Arizona State University

REDCap Policy and Usage Guidelines

Version:	1.0
Author:	REDCap Admin Group
Issued:	11/2022
Next Review:	11/2023

Overview of REDCap

REDCap (Research Electronic Data Capture) is a secure web application for building and managing online surveys and databases. This document is for the development of policies and procedures relating to the hosting and administration of the two REDCap versions managed jointly by the College of Health Solutions and Knowledge Enterprise.

Product instances

There are two instances of REDCap hosted by ASU;

Enterprise REDCap is hosted on-site by Research Computing: https://redcap.rc.asu.edu

HIPAA REDCap is hosted on Google Cloud Platform and managed by ASU personnel: https://esr.asu.edu/

Enterprise Instance

Enterprise REDCap is approved by the Research Technology Office for the collection of non-HIPAA research data. Enterprise REDCap is available to all ASU researchers and their collaborators, including faculty/staff from other institutions and companies. Enterprise REDCap follows a standard update schedule with weekly bug fixes (if needed), monthly minor improvements and changes, semi-annual major improvements, features, or modules.

HIPAA Instance

HIPAA-REDCap is approved by the Research Technology Office for the collection of HIPAA and “HIPAA-like” data. Sensitive data (data with the potential to harm survey participants if not sufficiently protected) requires additional management controls to ensure the data are properly protected. HIPAA-REDCap is hosted in a secure, private-cloud environment. Researchers wishing to use HIPAA-REDCap are expected to have had the IRB request approved prior to initiating projects in this system.

System security

REDCap security

Much of the security surrounding REDCap is dependent upon the IT infrastructure and environment in which REDCap has been installed. This includes the web server and database server, the communication between those two servers, and the communication of the web server with the REDCap end-user. The ASU Research Technology Office is responsible for the technical administration of both ASU REDCap installations

HIPAA REDCap security

HIPAA-REDCap is approved by the Research Technology Office for the collection of HIPAA (health/treatment data) and “HIPAA-like” data (with the potential to harm study participants if not sufficiently protected). These data require additional management controls to ensure the data are properly protected. HIPAA-REDCap is hosted in a secure, private-cloud environment and researchers wishing to use HIPAA-REDCap will require approvals from the Institutional Review Board (IRB) prior to initiating projects in this system.

