

REDCap Town Hall

Savas Sevil, REDCap Product Owner
Cate Bauer-Martinez, Senior REDCap Administrator
Priscilla Acquaye, REDCap Administrator
Jing Yang, Applications Support Analyst
Sheersha Kandwal, REDCap Technical Support Analyst

James Chip Masters, Director
Ranjini Kottaiyan, Senior Director
Mark Green, Executive Director
Patricia Kovatch, Professor and Dean

Scientific Computing and Data

Nov 11, 2024



Icahn
School of
Medicine at
**Mount
Sinai**

Introduction – Team Members



Patricia Kovatch

Professor and Dean for
Scientific Computing
and Data Div.



Ranjini Kottaiyan

Senior Director
Finance & Administration



Farhan Mahmood

Director, Scientific
Computing



Eric Rosenberg

System Administrator



Rupan Hossain

Database Administrator

Sheersha Kandwal

REDCap Technical Support
Analyst



Mark Green

Executive Director
Scientific Computing
and Data Div



**James Chip
Masters**

Director of Research
Data Services
Scientific Computing
and Data Div



Savas Sevil

REDCap Product
Owner



**Cate Bauer-
Martinez**

Senior REDCap
Analyst



**Priscilla
Acquaye**

REDCap Analyst



Jing Yang, PhD

Applications
Support Analyst

Agenda

- **Accomplishments over last six months**
- **Funding and publications**
- **Plans for next six months**
- **REDCap and 21 CFR 11 Implementation & Compliance**
- **REDCap API Usage Policy**

Accomplishments over last six months

REDCap Users and Projects

Active* Projects by Type, As of 18 October 2024:

Faculty Practice Associates (FPA) Operations	37	1%
Hospital Operations	571	18%
Medical Student Project	69	2%
Quality Improvement	788	25%
Research	1,660	53%
Total number of projects	3,125	

As of end of October 2024	
Total # user accounts	21,100
Active* # users	3,579
Total # projects	6,532
Active* # projects	3,125

*logged in/accessed in the past 6 months

REDCap Support Tickets

Presentation Metrics: 3/1/2024 to 11/1/2024

Customer Request Type

(Multiple values)

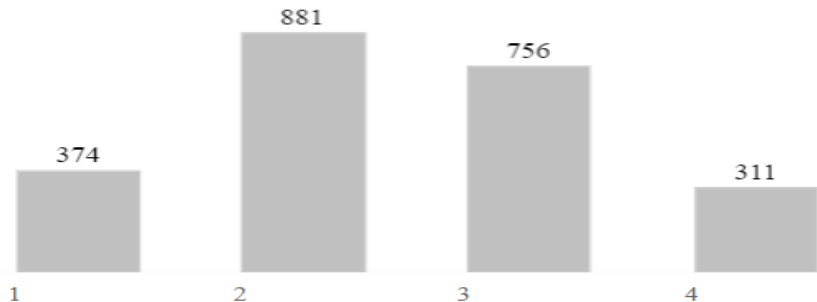
Start Date

3/1/2024

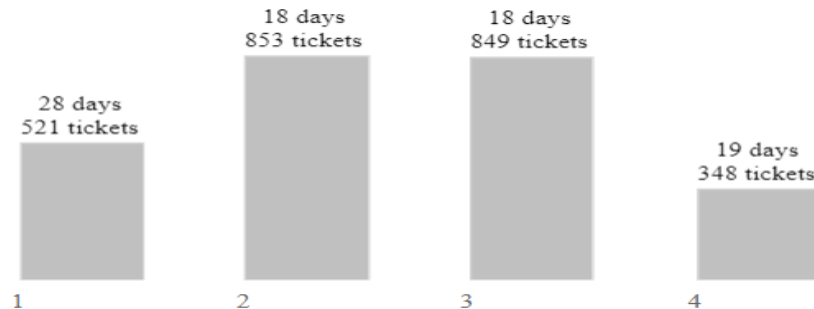
End Date

11/1/2024

Number of Tickets Created: 2,322



Number of Tickets Resolved: 2,571



Ticket Breakdown

	Percentage	# of tickets
Support: Project Specific Questions	42%	964
Support: Account Login	32%	754
Support: Review/Approve Project Changes	16%	360
Support: Non-Project Specific Questions	4%	99
Maintenance: Technical Support	4%	95
Project Build and CDP	2%	38
Support: Emailed Request	1%	12

