Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA



THE UNIVERSITY *of* EDINBURGH
Baillie Gifford Pandemic Science Hub

PSH_POL_RED_01:

REDCap System Validation Policy

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

Document Control Sheet

Revision History

Version	Revision Date	Reason for revision	Author	Signature and Date
1.0	**05Oct2026**	• **Initial Creation**	**Christopher White**	Signed by: Christopher White D2C419FC745D4B7... 04-Nov-2026 | 1

Document Review

Role	Organization	Name	Signature and Date
Data Manager	ECTU	Han Xiao	Signed by: Han Xiao 5CA0FE9348D54DA... 04-Nov-2026 | 15:

Document Approval

Role	Organization	Name	Signature and Date
QA Manager	ECTU	Tanya Tharakan	Signed by: Tanya Tharakan 3308878DBFF04BA... 04-Nov-2026 | 16:1
QA Manager	PSH	Kieran Burgess	Signed by: K Burgess D8FD9743965A4CD... 04-Nov-2026 | 16:0

This document is valid from the date of the final signature in the table above.

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

Table of Contents

1 Definitions 4
2 Purpose 5
3 Scope 6
4 Responsibilities 6
5 Validation Strategy 6
5.1 Detailed Strategies 6
5.2 Review and Maintenance 11
6 Relevant Documents and References 11

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

1 Definitions

Data Management groups:	Within this document, Data Management refers collectively to both the Pandemic Science Hub (PSH) and the Edinburgh Clinical Trials Unit (ECTU) Data Management teams and staff members (i.e., Data Managers) responsible for the execution of and recording of full system validation for their respective REDCap instances.
Server Manager:	The Server Manager is a representative from the University of Edinburgh's Central IS Services responsible for overseeing the management, maintenance, and recovery of the REDCap server. The Server Manager co-ordinates server-related tasks, including backup verification, restoration, and system availability testing
REDCap Consortium:	The REDCap Consortium is a collaborative network of REDCap administrators from numerous institutional partners across more than a hundred countries. Each institution maintains and supports its own REDCap system(s).
Regulatory and Software Validation Committee (RSVC):	The Regulatory and Software Validation Committee (RSVC) is a volunteer committee comprised of Vanderbilt University Medical Center employees and members of the REDCap Consortium. Its primary goal is to Identify core functions and develop feature tests. The RSVC creates and maintains resources, templates, and validation test scripts, specifically focusing on the core functionality of REDCap. These resources aid in the software validation process and provide guidance for meeting regulatory requirements, including those outlined in FDA's 21 CFR Part 11 (US Regulation) and ICH E6(R3).
VUMC:	Vanderbilt University Medical Center, the developer and provider for REDCap.
REDCap Development Life Cycle (Version Release Timeline):	REDCap follows a release cycle that includes Standard and Long-Term Support (LTS) releases. The LTS release is derived from the standard release and is supported explicitly with patches, without adding new features, for an extended period of 6 months. The RSVC perform validation based on Vanderbilt's 6-month LTS release schedule.
Installation Qualification (IQ):	Verifies that the Electronic Data Capture (i.e., REDCap) system has been properly installed in the local IT environment according to the vendor's specifications and institutional requirements (https://information-services.ed.ac.uk/about/policies-and-regulations/security-policies). It ensures that all required server configurations, and security settings are correctly implemented. **Includes:** • Verifying server setup (database, web server) • Confirming system security and permissions • Documenting installation and environment details • Can be completed both retrospectively and prior to system release
Operational Qualification (OQ):	Verifies that the core REDCap functionalities operate as intended under normal operating conditions. Ensures that features perform correctly and reliably within vendor requirements. **Includes:**

