Children's Trust Fund
Missouri's Foundation For Child Abuse Prevention

# REDCap™ POLICY AND USAGE GUIDELINES

| | |
|---|---|
| **Version:** | 14.3.14 |
| **Author:** | CTF REDCap Administrator |
| **REDCap Support Email:** | redcap@oa.mo.gov |
| **Issued:** | 7/2025 |
| **Next Review:** | 7/2026 |

## OVERVIEW OF REDCAP

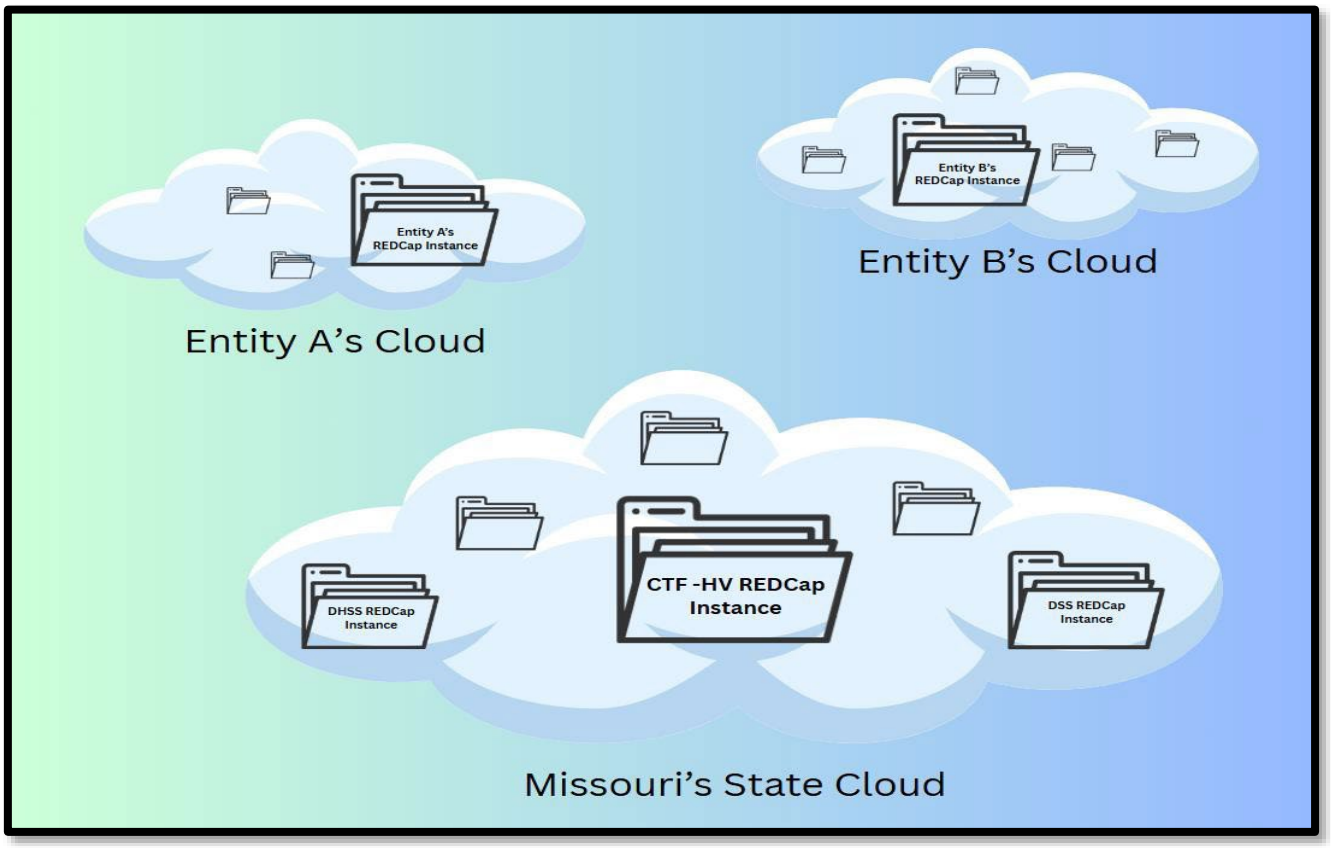
This document is for the development of policies and procedures relating to the hosting and administration of REDCap utilized by the Missouri Children's Trust Fund (MO CTF).