- 2,322 Tickets created
- 2,571 tickets resolved at a rate of 300+ tickets per month
- CDP: Clinical Data Pull

Major Accomplishments since Mar 2024

- **Upgraded REDCap** from version 14.0 to 14.0.29
 - Major security fix: A Stored XSS (Cross-site Scripting) vulnerability fix
 - Medium security fix: A Reflected XSS (Cross-site Scripting) vulnerability
 - 5 bug fixes
- **Collected 553 publications** enabled by REDCap (spanning 2017-2024)
- **Completed** 2024 REDCap chargeback collection
- **207** Digital Concierge one-to-one interactions and **2,475** service desk requests

Engaged with 565 REDCap Users: October 2023-October 2024

Date	Event	Event Details	Participants
10/12/2023	Training	REDCap Essentials	50
10/23/2023	Town Hall	Fall Town Hall	19
2/13/2024	Office Hours	Chargeback Special Office Hours	7
2/20/2024	Office Hours	Chargeback Special Office Hours	4
2/29/2024	Office Hours	Chargeback Special Office Hours	4
4/18/2024	Town Hall	Spring Town Hall	20
5/9/2024	Outreach	Lunch and Learn event for newer researchers	4
	Digital Concierge	October 2023-October 2024	361
9/24/2024	Training	REDCap Essentials	96

Total: 565

REDCap System Maintenance: April 2024 – October 2024

99.8% uptime

Planned:

- 2 planned downtime for 4.5 total hours for 2FA Testing and REDCap security updates

Unplanned:

- Five 1-2 minute (on 5/14, 5/23, 7/17 and 8/1), one 4 minutes (on 8/24), one 7 minutes (on 8/16) and one 10 minutes unplanned interruption (on 4/17)
 - Caused by a surge in database connections, the likely cause is API use
 - New API token requests must provide a summary of purpose and are reviewed on a case-by-case basis
 - Current communication rate cap for APIs and the API token monitoring that REDCap allows is not preventing these
 - To understand the cause and prevent this from happening again, we have:
 - In Q4 we are deploying MySQL enterprise version with more advanced monitoring tools
 - In Q4 we will enact a API usage policy that API users need to agree to

Working Towards 21 CFR Part 11 Compliance/Validation

- Draft version of Implementation Guide for 21 CFR Part 11 Compliance in REDCap created
 - 2FA will be implemented by 11/04/2024
- Cate attended REDCapCon
- We are participating in the monthly meetings for the newly established (in October/November 2023) CTSA REDCap 21 CFR Part 11 working group
- This a mix of institutions: some that have validated a REDCap installation (Vanderbilt University Medical Center, Cincinnati Children's Hospital Medical Center and others) and many that want to do so (Columbia Medical Center, Yale University, UNC-Chapel Hill and others).
- “This Working Group seeks to aid CTSA sites in achieving and maintaining 21 CFR Part 11 compliance for electronic records in clinical research, primarily those records collected through REDCap. We will develop and disseminate an implementation guide that provides clarity about the validation requirements and process for institutions to adopt.”

Two-Factor Authentication (2FA) Implementation

- 2FA is tested in QA
- Moved to PROD on 11/04/2024
- Benefits; 1. Compliance with Cybersecurity policies 2. Working towards 21 CFR checklist
- The feature is turned on and there was not any down time necessary

Funding and Publications

Funding and publication details

Service	# of pubs 2023	# of pubs since 2012	# of selected high impact pubs***	# of high impact pubs since 2012	# of citations of all pubs	Amount of funding**
REDCap	157	553	4	10	12,734	\$107,281,989

