REDCap at UWI Cave Hill

Operations & Maintenance Handover Guide

Ian R Hambleton

18 Jan 2026

Table of contents

1 REDCap at UWI Cave Hill

REDCap Operations Handover Runbook

1.1 What this guide is

- Audience:
- Scope:

1.2 What this guide is not

- REDCap user training:
- Instrument design tutorials:
- Statistical/analysis guidance:

1.3 Service ownership and responsibilities

- Service owner:
- Technical owner:
- Front-end support lead:
- Back-end support lead:
- Escalation contact(s):

1.4 Where to find official REDCap training and documentation

- Link(s) to official resources:
- Local policy links:

1.5 How to use this runbook

- Common workflows:
- Where to log changes/incidents:

1.6 Change log

- YYYY-MM-DD — summary — author

2 REDCap Service Overview

A Summary of the Cave Hill REDCap Data Platform

This document describes the REDCap service operated for The University of the West Indies (UWI), Cave Hill, and the institutional responsibilities associated with its operation.

REDCap is a secure, web-based data capture platform developed and licensed by Vanderbilt University under a non-profit end-user licence agreement. UWI participates in the REDCap Consortium and operates REDCap in accordance with Vanderbilt's licensing terms, governance expectations, and community standards.

The UWI REDCap instance has been project-managed by the CaribData project and hosted on dedicated infrastructure provided by HIPAA-Vault .

2.1 What the service provides

The service enables UWI researchers and operational teams to:

- build and manage electronic data collection instruments;
- deploy surveys and forms for online and offline data capture;
- manage role-based access to projects and data;
- maintain full audit trails of data entry, modification, and export;
- export data to standard statistical packages;
- support longitudinal, survey-based, and operational projects.

These capabilities align with Vanderbilt's definition of REDCap as a metadata-driven platform designed to support secure research and operational data workflows at scale.

2.2 Hosting and infrastructure responsibilities

The REDCap application is hosted on dedicated servers managed by HIPAA-Vault under a commercial hosting and support agreement with UWI. Under this arrangement, HIPAA-Vault is responsible for:

- server provisioning and maintenance;
- operating system patching and upgrades;
- managed firewalls and network security;
- infrastructure-level monitoring and incident response;
- data centre security and availability guarantees.

HIPAA-Vault provides infrastructure services only. Responsibility for REDCap configuration, user management, governance, and compliance remains with UWI and its designated administrators.

2.3 Licensing and support boundaries

Vanderbilt University licenses REDCap software to UWI but does not provide hosting, operational support, or system administration services. Participation in the REDCap Consortium grants access to:

- the REDCap software;
- documentation and community resources;
- training materials and videos;
- peer support via the REDCap community.

All operational responsibility for this instance lies with UWI and its service partners. This distinction is critical when planning support, staffing, and continuity arrangements.

2.4 Service ownership

The REDCap service should be treated as an institutional digital service rather than a project-specific tool. This implies clear ownership for:

- policy and governance;
- funding and contracts;
- continuity planning;
- compliance with data protection and research ethics requirements.

Day-to-day administration and user support are delegated functions within this broader ownership framework.

Part I

Front-end Ops

3 REDCap Administration

Administration of users and projects

This section describes how user access and REDCap projects are administered for the University of the West Indies (UWI) REDCap service.

Administrative functions are exercised on behalf of the institution. They exist to ensure that REDCap is used appropriately, securely, and in line with licensing, governance, and data protection requirements.

3.1 Administrative role and scope

REDCap administrators (sometimes referred to as "superusers") are responsible for the configuration and oversight of the REDCap system itself. This role is distinct from that of project managers, who control activity within individual projects.

Administrative responsibilities include user *account management*, *approval of projects and elevated functions*, and *oversight of the project lifecycle*.

3.2 User account management

All user accounts are created and managed centrally. Requests for access are submitted via the designated REDCap support email and should clearly state:

- the user's affiliation,
- intended use of REDCap,
- whether they are joining an existing project or proposing a new one.

Administrators are responsible for ensuring that:

- accounts are issued only to identifiable individuals;
- accounts use appropriate institutional or approved email addresses;
- access is removed or suspended promptly when affiliation ends;

- account expiration dates are used where appropriate.

Shared or generic accounts are not permitted, as they undermine auditability and accountability.

3.3 Project creation and approval

New projects require administrative approval before they are created or activated. This step ensures that projects are correctly classified (for example, research versus operational use) and that basic governance expectations are understood by project owners.

