STANDARD OPERATING PROCEDURE FOR DATA MANAGEMENT IN CLINICAL RESEARCH

SOP NUMBER:	TASC SOP053 v8
AUTHOR:	Marcus Achison
EFFECTIVE DATE:	28 April 2026
REVIEW DATE:	25 Aug 2027

1. PURPOSE

This Standard Operating Procedure (SOP) describes the management of clinical research data.

2. SCOPE

This SOP applies to clinical research studies sponsored or co-sponsored by the University of Dundee (UoD) and/or NHS Tayside (NHST). It is intended for use by all personnel involved with the management of data in clinical research studies. It should be used in conjunction with other relevant SOPs, as agreed and approved by Sponsor.

3. RESPONSIBILITIES

Research data must be collected, recorded, and managed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and UoD and NHST policies. In addition, data from studies involving human participation must be handled in accordance with applicable ethical and regulatory standards. Good Clinical Practice standards are a legal requirement for Clinical Trials of Investigational Medicinal Products (CTIMPs).

4. PROCEDURE

4.1 Data Management and Clinical Studies

Data management encompasses the receipt and tracking of clinical study data, data entry into the study database or equivalent electronic data capture system (EDC), generating and resolving data queries and database or EDC lock. An Excel Data Management System (DMS) may be used for CTIMPs with Sponsor approval, prior to study start. Please refer to TASC SOP "Data Management in Clinical Research Studies Using Excel" for detailed requirements and controls.

The development and management of a study-specific DMS may be performed by Tayside Clinical Trials Unit (TCTU), the study team or outsourced to an external third party. If the

development and management of a DMS is outsourced, the Chief Investigator (CI) must contact TASC Legal to prepare an appropriate collaboration or service agreement.

Each study requires documentation to prove that the DMS meets the requirements of the end users and that data can be stored, managed, and exported without alteration.

Study-specific documentation should include:

- A Data Management Plan (DMP).
- A DMS specification document based on the protocol and paper Case Report Form (pCRF), if one is to be used and updated with any subsequent modifications and agreed data validations.
- Evidence that the DMS has undergone and passed validation and that any study-specific configurations have passed testing. This includes validation of the export process and User Acceptance Testing.
- User instructions and record of user training.
- Documented sign-off by designated personnel or their representatives, followed by release of the DMS for "live" use.

4.2 Data Management Plan

The DMP describes the study-specific data management activities and must be put in place for each study. It must be reviewed and signed off by the CI, Study statistician, and staff responsible for data management and study management.

A DMP typically details:

- All data sources and how they will be integrated (i.e. the data flow).
- The DMS to be used, e.g. Castor EDC, OpenClinica, REDCap, Excel.
- Responsibility and procedures for the following activities:
    - Database development and testing.
    - Approval of the template pCRF or study variables if a pCRF is not used, and any subsequent modifications.
    - Data entry.
    - Data cleaning, including correction of queries.
    - Quality control measures (e.g. database audit, including predetermined data entry error rate and source record verification if required).
    - Preparation of data extracts.
    - Database lock and archiving.
    - Management and security of the DMS.
- Any additional study-specific instructions.
- Information on data requirements for Data Monitoring Committees and interim analysis (if relevant for the study).
- Data transfer, if required.
- Details of any external datasets that will form part of the analysis data.

4.3 Data Management System

The DMS should include the following:

- Reflect the layout and design of the pCRF/eCRF as accurately as possible to facilitate ease of data entry.
- Should not collect participant-identifiable data.
- Only collect date of birth in exceptional circumstances where it is vital to the study outcome. The use of date of birth should be included in the Sponsor's risk assessment and risks mitigated by employing suitable data security measures. Collecting age at consent instead of date of birth should be sufficient in the majority of studies.
- Include data validation functionality, e.g. range checks and checks for missing or inconsistent data, to ensure the highest quality data.
- Use unambiguous and unique identifying participant IDs. The code or file linking participants' names with their ID shall be kept secure and separate from the data used for study analysis.
- For blinded studies, the study blinding should be safeguarded. Treatment allocation shall not be broken by day-to-day usage of the system and must support any unblinding procedures put in place to ensure participant safety. Data which may inadvertently unblind staff, e.g. laboratory data, must remain inaccessible to the study team.
- Include a complete audit trail to ensure it is possible to determine when and by whom data has been originally entered or changed.
- May also include the option to record electronic Participant Recorded Outcome (ePRO) data, where participants complete study data themselves via managed access to the database (e.g. via email invites, mobile device, tablet etc.).
- It is recommended that representatives of intended participant populations and healthcare professionals are involved in the design of the system, where relevant, to ensure that computerised systems are suitable for use by the intended user population
- Aspects such as user authentication requirements and password management, firewall settings, antivirus software, security patching, system monitoring, and penetration testing should be considered
- Contingency procedures should be in place to prevent loss or lack of accessibility to data essential to participant safety, trial decisions, or trial outcomes.

If data are transformed during processing, e.g. calculation of BMI from height and weight, or if a partial date field (text field) is transformed into a real date field it must always be possible to compare the original data with the processed data.