** Subcontracts from other organization were only included if reported by the PIs or used for chargebacks

*** Journals with impact factor ≥ 30

How we collected the numbers

Service	Publication collection method	PI response rate for pubs	Funding collection method	PI response rate for funding
REDCap	PIs report via survey	227/673	PIs confirm via survey	121/185 PIs confirmed 120 NIH awards
			Paid by NIH awards	42 NIH awards

Plans for next
six months

Plans for next six months

- Begin to plan for **next REDCap major version upgrade** during 2025 Q1
 - This will be a LTS (Long Term Support) Release
 - 14.7.0 New Features
 - Multiple randomizations in a project: Users may now define more than one randomization model in a single project.
 - Blinded randomization support: Users may now create a randomization model that is blinded/concealed as a means of concealing the allocation (randomization value) from users to be able to have a truly blinded randomized clinical trial, for example.
 - New Smart Variables;
 - [rand-number] The randomization number assigned to the record.,
 - [rand-time] The server date and time at which a record was randomized.
 - [rand-utc-time] The UTC date and time at which a record was randomized.
 - New “Randomize Record” API method: This method allows an API user to randomize a record using the API.
 - New External Module Hook “redcap_module_randomize_record”: Allows custom actions to be performed prior to the randomization of a record - e.g., to override the default randomization allocation.
 - Real-Time Trigger Logic: Randomization can be automated to occur in real time when an instrument is saved and a specified logic expression becomes True, in which all required stratification information must be present.
- Work to automate some low-level REDCap Administrator tasks to **provide faster resolution of common issues for our users** (account unsuspension and project unlocking). Chatbot – Jing is planning to move it to PROD end of December 2024.

Reminder: Policy for deleting unpaid REDCap projects

- **9,618 REDCap projects were locked for nonpayment in the weeks following the January 31 payment deadline**
- **We marked to delete the 8,128 locked REDCap projects that are unpaid.**
- **The 1,490 projects are deleted by users or REDCap team extended their time to download the data or provide a fund number.**

- The process is:
 - We will notify the PIs and project users monthly if the project is unpaid for 9 months after the trial period or one year after the project creation date.
 - We will communicate to the PIs and project users of the impending project deletion.
 - We will delete the project at the one year mark from the project creation date.

REDCap and 21 CFR 11 Implementation & Compliance

About 21 CFR 11 Compliance & Requirements

- Title 21 Code of Federal Regulations (CFR), Part 11 outlines a set of criteria for the FDA which outline how trustworthy and reliable electronic records, signatures, and electronically stored handwritten signatures are
- These regulations are meant to encourage the adoption of electronic systems while protecting the public
- The FDA requires that parties conducting a study submit data and results for review which can include case report forms (CRFs), case report tabulations (CRTs), and datasets. While CRTs are aggregated level data, CRFs are the forms used by investigators to document data.
- Applies to Investigational New Drug (IND) or Investigational Device Exemption (IDE)
- Ensuring an information system (such as REDCap) is compliant with this is essential