Administrators should confirm that project managers understand their responsibilities for user management, data handling, and compliance within their projects.

3.4 Project lifecycle control

Administrators control key transitions in the project lifecycle, including:

- approval of project creation;
- moving projects from development to production;
- approval of project copies;
- archiving of completed or inactive projects;
- deletion of projects, where permitted by institutional policy.

Project deletion is irreversible and should only occur after confirming data retention and governance requirements.

3.5 Elevated permissions and features

Certain REDCap functions require explicit administrative approval because they introduce additional risk or system-level impact. These include *API access*, *activation of external modules*, *enabling mobile data collection*, and approval of *advanced project features*.

Administrative decisions should follow the principle of least privilege and be documented where appropriate.

3.6 Oversight and routine checks

As part of normal operations, administrators should periodically review user accounts, project status, and system logs to identify inactive users, stalled projects, or unusual patterns of data export or access.

These checks support institutional accountability and reduce the risk of unnoticed misuse.

4 Support Requests

User support and operational support model

This section describes how support for the UWI REDCap service is provided, including how requests are handled, triaged, and escalated.

The support model reflects the boundaries between REDCap software ownership (Vanderbilt University), local service operation (UWI and CaribData), and infrastructure hosting (HIPAA Vault).

4.1 Purpose of local support

Local REDCap support exists to enable effective and appropriate use of the platform. It focuses on helping users apply REDCap functionality correctly rather than providing research design, statistical, or methodological advice.

Support activities complement, rather than replace, the extensive documentation and training materials provided by Vanderbilt University.

4.2 Types of support requests

Support requests generally fall into three broad categories.

4.2.1 Account and access support

These requests relate to user authentication and access, including:

- password resets;
- account expiration or reactivation;
- account suspension or deletion;
- account creation and affiliation changes.

These are the most common requests and are usually resolved through the REDCap Control Center.

4.2.2 Project and permissions support

These requests relate to project-level governance and configuration, including:

- approval of new projects;
- moving projects from development to production;
- approving project copies or deletions;
- managing user permissions and roles;
- approving API access or external modules.

These requests require judgement, as they often have governance or data protection implications.

4.2.3 Technical and system-related support

A smaller number of requests involve more technical issues, such as:

- survey behaviour that appears inconsistent or broken;
- errors triggered by server security rules;
- mobile app synchronisation issues;
- issues following REDCap version upgrades.

Where issues relate to infrastructure or server configuration, they are escalated to the hosting provider.

4.3 Common administrative support procedures

This section documents the most frequent administrative actions carried out by REDCap administrators in response to user support requests.

Procedures assume administrator-level access and familiarity with REDCap terminology. They focus on what to do and what to check, rather than UI walkthroughs that may change between REDCap versions.

4.3.1 Resetting a user password

Password resets are required when users cannot log in or did not receive their original account email.

Breadcrumb
`Control Center → Browse Users → (select user) → Reset password / Send password reset email`

Procedure

1. Locate the user account.
2. Confirm the account is active and the email address is correct.
3. Trigger a password reset or reset email.
4. Advise the user to check inbox and spam or quarantine folders.

If the user does not receive the email, verify outbound email configuration and consider institutional mail filtering.

4.3.2 Extending or resetting a user account expiration date

User accounts may expire automatically based on institutional or administrative policy. Expired accounts prevent login but retain audit history.

Breadcrumb
`Control Center → Browse Users → (select user) → Edit user settings → Account expiration`

Procedure

1. Locate the user account.
2. Edit the expiration date or remove it where appropriate.
3. Save changes and confirm the account is active.

Expiration dates should be applied deliberately and reviewed periodically.

4.3.3 Suspending or reactivating a user account

Accounts may be suspended due to staff changes, temporary inactivity, or security concerns.

Breadcrumb
`Control Center → Browse Users → (select user) → Suspend user / Reactivate user`

Procedure

1. Change the account status as required.
2. Confirm the updated status has taken effect.

Suspension is reversible and preserves audit history. It is preferred to deletion in most cases.

4.3.4 Resending account creation emails

Users occasionally report not receiving their initial account creation email.

Breadcrumb
`Control Center → Browse Users → (select user) → Resend account email`

Procedure

1. Confirm the account exists and is active.
2. Verify the email address.
3. Resend the account or password email.
4. Ask the user to check spam or quarantine folders.