MO CTF program data is developed and maintained within a REDCap application (*i.e. CTF REDCap*). REDCap (Research Electronic Data Capture) is a secure web-based software application for building and managing online surveys and databases. REDCap is designed to support data capture providing 1) an intuitive interface for validated data entry and data collection; 2) audit trails for tracking data manipulation and export procedures; 3) automated export procedures for seamless data downloads to common statistical packages; and 4) procedures for importing data from aligned external sources.

REDCap software was developed by Vanderbilt University in 2004 to be utilized by individual entities obtaining a product license for research/data purposes. REDCap is available at no cost to academic, governmental and non-profit institutions through the REDCap Consortium. REDCap is adaptable and offers various customizations, allowing REDCap Administrators to tailor the platform to meet specific needs. It is used by thousands of organizations across 160 countries.

## PRODUCT INSTANCES

A REDCap instance is the platform where REDCap is installed and running. The CTF REDCap is hosted on a web-based Azure Cloud platform that is secured and protected by a state server and monitored/maintained by state personnel within the Missouri Information Technology Services Division (ITSD): https://redcapdese.azurewebsites.net/redcap/. ITSD Technicians are responsible for maintaining technical security within systems and applications and analyzing technical vulnerabilities in systems to mitigate risk.



What does this mean? The CTF REDCap *Instance* lives in the Azure cloud for the state of Missouri for security and oversight purposes; however, only approved users have access to REDCap within the cloud. REDCap can have multiple instances within a cloud. For example, a state entity may have a REDCap application for each of its internal departments that technically live within the same state cloud, but each department doesn't have access to each other's REDCap instances within that cloud.

Think of REDCap like a file on a shared drive (the cloud) that only specific users can see or utilize. Having access to REDCap doesn't give you access to the rest of the cloud and having access to the cloud doesn't give you access to REDCap (unless you're an ITSD Administrator).

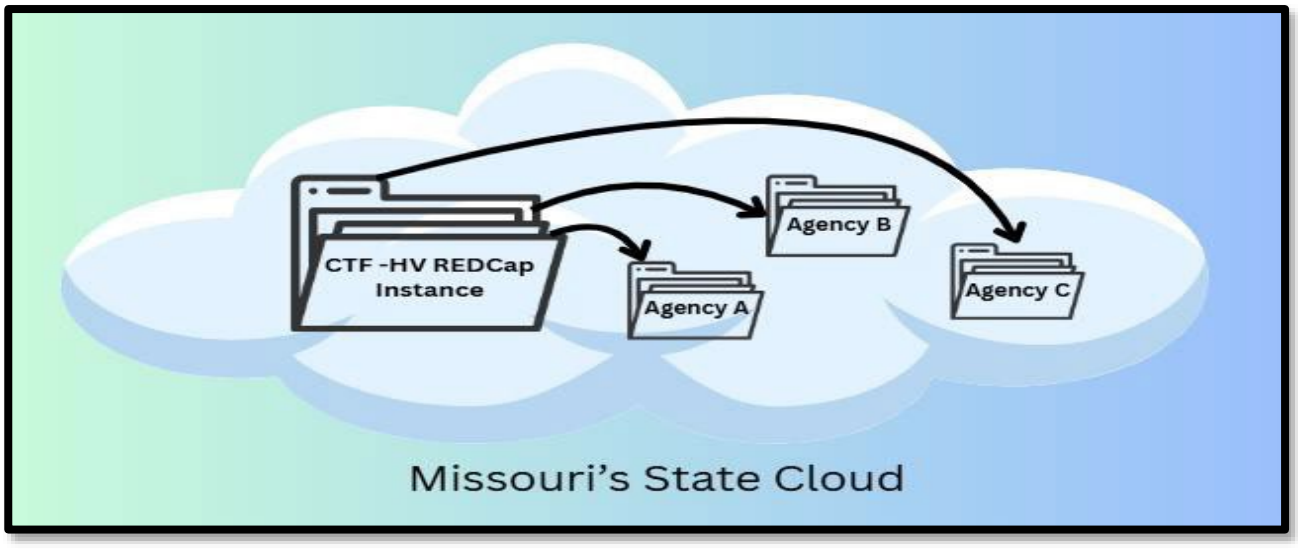
REDCap instances can also live in many different clouds (one per organization/entity utilizing the application). For example, you may have a university that has its own cloud and its own instance of REDCap. The university's cloud and licensed REDCap are within the university's digital walls and don't interact with other clouds or REDCaps just like you wouldn't have access to another organizations Excel software or shared drive. An example is shown in in the picture above.