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

	• Leveraging (evidencing) the extensive work of the REDCap Consortium group RSVC • Regular (approximately 6-monthly with releases) reviews of updated documentation to ensure meets all groups requirements
Performance Qualification (PQ):	Verifies that REDCap meets the specific performance requirements at an individual research project or study level. It ensures that validated functionality is tested in unique configurations on a study-by-study basis. **Includes**: • Study-specific testing (e.g., branching logic, calculated fields, instruments etc.). • Adherence to internal SOPs and data management plans • Required completion and document sign-off before project release
Core features:	A subset of functions used to define the basic features required to use REDCap as an Electronic Data Capture (EDC) software.
'Dev' instance:	The 'Dev' instance refers to the REDCap environment accessed via URL: https://igmm-redcapdev.igmm.ed.ac.uk/. The 'Dev' instance acts as a testing and validation environment only, allowing the Server Manager to release software patches and updates and Data Management teams to conduct system update checks and validate configurations without impacting live study data or business activities. The ECTU and PSH REDCap Production (Live) instances (which host live study and trial data) are both clones of the 'Dev' instance. All instances are hosted by the University of Edinburgh servers. Access to the 'Dev' instance is restricted to authorised members of the Data Management groups, ensuring controlled and secure testing separate from production operations.

2 Purpose

The purpose of this policy is to describe and justify the approach and responsibilities of the Pandemic Science Hub (PSH) and Edinburgh Clinical Trials Units (ECTU) in fully validating a REDCap instance within the University of Edinburgh's IT environment.

System-level validation of EDC system is a requirement for regulated clinical trials, serving as a critical component in ensuring that REDCap functions reliably, securely, and compliantly. This includes validating the installation, configuration, and general operability of the software system, independent of, and including, individual study requirements. System-level validation encompasses IQ: confirming proper and compliant technical installation, OQ: verifying core REDCap features work as intended, and PQ: which is carried out independently for each study to validate study-specific requirements.

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

This policy supports institutional compliance with relevant UK regulations, including MHRA GxP guidelines and UK GDPR, ensuring data integrity, information security, and operational transparency.

3 Scope

This policy is intended to cover full system validation for all instances of REDCap used by PSH and ECTU which are deployed as clones of the 'Dev' instance. All instances are maintained by the Server Manager. Specifically, this policy details the validation of REDCap following new installations and major upgrades as well as validation prior to project releases, and periodic business continuity reviews in accordance with institutional and regulatory standards (EU GMP Annex 11: Computerised Systems).

4 Responsibilities

Each Data Management group has ultimate responsibility for the full System Validation of their own REDCap instances. Specifically, it is the responsibility of the individual Data Management group (PSH & ECTU) to ensure processes and proper evidence are in place to validate their own PQ, as this deals on the study-specific level. Further, while technical setup (controlled by the Server Manager) of instances will for the most part be the same across both groups, IQ incorporates group specific elements, such as System Configurations (e.g., password settings, MFA) which can be modified by individual groups as per their needs.

On the other, validating OQ will be a shared activity given the cross-over and burden of effort this task will take. Both groups will share the majority of effort shared activities in obtaining and/or creation of any documentation relating to the OQ, and the carrying out any validation activities that may be required for this. These activities will be collaborative, and divided between the groups in a suitable way based on resources available.

5 Validation Strategy

5.1 Detailed Strategies

5.1.1 Installation Qualification (IQ)

The REDCap system has been installed and configured by the Server Manager in line with VUMC guidance (https://projectredcap.org/software/requirements/) and University of Edinburgh IT policies. User level System Configurations (e.g., password controls) are set by the Data Management team, confined to REDCap built-in settings and restrictions.

IQ will not be addressed through manual testing, rather local server specifications are evidenced against regulatory technical setups and security standards. Local specifications are described in detailed version-controlled documents which are reviewed regularly and retained as evidence. These documents confirm that REDCap has been deployed according to current best standards.

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

Full details can be found within the *REDCap Technical Architecture Diagram* and *System Level Security Policy* and *REDCap Information Security Audit* documentation.