Repeated failures usually indicate email filtering rather than a REDCap issue.

4.3.5 Creating a new user account

New accounts are created centrally to ensure traceability and appropriate use.

Breadcrumb
`Control Center → Add New User`

Procedure

1. Enter the user's name, email address, and institutional affiliation.
2. Set an expiration date if required.
3. Save the account and confirm the email notification is sent.

Shared or generic accounts should not be created.

4.3.6 Approving project creation

Requests for new projects require administrative approval.

Breadcrumb
`Control Center → Project requests / Pending project requests → Review request`

Procedure

1. Review the stated project purpose.
2. Confirm whether surveys, public links, API access, or sensitive data are involved.
3. Approve or reject the request accordingly.

Approval implies that baseline governance expectations have been communicated.

4.3.7 Moving a project to production

Projects must be reviewed before moving from development to production.

Breadcrumb (project initiates)
`Project → Setup → Move project to Production`

Breadcrumb (administrator approves)
`Control Center → Pending requests / Production move requests → Approve`

Procedure

1. Confirm testing is complete.
2. Verify that instruments and settings are stable.
3. Approve the move and document the action if non-routine.

Production status has audit and governance implications and should not be reversed lightly.

4.3.8 Approving API tokens

API access enables automated data exchange and introduces additional risk.

Breadcrumb (project initiates)
`Project → Applications → API → Request token`

Breadcrumb (administrator approves)
`Control Center → API token requests → Approve`

Procedure

1. Review the justification for API access.
2. Confirm the requester understands scope and security responsibilities.

3. Approve the token if appropriate.
4. Encourage least-privilege use and periodic review.

4.3.9 Activating external modules

External modules extend REDCap functionality but may affect system behaviour.

Breadcrumb (system level)
`Control Center → External Modules → Manage modules`

Breadcrumb (project level)
`Project → External Modules → Enable module`

Procedure

1. Review the purpose and documentation of the module.
2. Confirm compatibility with the current REDCap version.
3. Assess performance and security implications.
4. Enable and monitor usage.

Not all modules are appropriate for all installations.

4.4 REDCap Control Center: administrator orientation

The REDCap Control Center is the primary workspace for system administrators. It provides access to system-wide settings, approvals, and oversight tools.

Administrators should understand the structure of the Control Center rather than memorising individual menu items.

4.4.1 Core administrative areas

- **User management**
  `Control Center → Browse Users`
  `Control Center → Add New User`
- **Project governance and approvals**
  `Control Center → Project requests / Pending requests`
- **System configuration**
  `Control Center → System Configuration / General Configuration`

- **Email configuration**
  `Control Center → Email Configuration`
- **External modules**
  `Control Center → External Modules`
- **Logs and audit support**
  `Control Center → Logging / System logs`

4.4.2 Administrative mindset

The Control Center is intentionally powerful. Most changes made here affect all users and projects.

Administrators should act conservatively, document non-routine actions, and favour reversible changes wherever possible.

5 REDCap Emails

Email use, configuration, and governance

Email is a fundamental dependency for REDCap, enabling user notifications, survey distribution, and automated alerts. At the same time, it presents governance and security risks that require careful management.

This section documents how email is used within the UWI REDCap service and the principles governing its configuration.

5.1 Role of email in REDCap

REDCap uses email to support core functions such as account creation, password management, survey invitations, reminders, and Alerts & Notifications configured within projects.

While email delivery is essential for normal operation, REDCap does not require a fixed or branded sender address, provided that outbound email routing is correctly configured.

5.2 Universal FROM address considerations

A universal FROM address can provide consistency and simplify mail routing, but it also introduces a dependency on the continued availability of the associated domain and mailbox.

Where a universal FROM address is used, it should be institutionally owned, monitored, and reviewed periodically. Personal or externally funded mailboxes should be avoided.

Changes to the FROM address or SMTP configuration should be treated as service-level changes and tested accordingly.

The REDCap universal email address is: redcap@cavehill.uwi.edu

5.3 Governance and risk management

Email should always be treated as an insecure communication channel. As such, sensitive personal or health data must never be included in email bodies or attachments.

Project-level alerts and survey invitations should reference records using identifiers rather than names, and project teams should be reminded of these constraints during project approval.

These practices align with both Vanderbilt guidance and the security assumptions of the hosting environment.