## CTF REDCAP INSTANCE

CTF funded programs, including home visiting programs and/or home visiting programs participating in collective impact, are expected to use an approved/aligned REDCap application for data collection and referral system purposes.

The CTF REDCap is custom built to meet the needs of the grantor and its' programs. Within the REDCap Instance, each individual program has their own unique REDCap project(s). Projects may include a main data collection project where the program records their program data and activities and/or a Coordinated Referral & Intake (CRIS) project which connects them to their home visiting referrals.

REDCap projects are distinctive from one another and programs can only see their own individual REDCap projects data (as seen below).




For home visitation programs, all visible data is expected to be complete in the CASE MANAGEMENT module of any respective REDCap project following specific guidelines outlined in the view schedule

and associated screening and forms schedules. Recorded trainings are provided to help programs navigate CTF REDCap and one-on-one trainings can be provided as requested.

## REDCap projects for State Funded Home Visiting Grantees

CTF funded home visiting programs with a state home visiting grant will have a main data collection project to capture core home visiting data that is aligned across all CTF grantees and is expected as a part of their grant requirements. CTF's core data collection is aligned with MIECHV demographics, benchmarks and expectations to create a standard of data collection across Missouri. Additional data points may be collected at CTF's discretion.

These programs checkmark which home visiting grant each person in the family is funded under by completing the funding source form in REDCap (CTF-Home Visiting, MIECHV, MOPPP, etc.). CTF home visiting grantees are expected per their agreement to participate in their regional CI sites referral system (at minimum as a CRIS-Only partner).

If a program is also participating in a CI sites full data collection, then their main REDCap data collection project may be expanded to meet the needs of the CI site and be utilized for CTF data collection purposes - *eliminating the need for duplicate entry into multiple REDCap data collection projects.*

## REDCap projects for Collective Impact Site Participants

What is Home Visiting Collective Impact (CI)? Collective Impact is a structured approach to home visiting that brings together multiple models of home visiting to work towards a shared goal, common agenda, shared measurement, and mutually reinforcing activities with a backbone organization that supports/manages the partnership. In Missouri, there are five regional CI sites that are supported by CTF and that manage their regions collective activities, data collection to demonstrate collective outcomes, and Coordinated Referral and Intake Systems (CRIS). The data collected for the CI sites contains and is aligned with the CTF full core data collection and includes a few more forms to produce regional outcomes.

Home visiting programs participating in a CI site's REDCap project(s) can fall into two categories: (1) a CRIS-Only partners that is only receiving home visiting referrals and (2) a Full Implementation or Full Data Collection Partner that is fully participating in CRIS referrals, CI site data collection and other activities.

