



THE UNIVERSITY *of* EDINBURGH
Baillie Gifford Pandemic Science Hub


PSH_SOP_DM_04:

REDCap Disaster Recovery Test




Document Control Sheet


Revision History

Version	Revision Date	Reason for revision	Author	Signature and Date
1.0	02Apr2025	<ul style="list-style-type: none">Initial Creation	Christopher White	 <small>Christopher White (07-May-2025 14:55 GMT+1)</small> 07-May-2025

Document Review

Role	Organization	Name	Signature and Date
Assistant Data Manager	ECTU, University of Edinburgh	Krisztian Kozlov	 07-May-2025

Document Approval

Role	Organization	Name	Signature and Date
Healthcare Technology Portfolio Project and Development Manager	University of Edinburgh	Paul Fineran	 <small>PD Fineran (09-May-2025 12:08 GMT+1)</small> 09-May-2025

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



Table of Contents

1	Purpose	5
2	Scope	5
3	Responsibilities	5
4	Procedure.....	5
4.1	Preparations for Testing.....	5
4.2	Conducting Disaster Test	6
4.3	Validation	7
4.4	Test Frequency.....	7
4.5	Documentation and Filing.....	7
5	Relevant Documents and References.....	7



Definitions

Terms	Definition
Data Management	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.
REDCap Administrator	The REDCap administrator refers to the designated person(s) from the Data Management groups responsible for carrying out Disaster Recovery Test activities for their respective Data Management teams.
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. This individual co-ordinates server-related tasks, including backup verification, restoration, and system availability testing.
Unix Team	The Unix Team consists of system administrators from the University of Edinburgh's Central IS Services who provide support for the underlying Unix-based infrastructure hosting the REDCap server. They are responsible for tasks such as server provisioning, OS-level recovery, and ensuring that required system dependencies are operational during the disaster recovery test.
'Dev' Server	<p>The Dev Server is a duplicate of the Production (Live) Server, which hosts all live study and trial data. It serves as a testing and validation environment, allowing the Data Management teams to conduct system checks and validate configurations without impacting live study data or business activities.</p> <p>Access to the Dev Server is restricted to authorised members of the Data Management groups, ensuring controlled and secure testing separate from production operations.</p>

1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish a structured, step-by-step protocol for conducting a disaster recovery test for the REDCap server. This test is designed to evaluate the effectiveness of the disaster recovery process, verify the functionality and integrity of backups, and ensure REDCap data can be restored accurately and promptly in the event of a disaster. This SOP will be reviewed on a 2-year basis.

2 Scope

This SOP applies to all Data Management groups using the REDCap Server, licenced under the Institute for Genetics and Cancer license, with access to the 'Dev' server i.e., Edinburgh Clinical Trials Unit (ECTU) and Pandemic Science Hub (PSH) Data Management teams.

It does not cover server-level recovery actions (e.g., technical specifics in generating data back-ups and recovering deleted files), which are handled by the central University of Edinburgh (UoE) IS teams according to their own operating procedures.

3 Responsibilities

It is the responsibility of the REDCap administrator to coordinate with Server Manager to organise and appropriate date to conduct a disaster recovery test in accordance with this SOP. REDCap administrators are responsible for the creation and deletion of test projects, and of the evidencing and recording of test results and communicating results to all necessary parties (e.g., Server Manager).

It is the responsibility of the Server Manager and Unix Team to execute server-level disaster test actions (e.g., restoring back-ups in test environment), and provide technical support and address issues identified during testing.

4 Procedure

4.1 Preparations for Testing

4.1.1 Environment

All disaster testing should be undertaken in the 'Dev' server environment. The 'Dev' server contains no live data and is used solely for training and validation purposes. As a result, the conducting of the disaster recovery test will have minimal to no impact on business operations. However, once a date and time are agreed with the Server Manager to complete the test, Data Management teams should be made aware that no persons should access the Dev server or amend data for the duration of the test, other than the REDCap administrator responsible for carrying out test activities.

4.1.2 Schedule

The REDCap Project Disaster Recovery Test will be completed on an annual basis.

