

SOP-QA-20 V5

Title: Data management

Effective Date: 07-10-26 | Review Date: 07-10-29

Author: Louise King, Research Governance Manager

QA Approval: Richard Cowie, QA Manager

Approver: Prof Seshadri Vasani, R&D Director

Approver: Prof David Blackburn, Head of School



GRAMPIAN CLINICAL RESEARCH OFFICE



Document History

Version	Description of update	Date Effective
4	Clinical study updated to Research project at 1.1 Text updated to UK Data Protection Law at 1.2 Clarification on CTIMPs and MDCl audit trail at 3.2	09-08-23
5	Scheduled review. Removal of reference to surgical studies at 3.1 Reference to UAT and CSV requirements at 3.3 Reference to study monitoring plan at 3.3 and removal at 3.7 Clarification on completing CRFs at 3.4 Reference to anonymous and pseudonymised data t 3.8	07-10-26

1. Scope

- 1.1 This SOP applies to any individual involved in a research project sponsored, or co-sponsored, by University of Aberdeen (UoA) and/or NHS Grampian (NHSG) and describes the procedure for data collection, data management and security for data held in databases used in a research project.
- 1.2  In addition to the principles of GCP and appropriate UoA and NHSG policies, research data shall be collected, recorded and managed in accordance with the UK **Data Protection laws**.

2. Responsibilities

Sponsor	Ensure investigators have control of, and continuous access to, data reported to the Sponsor.
Chief Investigator (CI)	Acting on behalf of Sponsor, may delegate data management.

3. Procedure

3.1 Data Management System

-  The study protocol, or other study document, shall clearly specify the data to be collected using Case Report Forms (CRF) and/or stored electronically, and which data elements are to be retained upon archiving.
-  There shall be a unique identifying ID for each participant. The code or file linking participants' names with their IDs (Subject Identification Log) shall be kept secure and separate from the data used for study analysis.
-  Computerised systems shall safeguard study blinding where this exists. Blinding shall not be broken through day-to-day use of the computerised system.  Any data which may inadvertently break the blind (eg specific laboratory test data) must be inaccessible

Uncontrolled when printed. Please ensure that you are working on the most up to date version of this SOP.

Key to symbols  = Important point to note  = Warning

to the study team. The system shall provide protection against unintentional unblinding but support, where appropriate, any unblinding procedures described in the protocol.

-  Identifiable data shall not be retained for longer than is necessary to meet the requirements described in the study protocol and to meet requirements set by the grant-awarding body, Research Ethics Committee (REC) and regulatory authorities. All Clinical Trials of an Investigational Medicinal Product (CTIMPs) and Medical Device Clinical Investigations (MDCIs) shall be archived for **twenty-five years**, unless subject to any other third party obligations eg funder's terms and conditions, or are subject to legal requirements (ie Legal Hold). All other studies shall be archived as stated in the protocol, or Sponsor's institutional guidelines. Deleting data may require the physical destruction of digital media.
-  Any changes or updates to the system must be documented as part of a change control process and the relevant parts of the system revalidated.
-  The trial team shall be trained in completion of the CRF (paper or electronic) prior to recruitment of the first participant.

3.2 Data security

- Electronic data shall only be stored on devices that are backed-up securely and timely.
-  Data used for **study analysis** shall be pseudonymised. Data used for **study management** shall use the minimum number of personal identifiers necessary for study conduct and to ensure participant safety.
-  Personal data shall not be stored or transmitted on removable media or laptops without encryption. Datasets shall be encrypted prior to transmission, or transfer (eg on CD), using an industry-standard encryption mechanism (eg AES-128), or transferred securely using the nhs.scot email system or the UoA's preferred file transfer service (FTS); ZendTo.
-  All machines used by research staff to enter/access trial data shall have appropriate security software.
-  Access to the data shall be limited to authorised personnel and each user of the system shall have an individual account.
-  A record shall be kept in the TMF of authorised users and their access levels that apply.
-  Where possible the study database shall have an audit trail for any changes made to electronic data after initial entry. This shall include the original value together with the date of the change and who made that change. If possible, a brief explanation of why the change was made should also be recorded. For CTIMPs and MDCIs data capture systems without an audit trail should be discussed with Sponsor prior to implementation.
-  At the end of a study, data shall be locked to prevent further additions or changes to the data using the data management system's file-locking facility, if such a facility exists, otherwise a snapshot of the data should be taken for analysis and access to the data denied to anyone except the Data Manager or statistician.