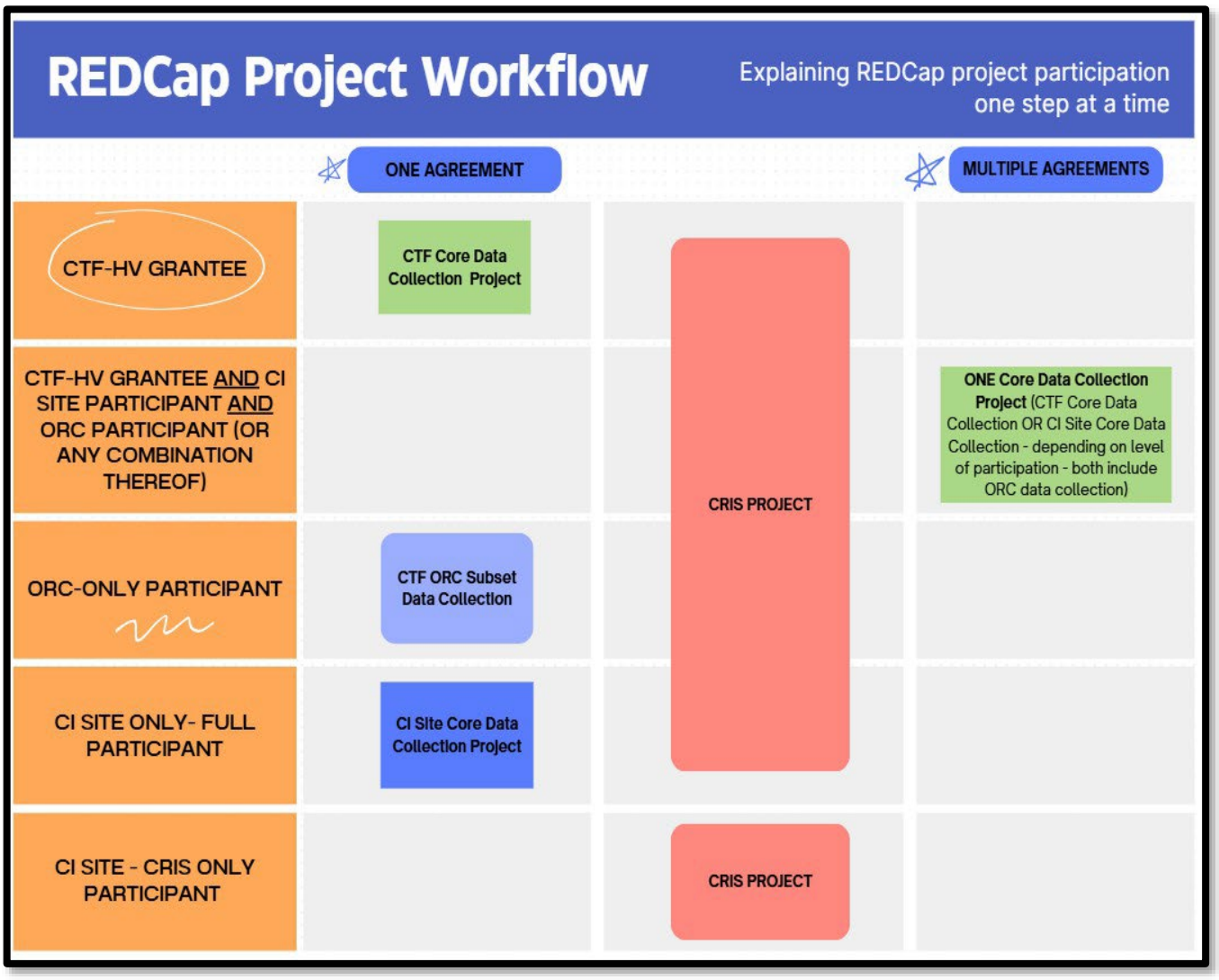
1) **CRIS-Only Partners –** these programs will have a CRIS-Only project where they will go to monitor and process home visiting referrals for their program.
2) **Full Implementation/Data Collection Partners -** these programs may have a CRIS project as well as a data collection project for the CI site or it may all be the same project depending on the situation.
    a. If a program is also a CTF home visiting grantee then their main data collection project may be expanded to meet the needs of the full CI data collection and utilized for CI purposes - *eliminating the need for duplicate entry into multiple REDCap projects.*
    b. Training for the CI sites specific data collection and referral system is provided directly by CI site staff. Note: *You may have more than one CRIS project if you cross over into multiple CI site regions (1 per region).*

## REDCap projects for Outcomes Rate Card (ORC) Participants

The data collected for the CTF ORC is a smaller subset of CTF's core data collection. Home visiting programs participating in the CTF Outcomes Rate Card (ORC) can fall into two categories: (1) a program already participating in REDCap data collection through a CTF home visiting grant AND/OR already participating in a collective impact sites data collection (CTF state funded grantee and/or CI site full implementation partner) and (2) a program that is not receiving a state home visiting grant and/or participating in a collective impact sites data collection (known as CTF-ORC Only).