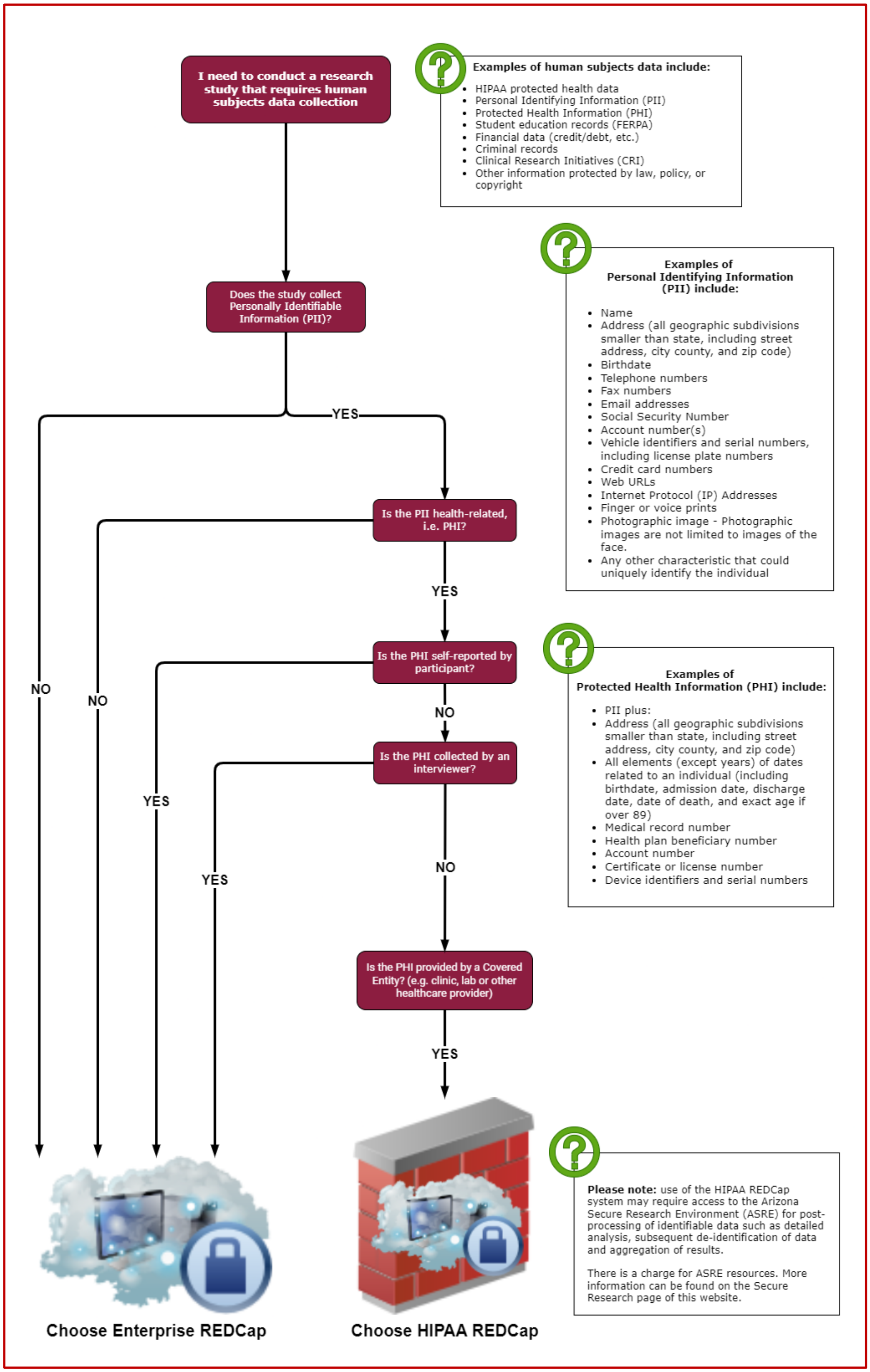
Regulatory compliance

ASU’s REDCap HIPAA instance has the necessary physical and operational security in place to meet or exceed Federal and State security and privacy regulations for data transmission and storage. This includes 21CFR Part 11, HIPAA, and FISMA. Project data can only be accessed by users who are given access rights from the Project Owner/Administrator. Project owners are fully responsible for data access.

Once data has been collected, a secure environment will be needed to preserve the collected data such as the Arizona Secure Research Environment (ASRE).

If you collect personal data of people in the European Union (EU), you are required to comply with GDPR (General Data Protection Regulation). The GDPR requires organizations to keep data secure and gives individuals more control over how their data is used. ASU’s REDCap HIPAA instance meets the requirements for compliance with GDPR.

Choosing which version to use



I need to conduct a research study that requires human subjects data collection
Does the study collect Personally Identifiable Information (PII)?
YES
NO
Is the PII health-related, i.e. PHI?
YES
NO
Is the PHI self-reported by participant?
YES
NO
Is the PHI collected by an interviewer?
YES
NO
Is the PHI provided by a Covered Entity? (e.g. clinic, lab or other healthcare provider)
YES
Choose Enterprise REDCap
Choose HIPAA REDCap

Examples of human subjects data include:

- HIPAA protected health data
- Personal Identifying Information (PII)
- Protected Health Information (PHI)
- Student education records (FERPA)
- Financial data (credit/debt, etc.)
- Criminal records
- Clinical Research Initiatives (CRI)
- Other information protected by law, policy, or copyright

Examples of Personal Identifying Information (PII) include:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- Birthdate
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security Number
- Account number(s)
- Vehicle identifiers and serial numbers, including license plate numbers
- Credit card numbers
- Web URLs
- Internet Protocol (IP) Addresses
- Finger or voice prints
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

Examples of Protected Health Information (PHI) include:

- PII plus:
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Device identifiers and serial numbers

Please note: use of the HIPAA REDCap system may require access to the Arizona Secure Research Environment (ASRE) for post-processing of identifiable data such as detailed analysis, subsequent de-identification of data and aggregation of results.

There is a charge for ASRE resources. More information can be found on the Secure Research page of this website.

User roles

Product administrators

The product administrators are responsible for ensuring that the REDCap service is generally available for use. The administration team:

- Monitors product availability
- Performs version upgrades, as required
- Provides user guidance in the form of:
  - Training
  - Office hours
  - Forum responses via product chat channel
- Manages user access including provisioning and suspension of user accounts

The REDCap Administration Team does not add, delete or modify user access within a project unless specific arrangements are approved by the team. Managing user access is the responsibility of the Project Owner (e.g., principal investigator, designated project coordinator/manager, or postdoctoral scholar).

System administrators

The systems administrator is responsible for ensuring that the underlying server infrastructure is running efficiently so that the applications remain generally available and accessible. This includes keeping the server software and operating system patched.

Project owner

ASU faculty and staff have the ability to create their own REDCap projects. Students and non-ASU personnel needing access to a REDCap project will need to be added by the project owner (typically the PI, Lab Manager, Program Manager) who administers the REDCap projects associated with the research. By default, the project owner has access to the User Rights module and can add users and enable/disable project or module access as needed. If a project owner adds a user to the project with User Rights access, that individual will also be able to manage user access. REDCap is designed so that the project owner has full access to most aspects of a REDCap Project. The daily maintenance and management of that project is fully the responsibility of the project owner and not the REDCap Support Team.

REDCap user

Any ASU faculty, student, or staff member can request an enterprise REDCap account. Student accounts must be sponsored by a Principal Investigator (ASU faculty or researcher). To accommodate a research collaborator that is external to ASU, an ASU faculty or staff member may grant user access to REDCap projects. External collaborators may have restrictions on access to specific components of a project. Please review User Rights information in each instance of REDCap offered at ASU.