21 CFR 11 Compliance: Responsibilities

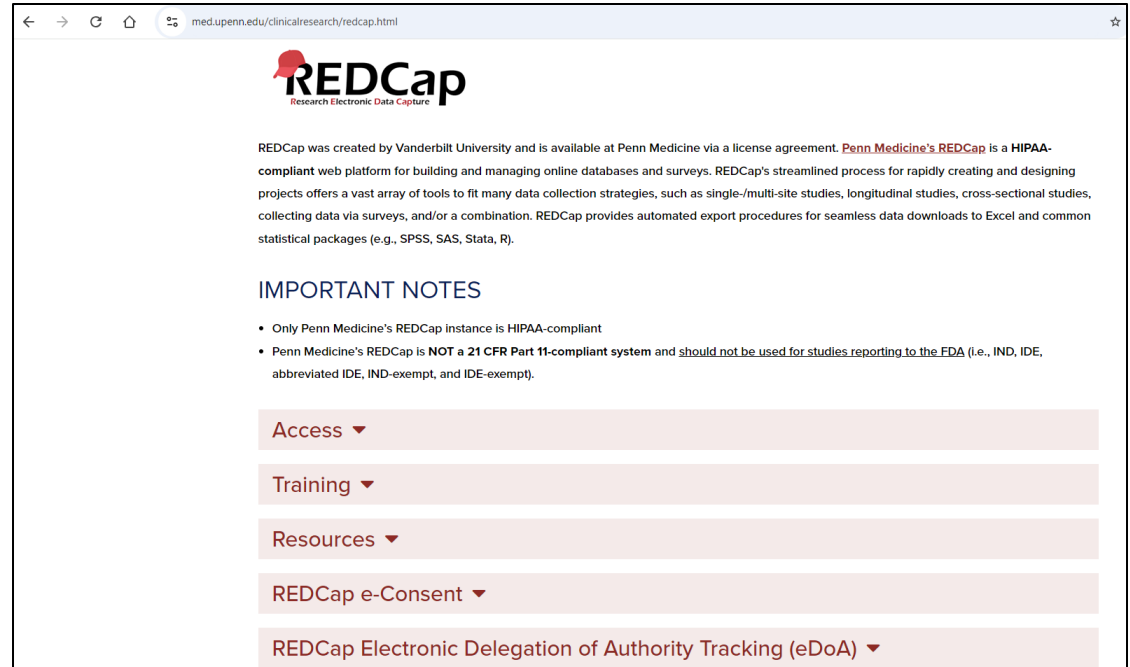
- HIPAA Compliance is not the same as CFR 21 Compliance – studies that report to the FDA require CFR21 compliant systems (IND, IDE, abbreviated IDE, IND-exempt, IDE-exempt)
- Organizations can implement infrastructure, processes, resources that will help research projects be 21 CFR 11 compliant
- However, researchers are ultimately responsible for ensuring compliance
- The FDA will audit AT THE PROJECT level, not at the organizational level – so PIs and researchers are responsible

What are the Key Compliance Requirements?

Item	Description
Server	The computer servers hosting software like REDCap need to be properly secured, have access control, proper password policies, etc.
Security	Ensure that strong password policies are in place, that 2-factor authentication, and other security procedures are implemented.
Personnel	Personnel are properly trained, including project leads and support staff.
Policies	Implement policies that ensure that researchers are using software, tools, and workflows that are 21 CFR 11 compliant.
Procedures	Create and maintain procedures for ensuring that researchers and projects are 21 CFR compliant.
Training	Researchers and staff are trained in policies ensuring compliance. This includes support staff maintaining software, legal departments, etc. A good example of a training video for eConsent is available from Northwestern University: https://redcap.nubic.northwestern.edu/redcap/surveys/?s=PTMYLMFFWP
Validation	Policies and procedures, including software systems, are validated and documented.
Documentation	Appropriate documents are kept at the organizational, departmental, and project level.

1. Don't Implement CFR 21

- Direct researchers to other resources (ex. REDCap Cloud)
- Make it clear on our website that we are not 21 CFR compliant – up to the PI, send announcements

