored in the database's Mobile App File Archive. These can be transmitted to the server (for one given project) via the Send Project Logs button on the Project menu. These logs record data creation, modifications, and uploads; renaming, deletion, and viewing of records; and downloads of project instruments and records.

16. What happens if a tablet or phone is stolen?

Go to REDCap and revoke the API token – unless there is more than one device distributed with this token. If there is only one device, revoking the API token will not allow the thief to send data, download new data, or refresh the project. Further, when online, the thief cannot access any existing data. If there are multiple devices, revoking the API token will disable ALL devices. Use with care. Either way, access is protected with a PIN.

17. Is GPS supported by the app?

Yes, via action tags in field annotations: @LONGITUDE and @LATITUDE.

18. What issues are involved with projects with a large amount of records?

The amount of data collection is only restricted by what your device's hard drive will allow. Sending a large amount of records to REDCap could cause a memory crash on certain devices.

USEFUL HINTS

Instrument Design Hints

- You can include any fields and images (including signatures).
- You can't include video or audio as those will not be downloaded.
- You can't include external PDFs as those will not be downloaded.
- Signatures will be downloaded as those seem important enough information for a small amount of bytes.
- Regular file fields will not be downloaded. Their filenames and sizes will attempt to be downloaded.
- Don't make your forms too long. Shorter (< 100 fields) fields seem to work better with users. 1000+ field forms can induce frustration. Making your form too long can crash your device. Break up a long form into smaller forms and use the "Save and Go to Next Instrument" button.
- Heavy amounts of branching logic and calculations will slow down the rendering of your form.

Device Hints

- The most popular Android devices are the Google Nexus 7/9 and the Samsung Galaxy Tablet.
- Android devices handle large projects better, for some reason.

- iOS devices receive the best marks for hardware, but they are also the most expensive.
- Android devices have more of a global appeal because Google is in more countries than Apple.
- Wi-Fi-only devices are ok in places where Wi-Fi is readily accessible. Devices that support data transmission over cellular networks are required for places without much Wi-Fi.