User access

Prerequisites for REDCap access

Enterprise REDCap

- Certified human subjects training (ASU or external institutional equivalent)
- ASU Information Security Training (or external institutional equivalent).

HIPAA REDCap

- As above, plus certified HIPAA training (ASU or external institutional equivalent)

Providing user accounts

REDCap support organizes users into a hierarchical structure. This approach is beneficial as it improves system security by allowing research teams to extend access for users still involved in a project. Users need to be entered into the REDCap system prior to accessing or creating any projects. The user requesting an account will receive an account creation email containing links to establish a password.

Providing project access

For an individual to be added to a REDCap project they must first be provided with a user account. After the user has access to the REDCap system, the project owner will need to add that user to any projects for which they are not the project creator/owner.

Revoking user project access

User accounts will be suspended on a predetermined date based on the user policy unless a user requests an account extension prior to the suspension. The content created by the user is not deleted and will be accessible after the account is extended or re-activated.

A user account may be revoked if:

- The user leaves the university
- The project reaches an end date
- The project owner or the sponsor requests the suspension of the user account
- The user is adjudged to have misused the system as per ACD125.

Renewing project access

Sponsors may request an extension of a user’s access privileges to a project through the user rights portion of the project. Users may also request an extension, but sponsors will still be required to confirm any request. When creating user access, the project owner can set access permissions up to one year per user.

Data retention

Inactive or suspended projects will be retained for a minimum of three years. During the retention period research personnel will be able to work with the REDCap support team to export the data in a form that meets the relevant security requirements.

Additional user roles

Principal Investigators (PIs): PIs usually have an oversight role in REDCap, but this depends on the faculty’s research team structure. PIs have the responsibility to ensure their research team has appropriate access to the system and that personnel and students are appropriately removed from projects when their role has expired. PIs must be sponsors of non-ASU collaborators, research staff, and students or delegate this responsibility to a Project Coordinator (PC). If you are the PI, you or the PC will be the sponsor for your research team. You can manage your team account in your Sponsor Dashboard.

Project coordinators (PCs): PCs oversee the design and implementation of REDCap projects and typically oversee student and faculty (ASU and non-ASU) collaborations. If you are the PC, you will be the sponsor for your research team if determined by the PI. You can manage your team account in your Sponsor Dashboard.

Project staff: project staff conduct special activities, usually in conjunction with the PCs. Typical responsibilities include interacting with participants to obtain consent or study data or customizing REDCap project pages to improve the participant or researcher interface, or developing specialized code to allow REDCap to interact with other programs (API). Project staff can work alongside the PCs to oversee students as well. Your PI or PC will be able to manage your account and project access.

Research assistants and/or students: RAs and students are typically involved with consenting or collecting participant data as well as similar activities as project staff. Your PI or PC will be able to manage your account and project access.

Non-ASU personnel: non-ASU personnel includes any faculty, staff, or student that is not in the ASU system, such as a non-ASU consultant, faculty from another institution collaborating on the project, or students/staff from a different institution for a multi-site project. Your PI or PC will be able to manage your account and project access.

User support

User support for this product is provided by the College of Health Solutions Biostats Core and Knowledge Enterprise.

Users should address all questions concerning their REDCap project and user accounts to the project owner. If the owner is unable to address a collaborator's issue, the question can be forwarded to the REDCap project administrator via the link in project settings.

External module management

Enterprise REDCap modules

External Modules are individual packages of software that can be downloaded and installed by a REDCap administrator. 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.

A REDCap administrator may enable any module that has been installed in REDCap for a specific project. Administrators or users with Project Setup/Design privileges can modify the configuration of any module after the module has been enabled by an administrator. Some configuration settings might be required to be set. Note: Normal project users will not be able to enable or disable modules.

Please be aware that External Modules are not part of the REDCap software but instead are add-on packages that, in most cases, have been created by software developers at other REDCap institutions. Be aware that the entire risk as to the quality and performance of the module as it is used in your REDCap project is borne by you and your local REDCap administrator.

HIPAA REDCap modules

A user requiring the use of an external module in the HIPAA REDCap may request that the module be activated in the system through the support team. The module will be reviewed and tested prior to inclusion to ensure the module meets ASU's security requirements and does not compromise existing system function

Application updates

Vanderbilt University provides REDCap updates on a weekly basis that include, at minimum, bug fixes. Minor improvements are rolled out monthly and major improvements are implemented bi-annually.

System audits

Both REDCap services may be audited for proper service and use. This is to ensure that projects are positioned in the correct version of the product. As a result of a project review, project owners may be advised to migrate a project from one version to another.

ASU REDCap administrators perform these operational audits as resources permit for both enterprise and HIPAA instances. REDCap also provides audit trails for tracking data manipulation and user activity within a project. These audit trails are available to project owners and system administrators.