5.1.1.1 REDCap Technical Architecture Diagram and System-Level Security Policy

The *REDCap Technical Architecture Diagram and System-Level Security Policy* Document provides a comprehensive overview of how the REDCap service is deployed, secured, and maintained within the University of Edinburgh's IT infrastructure. It outlines the technical environment, hosting arrangements, network and firewall configurations, user access controls, data protection measures, and system maintenance processes. This document formally evidences REDCap's installation and security in line with institutional standards. It is a key reference supporting IQ and broader system-level validation efforts. It demonstrates compliance with best practices in information security, system reliability, and operational integrity within a university research setting.

This document is controlled and maintained by the Server Manager and is applicable to the 'Dev' instance and all clones. Each Data Management group is responsible for ensuring that the most recent version of these documents is obtained and documented in their local shared drive.

5.1.1.2 REDCap Information Security Audit

The *REDCap Information Security Audit* is a locally implemented process for evaluating the security controls and compliance measures of a REDCap instance. The audit assesses the system against relevant UK regulatory requirements, guidance and institutional policies applicable to the use of REDCap in regulated clinical trials, including UK GDPR, MHRA GxP and, where applicable, EU GMP Annex 11. It covers key areas including authentication, access control, audit trails, data protection, vulnerability management, system hosting, data integrity, information security and system validation.

The information security audit is supported by a template adapted from materials provided by the REDCap Consortium through the RSVC. The template has been reviewed and modified to ensure that its audit items are relevant to the UK regulatory, research governance and institutional context. Where necessary, terminology and requirements have been adapted to reflect applicable UK requirements and institutional policies, while retaining relevant elements of the original RSVC structure.

This approach provides a consistent and risk-based process for assessing the security and compliance of REDCap instances operated by both Data Management groups within the regulated UK environment. The audit provides supporting evidence for the system-level validation of each REDCap instance.

Each Data Management group is responsible for maintaining and periodically reviewing the Information Security Audit for its own REDCap instance (see audit template for details). The review should be at a minimum every two-years

5.1.2 Operational Qualification (OQ)

OQ for REDCap will be evidenced primarily though the adoption of the VUMC RSVC REDCap validation materials, which provide documented testing of REDCap's core functions against the applicable release specifications. RSVC OQ testing is conducted in accordance with the consortium's release schedule which follows the six-monthly Long-Term Support (LTS) release schedule.

The RSVC REDCap Validation Materials provide an established and extensive body of evidence for the testing of standard REDCap functionality. Their use provides a proportionate and risk-based

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

approach to OQ by reducing duplication of testing and the resources required to independently test core REDCap functionality. For each applicable release, the RSVC Validation Materials (webpage) will be reviewed to confirm their applicability to the local REDCap instance, including version alignment and scope of coverage. Where gaps are identified, additional local OQ testing will be undertaken as required.

Basic business continuity checks are performed on our local REDCap instance prior to each System Version Update release (see *ECTU_SOP_REDCap_10 REDCap Application Updates*).

Documentation released as part of the RSVC Validation Package will be reviewed to ensure these match our current server specifications and used as evidence for our own OQ. These materials are an invaluable foundation for REDCap validation. However, the Data Management groups acknowledge that the **validation results provided by VUMC alone does not constitute full system validation**, and local OQ, IQ and PQ testing is required to complete full system validation.

5.1.2.1 RSVC REDCap Validation Materials

Validation materials are available from the RSVC Consortium webpage. Both Data Management groups will hold the relevant RSVC validation materials for all LTS Versions used on our local REDCap systems to leverage our OQ testing requirements. A review will be conducted and in specific circumstances, local validation materials may be created where there is determined to be a gap in the RSVC validations. For details on how local validations are handled see 5.2.2.2 below.

5.1.2.1.1 RSVC Validation Package Guide

This document provides a high-level summary of the files and documents included in the package. It describes the process used to develop the package and testing of the validation process.

For full understanding of the documentation held locally in evidence of OQ testing, the Validation Package Guide is an invaluable source.