3.3 Electronic Data capture

Data capture and entry shall be undertaken by suitably trained personnel.  Where bespoke electronic data capture systems are to be developed for use in locally Sponsored research, a realistic timeline shall be agreed and documented with the developers involved. This must allow sufficient time for essential Computer Systems Validation (CSV) to be completed, on the functionality required at baseline and early data collection points, including User Acceptance Testing (UAT).  Study activity shall not commence until this required CSV, including UAT, has been completed. Where a phased implementation has been agreed and documented in advance with the developers involved, CSV, including UAT, for later time points may be

completed after the study has gone live, however sufficient time must be allowed for UAT prior to use.

-  Electronic data capture systems shall reflect the layout, design and content of data capture documents.
-  Electronic systems shall include data validation, range checks and consistency checks, where agreed with the study team, to ensure good data quality.
- Actual dates/times of events or data collection points shall be recorded
- If necessary, data entry checking shall be considered for critical data. A study monitoring plan shall describe any data entry checking process to be used (eg single data entry and verification or double data entry), an acceptable data entry error limit and action to be taken if the error rate exceeds this limit.
- Data queries or data anomalies shall be handled following study specific guidelines.

3.4 Paper Case Report Forms

-  Paper CRFs shall be version controlled, paginated, with effective date on each page.
-  Participant ID shall be documented on every page.
-  The study identifier (eg name) shall be clearly stated.
-  No identifiable information shall be on the CRF except where there is a specific CRF designed to capture participants' details.
-  Paper CRFs shall set out all the data to be collected or procedure to be carried out, on each participant at each visit.
-  No information shall be collected that cannot be justified by the protocol or standard safety procedures.
-  Paper CRFs shall be completed in permanent ink.
-  Any error or alteration shall be crossed through once, initialled and dated, leaving the original value visible (see SOP-QA-27 – Good documentation practice).
-  All required fields shall be completed. If a procedure is not carried out, this shall be indicated.
-  To enable consistency, CRFs shall indicate which unit of measurement is to be used.
-  The CRF shall be designed so that questions can be completed succinctly and avoid providing free-text clarifications.

Raising Data Queries

- 3.5 All data queries shall be raised as soon after data collection as practicable. These may include missing, inconsistent or implausible data. As far as possible, all data queries shall be resolved prior to data lock. Data for analysis shall always remain verifiable against source data.

Data analysis

- 3.6 The data shall be presented in a form appropriate for the particular needs of the study.
- 3.7 There must be a quality check of data prior to interim and final analyses. Quality checks shall include checking for outliers, missing data, date checks and any inconsistencies.
- 3.8  When data is to be exported for statistical analysis, the dataset must be in an anonymous form to the statistician (the data may be pseudonymised, but the statistician shall not have access to the linked key).

- 3.9  Any files containing sensitive data must be encrypted and password protected before transfer. Passwords shall be communicated to the recipient separately.

Data protection

- 3.10  All person-identifiable data must be treated in an appropriate, confidential manner.
- 3.11  Paper or computer records shall be accessible to the minimum number of people needed to ensure the smooth delivery of the study. All of these staff shall be made aware of their responsibility to maintain confidentiality by the CI.
- 3.12  Personal information shall not be sent by email; encrypted files must be used, unless via the secure nhs.scot email system, or the UoA's preferred FTS.
- 3.13  Personal data shall not be transmitted in a way that could cause loss of data or allow interception by unauthorised parties.

4. Abbreviations and definitions

CI	Chief Investigator
CRF	Case Report Form
CSV	Computer Systems Validation
CTIMP	Clinical Trial of Investigational Medicinal Product
FTS	File Transfer Service
GCP	Good Clinical Practice
MDCI	Medical Device Clinical Investigation
REC	Research Ethics Committee
TMF	Trial Master File
UAT	User Acceptance testing

5. Related documentation and references

SOP-QA-12	Case Report Forms
SOP-QA-18	Randomisation and blinding for controlled trials
SOP-QA-27	Good documentation practice
SOP-QA-32	Archiving