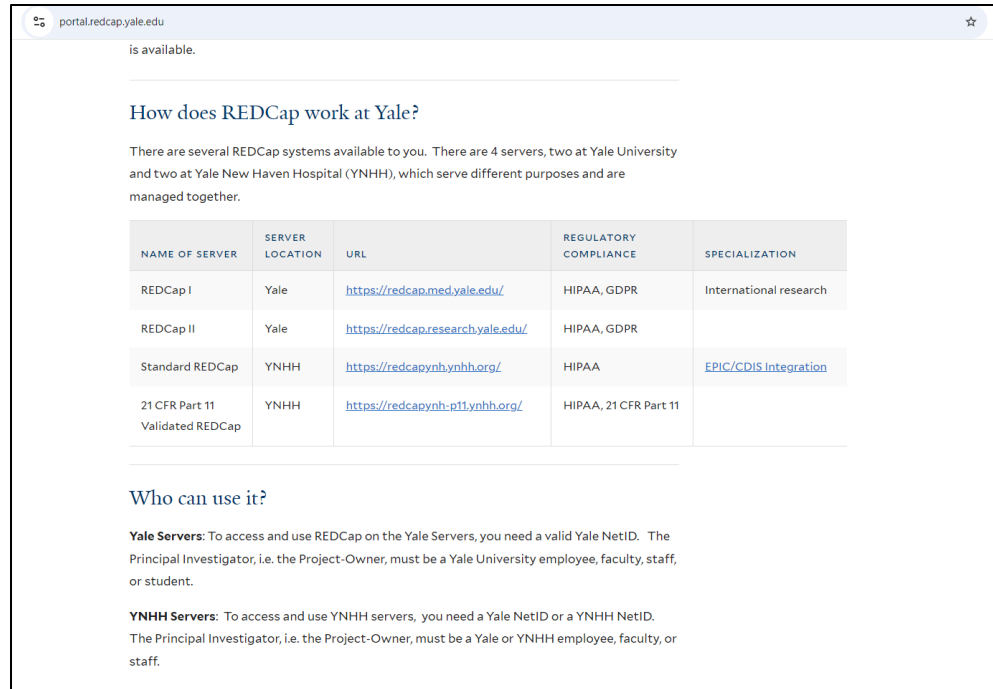


The screenshot shows the Penn Medicine REDCap website. The browser address bar displays "med.upenn.edu/clinicalresearch/redcap.html". The page features the REDCap logo (Research Electronic Data Capture) and a paragraph explaining that REDCap was created by Vanderbilt University and is available at Penn Medicine via a license agreement. It states that Penn Medicine's REDCap is a HIPAA-compliant web platform for building and managing online databases and surveys, offering a vast array of tools for various data collection strategies. Below this, there is a section titled "IMPORTANT NOTES" with two bullet points: "Only Penn Medicine's REDCap instance is HIPAA-compliant" and "Penn Medicine's REDCap is NOT a 21 CFR Part 11-compliant system and should not be used for studies reporting to the FDA (i.e., IND, IDE, abbreviated IDE, IND-exempt, and IDE-exempt)". At the bottom, there are five dropdown menus: "Access", "Training", "Resources", "REDCap e-Consent", and "REDCap Electronic Delegation of Authority Tracking (eDoA)".

UPenn does not have CFR 21 compliant REDCap

2. Fully Implement CFR21 Compliant REDCap

- Most organizations have a separate build
- This will require extra resources to build and maintain:
- 2 FTEs for 6 months – 1 FTE to maintain long term + \$50k for additional servers
- We need funding to do this



portal.redcap.yale.edu

is available.

How does REDCap work at Yale?

There are several REDCap systems available to you. There are 4 servers, two at Yale University and two at Yale New Haven Hospital (YNHH), which serve different purposes and are managed together.

NAME OF SERVER	SERVER LOCATION	URL	REGULATORY COMPLIANCE	SPECIALIZATION
REDCap I	Yale	https://redcap.med.yale.edu/	HIPAA, GDPR	International research
REDCap II	Yale	https://redcap.research.yale.edu/	HIPAA, GDPR	
Standard REDCap	YNHH	https://redcapynh.ynhh.org/	HIPAA	EPIC/CDIS Integration
21 CFR Part 11 Validated REDCap	YNHH	https://redcapynh-p11.ynhh.org/	HIPAA, 21 CFR Part 11	

Who can use it?

Yale Servers: To access and use REDCap on the Yale Servers, you need a valid Yale NetID. The Principal Investigator, i.e. the Project-Owner, must be a Yale University employee, faculty, staff, or student.

YNHH Servers: To access and use YNHH servers, you need a Yale NetID or a YNHH NetID. The Principal Investigator, i.e. the Project-Owner, must be a Yale or YNHH employee, faculty, or staff.