1) **CTF state funded grantee and/or CI site full implementation partner –** these programs already have a data collection project for CTF's or the CI sites core data collection. Since CTF ORC is a subset, these programs use their main data collection project as per usual and do not need to collect additional data or have a separate data collection project for ORC.
2) **CTF-ORC Only –** these programs, since not participating elsewhere in REDCap, will have a specific ORC only project for their data collection that just focuses on the subset data collection.

Both program categories mark "CTF ORC" on the funding source form for each person in the family to identify that they are ORC funded. ORC participants are expected per their agreement to participate in their regional CI sites referral system (at minimum as a CRIS-Only partner).



## SYSTEM SECURITY

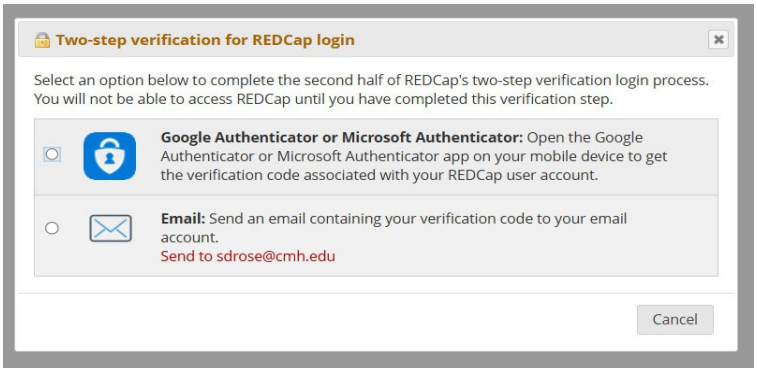
Security surrounding REDCap is dependent upon the IT infrastructure and environment in which REDCap has been installed. Missouri's ITSD team includes thousands of IT professionals with diverse skill sets. These state employees are dedicated to providing Missouri's state agencies with the systems, networks and technical support they need in order to provide services to Missouri's citizens, businesses and other government entities. This includes mitigating risk by providing secure servers, storage and email to store and process state data. ITSD also provides 24x7 Cyber-Security governance, expertise and operational management to protect resources and data. Designated ITSD staff are responsible for monitoring and maintaining REDCap and Azure cloud security for Missouri state departments including CTF. ITSD and state personnel managing system security regularly monitor systems and complete activities to prevent incidents. ITSD's Office of Cyber Security (OCS) is responsible for safeguarding the state's information systems. OCS promotes and provides expertise in information security management for all state agencies and supports national/local homeland information security efforts. Missouri's Chief Information Security Office (CISO) oversees OCS.

If a security threat or breach is discovered, it will be communicated to all involved parties. ITSD Breach policies, the CTF Privacy Policy and procedures related to contract compliance and notifications to specific funding entities will be followed. If you suspect that there has been theft of, or unauthorized access to, REDCap data you need to immediately communicate that with CTF staff and the CTF Privacy Officer. The Office of Administration, ITSD, CTF and CTF contracted staff are responsible for meeting any compliance requirements driven by applicable data protection laws. REDCap Administrators and CTF personnel that have access to individual level data in REDCap have completed any required data security, HIPAA, privacy/confidentiality and cyber security trainings.

### Regulatory Compliance

**Azure compliance.** https://learn.microsoft.com/en-us/azure/compliance/
**REDCap compliance.** REDCap is scanned for vulnerabilities utilizing various methods by Vanderbilt University prior to deployment of the software or updates. Third party vulnerability testers scan and report REDCap vulnerabilities and/or security flaws prior to releasing any updates to ensure ongoing security of the application. The Azure cloud solutions information/data is encrypted at rest and when transmitted for security purposes. The application provides access and account management features that provide security for the application. For example,

- Password requirements include: 9+ characters that are upper/lower case and numeric composition. The password expires after 60 days, and the maximum login attempts before lockout are 5 attempts (lockout time is 15 minutes).
- The system automatically logs users out if no activity within 30 minutes time.
- If you have not logged in within 90 days' time the system automatically suspends your account *(A REDCap Administrator can reactivate the account as needed).*
- Browser auto-completion to fill in your REDCap login username/password is not available.
- The application employes a two-factor authentication required to log into the application.



## USER ROLES

Specific roles are assigned within each REDCap project which determine the level of user rights that are available to them in REDCap.

