Mount Sinai

**REDCap Token and Application Programming Interface Fair Use (API) Policy**

## 1. Summary

Research Electronic Data Capture (REDCap) is a secure, web-based application designed exclusively to support data capture for research studies, allowing users to build and manage online surveys and databases quickly and securely.  The REDCap API (Application Programming Interface) is a powerful tool designed to allow project teams to programmatically interact with their REDCap projects in a secure and efficient manner. As the REDCap application is an enterprise resource, it is imperative that usage of the API is regulated to ensure operational uptime and prevent inadvertent performance impacts due to misuse. This policy outlines the guidelines for appropriate usage of the REDCap API.

## 2. Fair Use

Appropriate use of the API includes tasks such as automating nightly data imports or exports, syncing participant information with other systems, or triggering real-time updates to support clinical workflows. Examples of appropriate usage include:

- Scheduled extraction of recent data collection for dashboards or custom reports,
- Upload of instrument data at regular off-peak intervals,
- Integration with mobile applications for offline data capture, participant self-reporting, and barcode or image-based data entry.

While these features enable advanced research workflows, misuse of the API can cause significant performance degradation for all REDCap users. Examples of inappropriate usage include but are not limited to:

- Bulk downloading entire datasets, or large data types (such as images or video) during peak business hours,
- Executing repeated full project exports without use of filters or timestamps for incremental data downloads,
- Launching high-frequency API requests (e.g., polling every few seconds) that strain system resources.

To maintain REDCap system stability and responsiveness, project teams should follow best practices such as limiting the volume and frequency of API calls, using filters and record lists to minimize data scope, and scheduling large data operations during off-peak hours (evenings or weekends). More information on best practices is included in the REDCap API - Developer Guide.

## 3. Usage of REDCap API tokens

Requests for REDCap API access are submitted via the REDCap application. Requestors will be required to provide details on intended usage and agree to REDCap API Fair Use Policy prior to release of an API Token. REDCap API tokens are provided at the user and project level. Service accounts are not permitted for API tokens for any REDCap environment. Usage is permitted only within the following guidelines.

### User Responsibilities

1. API tokens are user specific and should not be shared. Giving someone else access to your token may result in a breach of data or HIPAA violation. User activity is tracked by account credentials, and individuals who share their credentials are responsible for any activity or actions performed with their credentials. If you believe your API token has been compromised, contact REDCap support to regenerate your token.
2. API tokens are environment specific. Users will be granted an API token with access to the REDCap QA environment initially for the purpose of developing testing against the interface. API tokens for production are issued only after development testing is complete, and the code has been reviewed and approved by the REDCap team.
3. API tokens should never be tested in browsers. Using an API token in plain text within a script is unsecure. An API token should be encrypted within a script and called via secure environment variables or via other secure mechanisms.
4. API tokens should be removed from code before sharing with others. This includes sharing code via email, GitHub, etc.
5. If you are no longer using the API functionality on your project, contact REDCap support to delete your token.
6. External users are permitted, provided that a MSH resource has followed the appropriate process for external users. The MSH resource who approved access is responsible for ensuring account usage aligns with all relevant policies and procedures.
    a. Tokens for resources that leave the organization should be revoked by the project team immediately.
    b. Users must follow all appropriate guidelines for external users.

### Requesting a REDCap API token

Requests are submitted through the REDCap application by a REDCap account holder with API rights enabled in their project. Users will be required to complete a survey to describe the intended usage of the API. Tokens are granted permissions to Import data, Export data, or to leverage REDCap mobile applications for offline data capture.

## Development guidelines for using the REDCap API

To protect the system from long running or resource intensive usage that may impact application performance, API development must be:

- In alignment with established best practices. See the REDCap API Developer Guide.
- Tested within the REDCap QA environment before Production release.
- Reviewed by an API specialist on the REDCap team.
- Formally approved for release by a REDCap administrator.

## Expiration, Suspension, and Revocation of API tokens

API tokens are valid for 1 year. API users will receive notice of expiration 30 days prior to expiration that will include a REDCap Survey. Users will need to complete the survey to confirm that the token is still required. Once confirmed, the token can be extended for another year. If the form is not completed, the token will expire.

API tokens may be revoked at any time if REDCap application performance is impacted. Suspended tokens will not be reinstated until the code is reviewed and retested in the REDCap QA environment. If repeated performance impacts on the REDCap application are observed, a user's access to tokens may be permanently revoked.

Any changes to the code after it has been moved to the REDCap production environment will require re-testing in the REDCap QA environment. It is the responsibility of the API user to ensure that any changes are reviewed appropriately. Untested code changes which negatively impact system performance will result in a suspension of API Tokens.

Tokens that are unused after six months are automatically revoked. To recertify a new token, the process must be initiated anew. All token holders are required to attest to the policy on an annual basis. Failure to complete attestation and sign-off may result in revocation of API tokens.

## Project administrator responsibilities

The Primary Investigator (PI) or designee is responsible for regularly maintaining user accounts within the REDCap project. Responsibilities include:

1. Perform regular user account maintenance of project team members to ensure users are granted minimum necessary access to perform their responsibilities.
2. Disable user accounts immediately when individuals leave the project.
3. Revoke API tokens for users who are no longer associated with the project.