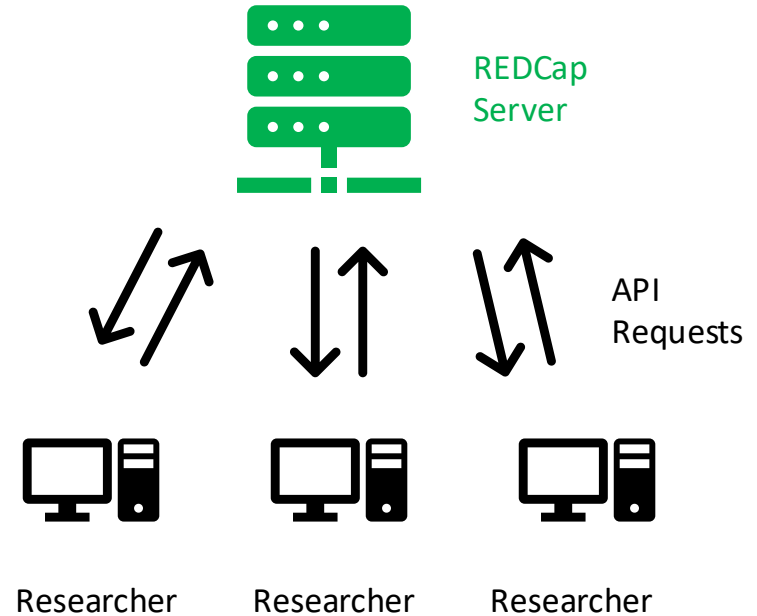
REDCap API Usage Policy

Overview

- About the API
- Current User Statistics
- Existing Policies and Standards
- Draft API Usage Policy
- Future Steps

About the API

- REDCap offers a set of API endpoints for retrieving data from their database
- Some of the endpoints trigger simple queries which are very easy to handle
- Others are more complex and much slower, which can block the ability of others to access services
- We have issued nearly 1000 tokens to enable user code to connect to the API the past few years
- **In the past 12 months: we've had recurring outages due to user code**



Current State: API User Statistics

- In the past 6 months:
 - 406 separate projects
 - 106 unique users
 - Top 10 users responsible for 50% of API calls
 - Top 20 users responsible for 67% of API calls
- We propose a simple policy to increase REDCap reliability

Best Practices: Existing Policies and Standards

- Several existing standards exist (ex. UT Southwestern)
- There are also several software libraries already written which can help with writing standardized, safe code (ex. PyCap)

Best Practices for APIs in REDCap

Statement from REDCap Developer's at Vanderbilt:

Direct database back-end access in REDCap should not be allowed. Not only does back-end access bypass REDCap's built-in logging abilities (thus creating compliance issues), but it is likely to cause permanent damage to data. REDCap's data model is very complex and is always changing, so a simple mistake could cause great damage to valuable data. Additionally, some back-end queries that might be correct now might no longer be correct in a future version of REDCap as the data model changes with every new version. For all these reasons, we (the REDCap developers at Vanderbilt) only recommend using front-end methods in the application (website and API) for extracting data. Any other method is not recommended.

The only method of interfacing data for the UT Southwestern Instant of REDCap that is supported is the built-in API functionality using the secure API key. This is the only way to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (Title 45, Parts 160 and 164, subparts A and E of the Code of Federal Regulation (the "Privacy Rule"). The following is some best practice guidelines for writing APIs for REDCap.

1. Use the API Playground if possible to generate your code. Why struggle when a computer can struggle for you?
2. API Export and Import use the same data structure formats. If you have trouble having API Import's data to be formatted properly, do an API Export. Make the data structure viewable in some form via whatever language you want (json_encode for PHP, JSON.stringify for JavaScript, etc.). Then modify the data values logically to form a new JSON to put into an API Import call.
3. Put the data into a JSON. Do not leave it in its native structure. For some languages, like JavaScript, this is not a big deal. For other languages that do not use JSON-compatible data structures (like PHP, Objective-C, Swift, etc.), putting the native structure into the POST command dooms you to failure. Just throw it into a JSON-encoded structure (which most likely will be a string in standard JSON format), and put it into the data field. I promise, it'll work.
4. API JSON data structures are in arrays ([...]). If you leave it as a hash ({ ... }), your call will not succeed. Easy to say, easy to forget.
5. API Import calls have a data parameter; API export calls do not. If the content is the same, they are probably the same except for that data parameter. Save yourself a little time.
6. Decode JSONs in PHP using json_decode(json, true). If you leave off the parameter with the true, PHP will attempt to decode the JSON as a hash; since it is not a hash, it will fail and leave you wondering like you've been stood up on a date. Always, always put the true as the second parameter when dealing with REDCap.
7. Keep in mind memory limitations when the API will be communicating with a phone or tablet. You may need to change the synchronization process to proceed one record at a time. Sometimes you have to break up API Import or Export calls.
8. Any mobile calls are almost certainly cross domain. Turn this on if it is available on your program (as it was available with my on JavaScript's AJAX calls). Read up on JSONP if you wish.
9. JSONs easier to handle than XML or CSV. To some extent, this is a personal preference, but JSON parsers seem more friendly than XML or CSV to me for computational processing. Of course, this depends on your application.
10. When using the same basic API code for a new project, duplicate it, then just change the PID and the API Token and you should be good to go.