5.1.2.1.2 RSVC URS, FRS and Change log review

Of the materials provided, the User Requirement Specification (URS) is the foundation for validation activities. It is released by the **VUMC** and outlines the essential requirements and risk assessment procedures necessary for validating REDCap. As this is a vendor released document this cannot be, and should not, be changed as part of the validation process. From the URS, key decision making on the part of the RSVC group goes into developing the RSVC Functional Requirement Specification (FRS), a document outlining the core features of REDCap ensuring the system functions correctly with traceability scenarios that can be used to test and validate each requirement within the URS. The FRS describes the scenarios (i.e., the *how*) to ensure the user requirement of each function is met, and maps each function to specific REDCap features or modules (e.g., user management, project creation, data exports). The RSVC has developed detailed testing scripts for all scenarios detailed within its RSVC which capture the precise steps taken to test a function. These form the basis of their semi-automated testing.

During the time period in between LTS releases, the RSVC reviews the change logs for new or changed functionality which may impact on the core set of functionalities. The RSVC assesses whether these changes meet the inclusion criteria and require addition into or amendment of the next FRS to be released. Details of this Change Log Report are released as part of the validation materials.

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

In summary, the content of the URS, RSVC FRS and change log assessment report documents will not be altered, rather, they will be retained to evidence exactly how core features are expected to function, and the steps that informed the feature test report.

5.1.2.1.3 Feature Test report

The RSVC uses predominantly automated testing in their OQ tests, and where automation is not possible, manual testing is used. The results of these tests are included with the Feature Test Report, which includes exact steps used in tests as well as the results of each test (e.g, pass or fail). All results are available as videos within the test report. The results of these test will be reviewed at each LTS release locally to confirm all tests were undertaken fully and where not, the review will assess whether local testing is required (see 5.2.2.2).

5.1.2.1.4 RSVC Certificate of Completion

Validation is released in three tiers (A, B, and C). The Core Validation is considered complete when all three tiers are signed off. Features or functions designated as Tier D are outside the scope of the RSVC validation, as well as the scope of PSH / ECTU validation review. For details of tiers, see RSVC Validation Package Guide.

5.1.2.1.5 Documentation and Oversight

Each individual Data Management team is responsible for retaining all validation documentation within their respective shared areas. All current and historical RSVC validation materials can be located here: https://redcap.vumc.org/plugins/redcap_consortium/regval_materials.php

5.1.2.2 Local REDCap Validation Materials

In addition to the materials provided by RSVC, local documentation will accompany these to ensure that proper reviews of RSVC materials and any core functionalities in use locally (not included in RSVC) are tested. At a minimum this will include the validation verification. Where gaps are found in the validation package, this may require local testing and/or a local FRS. For example, any external modules used by an individual group, that did not meet the criteria to be included as part of the RSVC validation package, will be adopted into a local FRS and may require testing only where this cannot be done as part of PQ. In cases where a core function is listed in the RSVC FRS but tests were not fully completed, then this will not require adoption into the local FRS but will require documented local testing.

5.1.2.2.1 Local Validation Verification

The Local Validation Verification worksheet is a tool used to combine reviews of the RSVC materials to confirm that each new LTS production release is supported by the correct vendor validation package, that all required tier A–C validation documents are present, and that core REDCap features have been tested and passed. It also evidences review of RSVC change log between the previous and current validated LTS versions, records an assessment of whether reported core changes require additional local validation (with justification), and provides a controlled place to document additional local testing, corrective actions, and supporting evidence, creating an auditable record that the local production update aligns with RSVC validation expectations.

5.1.2.2.2 Local FRS

External modules used locally and those requirements within the URS that did not meet the criteria to be included as part of the RSVC validation package, are to be reviewed, and if needed for local use, form a Local FRS required for full validation of functionality. Within the local FRS, each function will be assigned a Functional Requirement Number (FRN) number following the same nomenclature

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

of the RSVC materials for test traceability, a category and feature which the function comes under (in keeping with RSVC category list), and a detail requirement of the functions expected action.