### ITSD System Administrators

The ITSD Systems Administrator is responsible for ensuring that the underlying server and cloud infrastructure is running efficiently so applications remain generally available and accessible. This includes keeping the server software and operating system patched and performing REDCap version upgrades, as required. ITSD has access to the entirety of the REDCap system to maintain the application within the cloud, but they do not interact directly with the data within the system as a part of their work.

### REDCap Administrators & CTF Data Team

A small group of specialized, ethically trained REDCap Administrators and the CTF Data Team can see all the information for database maintenance and data management purposes. The REDCap Administrators are responsible for ensuring that REDCap is generally available for use and the systems projects and data collection are created and maintained. The REDCap Administration team:

- Manages REDCap user access including provisioning/suspension of user accounts and password resets.
    - The REDCap Administration Team may add, delete or modify user access within a project if specific arrangements are made with the Project Owners.
- Manages or assist with individual project user rights and caseload (DAG) set up.
    - *Note: Individual access and removal requests for CRIS or CI site data collection projects need to be processed through CI site staff who will coordinate with the appropriate REDCap Administrator.*
- Removes duplicated or accidentally entered records, as needed.
- Provides REDCap user guidance/technical assistance through recorded or 1-on-1 training sessions.
- Specific contracted REDCap Administrators are responsible for creating, customizing and managing alignment of data collection systems and developing projects and custom modules (including custom reporting features, referral systems, and reminder windows).
- REDCap Administrators and the CTF Data Team are also utilized to analyze/arrange data and report findings for quality improvement, quality assurance, and evaluation purposes.

### Project Owner

The Project Owner is typically a program/agency that has an appointed Supervisor/Manager. If the program is participating in a CI sites data collection and/or CRIS then the Supervisor should communicate their needs to their respective CI Site Coordinator/Manager, as the CI site is the Project Owner and manager for their respective CI site projects.

For data collection projects, the home visiting Project Owner has access to Data Access Groups (DAGS) or "caseloads" and can create/remove DAGs as necessary except for the "unassigned" and "closed cases" DAG. Each home visitor should have their own DAG in the system alongside other DAGs (caseloads/files). Program Project Owners are expected to assign/reassign families to specific DAGs in the system, as changes occur.

Project Owners should be marked to see all records/DAGs in their individual project in the DAG section including in the DAG switcher. Individual home visitors should be set to either see their own DAG and records (families assigned) only in the DAG assignment and DAG switcher OR it is an option for them to see more than one DAG in the DAG switcher, if necessary. The daily maintenance and data entry management of that project is fully the responsibility of the program Project Owner and not the REDCap Support Team.

### Other REDcap Users

REDCap users may have access to different functions in REDCap depending on their user role (see above). Program staff typically are entering or reviewing data and are responsible for case management activities. CTF grant managers/staff may have user rights within projects only to run aggregate reports and are unable to see individual level data in REDCap.

## USER ACCESS

### Prerequisites for CTF REDCap Access

- CTF REDCap Administrators, CTF Data Team and ITSD Administrators
- State personnel overseeing CTF program grants utilizing CTF REDCap
- Current staff from a program that is funded by CTF grants and/or participating in a collective impact site.
- Collective Impact site staff

### Providing User Accounts/Access

Users need to gain access to the REDCap system prior to accessing projects. The Project Owner will need to make a request to a REDCap Administrator (that includes the users name and email address) if personnel need access to REDCap, a specific REDCap project, and specific custom features such as the reporting feature or Coordinated Referral and Intake Systems (CRIS).

The user requesting an account will receive an account creation email containing links to establish a password. After the user has access to REDCap, Administrators or CI Site staff will need to add that user to any associated projects. Project access can be time-limited for users upon the request of the Project Owner.

### Revoking User Project Access

User accounts may be suspended by a Redcap Administrator. A user account may be revoked if:

• The user leaves the program and/or the Project Owners organization or the Project Owner or the sponsor requests the suspension of the user account.
• Automatically if no log ins have occurred within the last 90 days.
• The user is adjudged to have misused the system.