Draft API Usage Policy

- Using existing standards, we drafted a brief policy for API usage based on existing policies in other organizations
- Addressed using best practices suggested by Vanderbilt, using existing coding libraries, testing, throttling requests, monitoring, etc.

**REDCap Token and Application Programming Interface (API)
Use Process and Policy 1.0
Scientific Computing and Data
Icahn School of Medicine at Mount Sinai
October 25, 2024**

Mount Sinai's REDCap instance enables users to request REDCap data using their own code via API calls. This policy is intended to ensure a reliable and responsive REDCap experience for all users.

The process and policy are as follows:

1. Request an API token
 - Please complete the request form at <https://redcapform>.
 - Provide justification for the token, including any feature requests.
 - **Please note:** REDCap API tokens are user and project specific.
2. **Users must attest that they have read the best practices and policy and agree with signature to abide by them** Complete REDCap API training on best practices. Relevant documents are: located here: https://www.utsouthwestern.edu/edumedia/edufiles/about_us/admin_offices/academic_information_services/redcap/best-practices-apis.pdf +++++ more requirements
 - Please consider reusing existing REDCap API code and libraries as described here: <https://github.com/d3b-center/d3b-redcap-api-python> and PyCap (<https://redcap-tools.github.io/PyCap/>) for Python, <https://cran.r-project.org/web/packages/REDCapR/> and <https://github.com/nutterb/redcapAPI> for R.
 - Examples of how to connect to REDCap using Python, R, Java, and other languages can be found here: <https://confluence.research.cchmc.org/display/CCTSTRED/REDCap+API+Examples>.
 - Upon **training completion attestation and signoff to best practices and policy**, certification will be sent to the REDCap team.
 - A QA token will only be issued upon user agreement to this process and policy **and completion of required training**.
 - **Attestation and signoff to best practices and policy Training** must be **taken given annually**.
 - **Incomplete training Absence of attestation and signoff** will result in API tokens being revoked.
3. Testing of user-developed APIs in the REDCap QA environment is mandatory. To comply:
 - Open a ticket for access to the REDCap QA environment to test your API request code and include your preferred time to test.
 - The REDCap team will respond with a time to test your code.

Implementation

- The policy includes user training, agreement to abide by best practices, monitoring, revalidation, revocation policies
- All existing user code needs to be validated in our user environment before usage
- Will phase in the policy over 6 months to groups of users in batches, addressing high API usage researchers first in a targeted fashion
- Will iterate and update the policy as needed
- **Question: do you agree with the timeline?**

Thank you

Scientific Computing and Data

Nov 11, 2024



Icahn
School of
Medicine at
**Mount
Sinai**

Appendix

Results of the required CTSA acknowledgement agreement

- REDCap PIs agree to cite the CTSA acknowledgment, since the operation of REDCap is supported by CTSA
- We sent rounds of email communications with a survey link to 411 PIs with active REDCap projects and required users to cite the acknowledgement by Friday 3/22/2024.
- **374 PIs agreed to the acknowledgement**
- The 27 REDCap user accounts held by the remaining 37 PIs are suspended
- Proceeding with locking REDCap projects associated with these 37 PIs

“This work was supported in part through the computational and data resources and staff expertise provided by Scientific Computing and Data at the Icahn School of Medicine at Mount Sinai and supported by the Clinical and Translational Science Awards (CTSA) grant UL1TR004419 from the National Center for Advancing Translational Sciences.”