5.4 Testing and change management

Any change to email configuration should be followed by systematic testing, including account notifications, survey invitations, and alerts from a test project.

Email issues are often invisible until users report failures, so short-term monitoring after changes is essential to ensure continuity of service.

Part II

Back-end Ops

6 System Maintenance

System maintenance and upgrades

This section describes how routine maintenance and upgrades are managed for the UWI REDCap service.

The REDCap application runs on a dedicated Linux virtual machine hosted by HIPAA Vault. This is a fixed-capacity, managed environment. Maintenance activities therefore require coordination between REDCap administrators and the hosting provider and should follow predictable, documented procedures.

6.1 Responsibility boundaries

System maintenance spans multiple layers, each with a different owner.

HIPAA Vault is responsible for the underlying infrastructure, including server hardware, operating system patching, firewall management, and network security.

UWI, through its REDCap administrators, is responsible for the REDCap application itself, including configuration, upgrades, testing, and user communication.

Vanderbilt University provides the REDCap software and documentation but does not perform upgrades, host the system, or provide operational support.

Understanding these boundaries is essential when planning or responding to maintenance activities.

6.2 Routine system checks

Administrators should perform periodic checks to confirm that REDCap is functioning as expected. These checks are typically lightweight and include verifying user access, confirming that surveys and alerts are running, and reviewing system messages or logs for warnings.

Routine checks help detect emerging issues early, particularly in a fixed-resource environment where gradual changes in usage can affect performance.

6.3 REDCap version upgrades

REDCap releases frequent updates, including feature enhancements, bug fixes, and occasional security patches. UWI policy is to keep the system reasonably up to date while avoiding unnecessary disruption to users.

Upgrades should be informed by Vanderbilt release notes and changelogs. Not all releases require immediate action, but security-related updates should be prioritised.

6.4 Pre-upgrade preparation

Before any upgrade, administrators should coordinate with HIPAA Vault to ensure a recent server snapshot is available. This provides a rollback option if the upgrade fails or introduces unexpected behaviour.

Where possible, new REDCap versions should be tested on a development or staging environment before being applied to the production system. Testing should focus on core functionality, authentication, surveys, alerts, and any enabled external modules.

Administrators should also notify users in advance if an upgrade is expected to cause service interruption.

6.5 Performing upgrades

REDCap upgrades are typically applied by administrators with appropriate access to the server environment. In some cases, HIPAA Vault may assist with server-level changes required to support the upgrade, such as PHP or database adjustments.

Upgrades should be scheduled during periods of low usage where possible and should be followed immediately by basic functional checks.

6.6 Post-upgrade validation

After an upgrade, administrators should confirm that:

- users can log in normally;
- projects open and behave as expected;
- surveys and alerts function correctly;
- no unexpected errors appear in logs or system messages.

Any issues should be investigated promptly. If necessary, administrators may revert to the pre-upgrade snapshot in coordination with HIPAA Vault.

6.7 Unplanned maintenance and incidents

Occasionally, unplanned maintenance may be required in response to security vulnerabilities, system instability, or hosting issues.

In such cases, the priority is service stability and data protection. Administrators should document the issue, actions taken, and outcomes, and communicate clearly with users if service availability is affected.

7 System Backups

Backups, recovery, and data continuity

This section describes how backups and data recovery are handled for the UWI REDCap service.

Backups are a shared responsibility across infrastructure, application, and project levels. No single mechanism provides complete protection against data loss, and it is important to understand what each layer does — and does not — provide.

7.1 Infrastructure-level backups

HIPAA Vault provides infrastructure-level backups and snapshots as part of its hosting service. These backups are designed to support disaster recovery in the event of server failure, corruption, or major incidents.

Infrastructure backups typically capture the state of the server at a point in time. They are not intended for routine data retrieval or fine-grained restoration of individual records or projects.

Retention periods and recovery windows are finite and governed by the hosting agreement. In the event of contract termination or prolonged service disruption, data availability is time-limited.

7.2 Application-level safeguards in REDCap

REDCap includes built-in safeguards that support data integrity, including audit logs, change tracking, and controlled data exports.

These features support transparency and traceability but do not replace backups. They are most useful for understanding what changed and when, rather than for restoring lost data.

7.3 Project-level data exports

Project teams are responsible for exporting and retaining copies of their own data in accordance with institutional policies and research governance requirements.

Regular data exports are the most reliable way for projects to ensure continuity, particularly for long-running studies or operational systems. Exports should be stored securely outside the REDCap environment.