5.1.2.2.3 Local Feature Tests and Scripts

Where required, feature tests and scripts will be generated locally. Within the FRS, functions are categorised by feature (e.g., Project Setup, Data Quality) depending on what each particular function relates to. For the purposes of creating local testing documentation, functions will be tested per feature. The testing scripts (i.e., the exact steps taken to evidence a function acts as expected according to its requirement) will be created by the Data Management groups (or group if only required by one team) including the specific functions to be tested, detailed test procedures, the environment and user details used for testing, and a space to confirm whether this function passed and failed. Functions may contain multiple scenarios to increase granularity. Each feature testing document should include a sign off.

5.1.2.2.4 Completing Tests and Recording Evidence

All local tests are executed within the 'Dev' instance by a suitably trained Data Manager. The specific steps taken to test a function is described within the feature tests and scripts, and by marking the test as passed or failed, the tester confirms the completion of this test. Where tests require the creation of a project, the project name should be the LTS release version and functional requirement number, for audit purposes.

Each test should be screen recorded (e.g., video, images) and saved as evidence. Where it is not possible to use screen recordings, xml and/or CSV files should be retained.

The review of local OQ testing is repeated for each REDCap LTS Version release.

5.1.2.3 Local Certificate of Completion

Upon the successful completion of all local feature tests, a formal Certificate of Completion will be issued. Detailed within the certificate: the validated REDCap LTS Version, the date of completion, identity of the individuals responsible for the testing. The certificate serves as a formal record for audits and inspections.

5.1.2.4 Documentation and Oversight

Each individual Data Management team is responsible for retaining all validation documentation within their respective shared areas. These should be saved alongside RSVC materials.

5.1.3 Performance Qualification (PQ)

Features that have been validated during OQ are implemented at the individual project level. However, within each project, these features are specifically configured according to the unique requirements of the study protocol. Because of this customisation, additional validation and testing are necessary to ensure the system performs as intended under real-world, study-specific conditions.

In this context, PQ represents the final phase of validation and focuses on verifying that the system, as configured for a particular study, reliably supports all required tasks and data workflows.

As part of the PQ process, a project-specific validation plan is created. This plan outlines the key instruments and core system functions that need to be tested based on protocol requirements. It defines the scope of validation activities and serves as the foundation for all subsequent testing efforts. All project validation documents are generated by the Data Manager responsible for building

Docusign Envelope ID: 8FD21412-C9A5-83A4-8216-A25614317EEA

the study project. The study team is accountable for executing testing and completing these documents to demonstrate compliance.

The full study validation process including planning, documentation, system testing, and final approval, is described in detail in the PSH and ECTU respective Data Management SOPs. All study-specific projects must complete this process and be fully validated before being released for use.

5.2 Review and Maintenance

This policy will be reviewed every 2-years from release date.

6 Relevant Documents and References

Held centrally within PSH Data Management SharePoint:

- PSH_SOP_RED_02 REDCap Project Validation and Release
- PSH_DM026_REDCap Information Security Audit Template

Available from the ECTU SOP Webpage (*https://usher.ed.ac.uk/edinburgh-clinical-trials/supporting-trials/governance/standard-operating-procedures****)***

- ECTU_SOP_REDCAP_04 Study Database Validation
- ECTU_SOP_REDCap_05 Study Database Release
- ECTU_SOP_REDCap_10 REDCap Application Updates

Available from ACCORD Website (*https://www.accord.scot/research-access/resources-researchers****):***

- ACCORD POL007 COMPUTER SYSTEM VALIDATION

Other:

- University of Edinburgh Information Security Policies Available here: https://information-services.ed.ac.uk/about/policies-and-regulations/security-policies
- RSVC Validation Packages available here: https://redcap.vumc.org/plugins/redcap_consortium/regval_materials.php
- REDCap Technical Architecture Diagram and System Level Security Policy Document
- EU GMP Annex 11: Computerised Systems available here: https://www.gmp-compliance.org/guidelines/gmp-guideline/eu-gmp-annex-11-computerised-systems