To associate the CTSA grant UL1TR004419 to an existing publication, please follow [these instructions](#) from the NIH (see the section "Associating Funding to your Publications").



CTSA Acknowledgement

Principal Investigators on projects that use Scientific Computing and Data CTSA-supported services (Mount Sinai Data Warehouse, REDCap, Leaf and Atlas cohort query tools) are required to acknowledge this support by including the following acknowledgement in a publication of any material, whether copyrighted or not.

"This work was supported in part through the computational and data resources and staff expertise provided by ScientificComputing and Data at the Icahn School of Medicine at Mount Sinai and supported by the Clinical and Translational Science Awards (CTSA) grant UL1TR004419 from the National Center for Advancing Translational Sciences."

To associate the CTSA grant UL1TR004419 to an existing publication, please follow [these instructions](#) from NIH (see the section "Associating Funding to your Publications")

[Scientific Computing](#)

REDCap Service Desk

Welcome! You can raise a REDCap Service Desk request from the options provided.

Clinical Data Pull Project users to validate data access and permission level

- We are planning to require the projects/users that want to use clinical data pull with EPIC to first validate their data access and permission level with the EPIC team before we begin work on their CDP request?
- Users need to raise a ticket with EPIC data access groups to validate their permission and access level. If they do not have sufficient data access level, they can provide the necessary documents to obtain it.
- We are working on a standard operating procedure for initiating and fulfilling a clinical data pull project.
- **Do you agree with this approach?**

REDCap 14.0.29 upgrade

- **CHANGES IN THIS VERSION:**

- **Major security fix:** A Stored XSS (Cross-site Scripting) vulnerability was discovered in which a malicious user could potentially exploit it by inserting custom HTML and JavaScript in a specially crafted way into any user input that is then output on a page in REDCap (e.g., field labels, survey instructions, data displayed on a report). This vulnerability can be exploited by authenticated users and also by survey participants entering data. Bug exists in all REDCap versions.
- **Medium security fix:** A Reflected XSS (Cross-site Scripting) vulnerability was discovered in which a malicious user could potentially exploit it by inserting custom HTML and JavaScript in a specially crafted way into a specific API parameter's value that is used in the API File Import, File Export, and File Delete methods. This vulnerability can be exploited only by users with a valid API token. Bug exists in all REDCap versions.
- **Minor security fix:** An authenticated user could make a simple request to a very specific REDCap end-point, in which it would reset the REDCap Base URL and thus make the application temporarily unusable to users accessing REDCap in a web browser.
- **Bug fix:** In the previous version, it was mistakenly thought that the variable name "calculate" needed to be added to the reserved variable name list, but that turned out not to be true. Because of some new underlying code fixes, that variable name is still allowed (Ticket #231128b)
- **Bug fix:** When exporting an instrument PDF, the word "Confidential" would fail to be displayed in the PDF's left header by default (this excludes participant-facing PDFs, which should not display this text).
- **Bug fix:** When making a call to the Export Logging API method for a longitudinal project, the event name would mistakenly be omitted in the API response. (Ticket #210938)
- **Bug fix:** Long choice labels for fields used in Smart Charts, specifically bar charts, might mistakenly appear as too wide on the chart and thus might overlap with other text, making it hard to read.
- **Bug fix:** The survey queue was mistakenly not translated in MLM-enabled projects when it was displayed on the survey page itself (as opposed to when specifically viewing the survey queue page after completing the survey).

Need Your Guidance

Question #1

Providing a 21 CFR Part 11 compliant version of REDCap for FDA compliance purposes.

- Providing a 21 CFR Part 11 compliant version of REDCap for FDA sponsored clinical trial
- The two options are:
 - 1. Do not implement 21 CFR Part 11 – direct researchers elsewhere to REDCap cloud or other resources
 - 2. Fully implement 21 CFR Part 11 compliant instance of REDCap – common but requires additional resources
- **Question: which approach do you agree with?**

Question #2

Implementing an API Policy to test API code in QA

- Do you agree with the timeline proposed, which involves phasing in the policy over 6 months?