Administrators should remind project owners that REDCap is a live system, not a long-term archival solution.

7.4 Recovery scenarios

Different types of data loss require different responses.

In the case of accidental record deletion or user error, recovery may not be possible unless the project team has retained recent exports.

In the case of system-level failure, administrators may work with HIPAA Vault to restore the server from a recent snapshot. This process restores the system to a previous state and may result in loss of recent changes.

Clear communication with affected users is essential in all recovery scenarios.

7.5 Testing and assurance

While full restoration tests are rare, administrators should periodically review backup arrangements with the hosting provider and confirm that snapshots are being taken as expected.

Understanding backup scope and limitations is a key part of service continuity planning.

7.6 End-of-service considerations

If the REDCap service is migrated, decommissioned, or transferred to another institutional owner, data retrieval timelines become critical.

Project teams should be given clear notice and sufficient time to export their data. After hosting services are terminated, unretrieved data may become permanently inaccessible.

Part III

Risk and continuity

8 System Security

Security model and risk management

This section describes the security posture of the UWI REDCap service and the shared responsibilities that underpin it.

Security in REDCap is not a single control or technology. It is a layered model that combines infrastructure protections, application-level safeguards, and institutional governance. Weakness at any one layer can undermine the others.

8.1 Layered security model

The UWI REDCap service operates within three distinct security layers.

At the infrastructure layer, HIPAA Vault provides physical data centre security, operating system hardening, managed firewalls, encrypted network connections, and continuous monitoring. This layer protects the server environment but does not control how REDCap is configured or used.

HIPAA Vault has GDPR certification.

At the application layer, REDCap provides role-based access control, audit logging, data validation, and secure authentication mechanisms. These features govern how users interact with data but depend on correct configuration.

At the institutional layer, UWI defines who may use REDCap, for what purposes, and under what conditions. Policies, training, and administrative oversight sit at this layer and are critical to effective security.

8.2 Authentication and access control

Access to REDCap is granted through individual user accounts. Each account is tied to a specific person and email address and is subject to role-based permissions within projects.

Administrators are responsible for ensuring that access is appropriate, proportionate, and time-limited where necessary. Project managers are responsible for managing access within their own projects.

Shared accounts, excessive permissions, and dormant users represent security risks and should be actively avoided.

8.3 Data protection and privacy

REDCap is designed to support secure data capture, including for sensitive research and operational data. However, the platform does not absolve users or the institution of their data protection responsibilities.

Project teams are responsible for ensuring that their use of REDCap complies with applicable ethics approvals, data protection legislation, and institutional policies.

Administrators should pay particular attention to features that increase exposure risk, such as public surveys, API access, and external modules.

8.4 Email and indirect data exposure

Email is an essential but inherently insecure component of REDCap workflows. While email enables notifications and survey distribution, it should never be used to transmit sensitive data.

Administrators should ensure that project teams understand this limitation and design alerts and invitations accordingly. This is a recurring risk area and merits ongoing attention.

8.5 Incident awareness and response

Not all security incidents are technical breaches. Misconfigured permissions, accidental data exports, or inappropriate sharing can all constitute security events.

When a potential incident is identified, the priority is to contain risk, preserve evidence, and escalate appropriately within institutional governance structures. Documentation of incidents and responses supports learning and accountability.

8.6 Security as an ongoing process

Security is not static. Changes in usage patterns, staffing, or external threats can alter the risk profile of the service over time.

Regular review of user access, project configurations, and system behaviour helps ensure that security controls remain effective and proportionate.

9 Useful Checklists

Operational checklists and continuity aids

This section provides practical checklists to support continuity of the UWI REDCap service.

The aim is not to replace judgement, but to reduce reliance on memory during routine tasks, staff transitions, or stressful situations.

9.1 Routine operational checks

At regular intervals, administrators should confirm that the service is functioning as expected. This includes checking user access, reviewing recent support requests for patterns, and ensuring that system messages or warnings have not been overlooked.

These checks are especially important in a fixed-capacity hosting environment, where gradual increases in usage may have cumulative effects.

9.2 Pre-upgrade checklist

Before performing a REDCap upgrade, administrators should confirm that:

- the upgrade is justified by feature, bug-fix, or security needs;
- release notes have been reviewed;
- a recent server snapshot is available;
- users have been notified if disruption is expected;
- testing arrangements are in place where possible.