The content created by the user is not deleted and will be accessible after the user no longer has access to REDCap or associated projects. Programs are required to notify a REDCap Administrator when an employee no longer needs access to CTF REDCap.

## Informed Consent & Data Retention

Program participants are informed about and sign consent forms for their data to be contained within REDCap when enrolling in services. Inactive or suspended projects will be retained in the system for historical data reference purposes. If a program should end, or no longer be contracted with CTF, the Project Owner(s) will continue to have access to historical data but will not be able to enter new data. Information obtained through REDCap is securely stored and retained for long-term data analysis and reporting purposes.

## User Support

- User support for REDCap is provided by CTF REDCap Administrators. Users should address all questions concerning REDCap functionality and user accounts to the respective Project Owner *(Program Supervisor or CI Site Coordinator/Manager*). If the owner is unable to address an issue, the question can be forwarded to a CTF REDCap Administrator using the CTF REDCap Support Email: redcap@oa.mo.gov.
- There is no user cost associated with the REDCap application.
- REDCap applications are best utilized on a Chrome browser for optimal performance.
- ITSD Administrators can report to Vanderbilt if there are base level issues with the REDCap application although any concerns should be routed through a REDCap Administrator.

## External Module Management

Modules can extend REDCap's current functionality and can also provide customizations and enhancements for REDCap's existing behavior and appearance at the system or project level. Please be aware that External Modules are not part of atypical REDCap software but instead are add-on packages that, in most cases, have been created by software developers. A REDCap Administrator may enable of modify any module that has been installed in REDCap for a specific project. *Note: Project owners/users will not be able to enable or disable modules.*

Any issues relating to external modules including CRIS, the custom reporting feature, case management, the pop-up window or view schedule should be communicated to the REDCap Administrator assigned to system set-up/design. If participating in a CI site, issues with these modules needs to be communicated to the CI site first and then the CI site will reach out to the REDCap Administrator.

## REDCap Application Updates

Vanderbilt University makes REDCap updates available on a weekly basis that include, at minimum, bug fixes. ITSD accepts and initiates Vanderbilt updates to the REDCap instances on a 6-month cadence to keep within the state policy of maintaining updated versions of software. REDCap Administrators may make minor improvements to REDCap and individual projects that are rolled out as needed. If major improvements are needed, they would be scheduled with end users by REDCap Administrators. ITSD typically has a 3-day lead time for scheduled maintenance to the Azure cloud; but these updates typically do not impact end users or create down time of the application.

Loss of availability of the application or information loss is not expected. However, disaster recovery plans are in place and practice drills are conducted bi-yearly. Data backups are taken every hour and retained for 30-days to ensure availability of backups in case recovery is needed.

## System Audits

REDCap services may be audited for proper service and use. This is to ensure that projects are positioned in the correct version of the application. Although it's not common, as a result of a project review REDCap Administrators may be advised to migrate a project from one version to another. Administrators perform these operational audits as resources permit. REDCap also provides audit trails or "logging" for tracking data entry/changes and user activity within a project. These audit trails are available to view by Project Owners and REDCap Administrators. REDCap Administrators will periodically review REDCap user accounts and remove suspended accounts from the system.

## Notice – External Media

Missouri Children's Trust Fund has a legal and ethical responsibility to maintain the confidentiality, privacy and security of all information including family records created in REDCap. The purpose of this statement is to ensure appropriate safeguards against the loss; theft; and unauthorized access, use, disclosure, alteration or destruction of such information. Therefore, any information stored in REDCap cannot be downloaded onto any media external to your device that would allow for the physical removal or transport of such information (including, but not limited to, USB drives, External Hard Drives, etc.). The contracting program using REDCap shall use measures, and implement procedures, that do not allow these external media devices to be used for REDCap data including the contracting organization blocking or disabling external media systems and devices within their environment that interact with REDCap.

## CTF CONTACTS

**REDCap Administrator** (REDCap Questions or Requests): **redcap@oa.mo.gov.**

**CTF Grant Management & Privacy Officer** (Questions related to Grant Requirements, Reporting of Data Breaches or General CTF policies/practices): **ctf@oa.mo.gov**

**CTF Invoicing** (Invoice Submission and Questions Related to Invoicing/Billing): **ctf.invoices@oa.mo.gov**