A few months in advance of the expected renewal, the Data Management group will coordinate internally to determine the course of action, providing enough time to contact IS and schedule a date. A REDCap Administrator will contact the central IS Services or REDCap server manager in good time (typically 1-3months in advance) to arrange an appropriate date to conduct the test. It is recommended this is done during low-usage periods (e.g., early morning).

In order to carry out the Disaster Recovery Test, it will require the availability of three parties:

1. Data Management group
2. Server Manager
3. Unix Team

Details of scheduling should be captured in the Disaster Recovery Test report completed by the REDCap administrator.

4.2 Conducting the Disaster Test

4.2.1 Back-up Snapshot

On the agreed date, the REDCap Administrator will create a test project within the 'Dev' Server titled 'testProjectA[creation_date]' (where [creation_date] should be replaced with the date of project creation). Within this project, an instrument will be setup with a variety of field types containing sample (dummy) data to simulate real entries, after which a data export will be downloaded for comparison to recovered data, along with the data dictionary. To evidence the project creation and documentation downloads, the REDCap Administrator will download the Logging data (i.e., audit log) from the project applications. Once project documentation is obtained, a screenshot of the latest User Activity Log (available from the Control Centre) will be collected for later comparison. Time of project creation, Data Dictionary download, Data Export download, Logging and User Activity Log downloads will be recorded in the Disaster Recovery Test report.

Following this, the REDCap Administrator should inform the Server Manager that the system is ready for a snapshot of the server to be taken.

4.2.2 Backup Verification

The Server Manager will liaise with the Unix team to confirm a snapshot of the server has been taken (containing testProjectA) and inform the REDCap Administrator that a backup of the current state of the 'Dev' server exists prior to the disaster test begins. If available, the time of back-up should be recorded.

4.2.3 Disaster Scenario Creation

The REDCap Administrator will simulate a disaster scenario by deleting the testProjectA and all associated data, permanently. REDCap projects must be deleted 'twice' in order to delete permanently. In addition to deleting testProjectA, the REDCap Administrator will create a new project titled 'testProjectB[creation_date]'.

A screenshot of User Activity Log (available from the Control Centre) should be retained showing deletion of testProjectA and creation of testProjectB. Times of project amendments and screenshots should be recorded in the Disaster Recovery Test report.

Once both actions are completed and screenshots collected, the REDCap Administrator will confirm with the Server Manager that the 'disaster' has been simulated.

4.2.4 Restoration

The Unix team will then restore the 'Dev' server from the most recent backup using their established disaster recovery procedure. The Server Manager will confirm via email when this has been completed.

4.3 Validation

4.3.1 Verify Restoration

Following recovery, the REDCap Administrator should navigate to the 'Dev' server to confirm testProjectA is now available, with all data returned, and that testProjectB is no longer available. To evidence this, the REDCap Administrator will obtain testProjectA Data Export, Data Dictionary, Logging downloads and compare these to pre-disaster documentation to ensure there are no differences. Further to this, a screenshot of the latest User Activity Log will be compared to both pre-recovery User Activity Logs (i.e., pre- and post-disaster). The recovery User Activity Log should be identical to the pre-disaster screenshot.

Full results should be recorded in the Disaster Recovery Test Report and the Server Manager notified of the results. Times of all downloaded documentation used to evidence results of the test will be recorded in the Disaster Recovery Test Report.

To confirm completion of the Disaster Recovery Test, a REDCap Administrator from both PSH and ECTU Data Management teams along with the Server Manager will sign-off the Disaster Recovery Test report.

4.3.2 Reporting Failure

If any testing fails, this should be immediately escalated to the Server Manager for resolution, details of failure should be recorded within the report and signed off by all relevant parties. Once the located issue is resolved, another Disaster Recovery Test should be undertaken at the next possible window.

4.4 Test Frequency

Disaster recovery tests will be conducted annually.

4.5 Documentation and Filing

All testing documentation, including project comparisons and test results will be held digitally in the central Data Management folder (e.g., PSH DM SharePoint, ECTU DM DataStore).

Emails relating to testing will be filed in the generic Data Management inbox under relevant folders.

5 Relevant Documents and References

Held centrally within PSH Data Management SharePoint:

- PSH_DM025_Disaster Recovery Test Report

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>