Skipping preparation increases the risk of avoidable service interruption.

9.3 Post-upgrade checklist

After an upgrade, administrators should verify that core functionality is intact. This includes login, project access, surveys, alerts, and any enabled external modules.

Unexpected behaviour should be investigated promptly, and rollback options considered if stability is compromised.

9.4 Incident response checklist

When something goes wrong, the immediate goals are to stabilise the system, protect data, and communicate clearly.

Administrators should identify whether the issue is user-related, application-level, or infrastructure-level, and escalate accordingly. Actions taken should be documented, even if the resolution is straightforward.

9.5 Staff transition and handover

REDCap continuity depends on more than documentation. When administrative responsibility changes, access credentials, vendor contacts, and institutional knowledge must be deliberately transferred.

This guide is intended to support that process, but it cannot replace structured handover and oversight.

9.6 Periodic review

At least annually, administrators should step back and review whether the service configuration, support model, and governance arrangements still reflect how REDCap is actually being used.

Quiet drift is a common source of operational risk. Periodic review helps bring assumptions back into line with reality.

Part IV

Appendices

10 Useful Templates

Reference templates and standard texts

This section provides standard text and lightweight templates used in the operation of the UWI REDCap service.

The intent is consistency, not bureaucracy. These templates should be adapted as needed, but deviations should be deliberate.

10.1 Standard service description

The following text may be used in institutional documentation, presentations, or onboarding materials:

"REDCap (Research Electronic Data Capture) is a secure, web-based software platform developed by Vanderbilt University and hosted for The University of the West Indies by CaribData. It is designed to support the collection and management of research and operational data through validated data capture, audit trails, and controlled data export."

10.2 Suggested REDCap citation text

For use in publications, reports, or methods sections:

"Data were collected and managed using REDCap electronic data capture tools hosted by CaribData for The University of the West Indies, Cave Hill."

Project teams should also include standard REDCap methodological citations as recommended by the REDCap Consortium.

10.3 User account request information

When requesting a new REDCap user account, the following information should be provided:

- Full name
- Email address
- Institutional affiliation
- Intended use of REDCap
- Whether the user will join an existing project or request approval for a new project

Providing complete information helps reduce delays in account creation.

10.4 Project request summary (informal)

When requesting approval for a new project, project leads should be prepared to describe:

- the purpose of the project (research, operational, teaching, etc.);
- the type of data to be collected;
- whether surveys or public links will be used;
- whether sensitive or personal data are involved.

This information supports appropriate governance without creating unnecessary administrative burden.

10.5 Change notification text (example)

The following text may be adapted when notifying users of planned maintenance or upgrades:

"A scheduled update to the UWI REDCap system will take place on [date/time]. Short service interruptions may occur during this period. Please ensure that critical work is saved in advance."

10.6 Incident notification text (example)

Where appropriate, the following wording may be used to communicate service issues:

"We are currently investigating an issue affecting the UWI REDCap service. Updates will be provided as more information becomes available."

11 External Links

Useful links and resources

12

This section provides links to authoritative external resources relevant to the UWI REDCap service.

Where possible, users and administrators should rely on these sources rather than informal guidance or third-party tutorials.

12.1 REDCap consortium and documentation

- REDCap Consortium home: https://projectredcap.org/
- Official documentation and resources: https://projectredcap.org/resources/
- How to cite REDCap: https://projectredcap.org/resources/citations/
- REDCap community (login required): https://redcap.vanderbilt.edu/community/

These are the primary sources for understanding REDCap functionality, updates, and recommended practices.

12.2 REDCap training materials

- Official training videos: https://projectredcap.org/resources/videos/

These videos provide structured introductions to REDCap concepts, project types, instrument design, and built-in applications. They are the preferred starting point for new users.

12.3 UWI REDCap service access

- REDCap login URL: https://caribdata.org/redcap/
- REDCap support contact: redcap@cavehill.uwi.edu

These are the authoritative access points for the UWI installation.

12.4 Hosting and infrastructure

- HIPAA Vault: https://www.hipaavault.com/

HIPAA Vault provides the hosting infrastructure for the UWI REDCap service. Contractual details and support interactions are managed institutionally.

12.5 Governance and compliance

Users should consult relevant institutional policies and ethics guidance applicable to their work, including data protection, research ethics, and information security policies.

REDCap is a tool; responsibility for compliant use rests with the institution and its users.