4.4 Validation and Functional Testing

The DMS must undergo a process of validation, functional testing, and User Acceptance Testing to demonstrate that it is fit for purpose and performs consistently.

4.5 Training

All DMS users must be trained by an appropriate trainer and provided with user guides and any other required training materials.

Training must be documented both in the individual's training log and also retained in the study-specific Data Management folder/Trial Master File.

4.6 User Access

A record of DMS users, their access levels and when access was granted and revoked, must be recorded. User access must be revoked when access is no longer required.

This record may be stored within the DMS, if this function is available, or in the study Trial Master File.

4.7 Data Quality

4.7.1 Data Entry and Data Queries

Data must be entered into the DMS exactly as recorded in the pCRF (where used) and shall be verifiable against source records.

Data queries may be raised as a result of visual inspection of the data or by point of data entry checks present in the DMS. This can be performed as the data is entered or by data validation processes such as batch validation, which is used to perform checks that cannot be carried out at the point of data entry.
Where pCRFs are used, the data recorded in the pCRF and DMS must be kept consistent with one another. If a correction is made to the DMS as a result of the data querying process, the pCRF must also be updated by crossing through the original value without obscuring it, writing the new value, and initialling and dating the correction. If a change is made to the pCRF, a reason must also be provided on the pCRF to explain why the change was necessary.

Where data entry is not performed at the location, the original pCRF must remain at the location with a copy being sent for data entry. Scanned copies of pCRFs may be transferred electronically via secure methods to facilitate data entry. Any changes to the original pCRF must be notified to the data entry team by means of an updated copy of the original being sent to the data entry team. Any copies of the pCRF should be checked and any participant identifiable data removed prior to transfer.

4.7.2 Identification of Source Records

Data points for Source Records Verification should be selected using a risk-based approach. This includes safety data and data linked to the main outcomes of the study.

Data recorded using ePRO or participant-completed paper questionnaires is considered source records. Changes to these records should be rare and must be supported by documentation in the participant's medical record.

The DMS, including ePRO, must have a complete audit trail. This audit trail must retain the original value of any changed data, along with a record of who made the change, when it was made, and the reason for change.

The DMS should prompt users to enter a reason for changing the data. Typical reasons include correction of a data entry error or response to a data query.

4.7.3 External Data Reconciliation

Data from randomisation systems or external datasets may not be imported or entered into the DMS but will be merged with the data from the DMS for later analysis.

External datasets must be reconciled against the related DMS data to ensure that all expected data are present. Where the same data are held in both systems, they must be reconciled, and any inconsistencies identified and resolved to ensure data accuracy.

Where data is imported into the DMS, consideration must be taken to ensure that data accuracy and integrity is maintained, e.g., data is verifiable against source and that suitable data management and monitoring processes are in place to deal with data inconsistencies/queries.

4.8 Principal Investigator Oversight of Study Data

For studies which use a pCRF or eCRF, all data entries and updates must be performed by a delegated individual following the procedures described above in section 4.7.1. When all data have been entered and confirmed as correct, a final sign-off of the study data must be provided in the pCRF or the eCRF by the location Principal Investigator.

4.9 Data Lock, Unlock and Archive

The DMS will be locked when data entry is complete and the data have been cleaned to the satisfaction of the study Statistician and the Chief Investigator (CI). For studies using pCRFs, this includes quality checks of the data to ensure a predetermined data entry error rate has been met.

Database unlock must be strictly controlled and only carried out in exceptional circumstances with the approval of the CI, Sponsor, and study Statistician.

Refer to TASC SOPs on Database Lock and Archiving for detailed procedures.

4.10 Ensuring Location Investigators maintain control of Location Data (eCRF studies)

For studies using eCRF, it has to be ensured that locations have continuous access to their data.
Therefore, study data should be transferred to the location as soon as possible after database lock. Principal Investigators should have read-only access to their study data in the

DMS until the study data and associated documentation is transferred to the location and a data acceptance sign-off is provided. This is required to ensure that investigators retain control of their data and to facilitate archiving of their study data according to the local location archiving procedure.

4.11 Data Transfer to Third Parties

When data are to be transferred to a third party (i.e. a party outwith the UoD and NHS Tayside), the CI must ensure with TASC Legal, where appropriate, that Data Transfer Agreements are in place with the recipient of the data to ensure that it is used and stored in compliance with applicable regulations.

Datasets must be encrypted, using an industry-standard encryption mechanism, such as AES-128, prior to transfer (whether electronic or on removable media). Alternatively, a web-based secure data repository may be used (e.g. LabKey). In this case, the software must be installed on a secure UoD server with access restricted to password-protected authorised personnel only.

All methods of data transfer must be carried out in accordance with the principles of data confidentiality set out in the UK GDPR.

5. ABBREVIATIONS & DEFINITIONS

CI	Chief Investigator
CRF	Case Report Form
CTIMP	Clinical Trial of Investigational Medicinal Product
DMP	Data Management Plan
DMS	Data Management System
eCRF	electronic Case Report Form
EDC	Electronic Data Capture
ePRO	electronic Participant Recorded Outcome
GDPR	General Data Protection Regulation
NHST	NHS Tayside
pCRF	paper Case Report Form
SOP	Standard Operating Procedure
TASC	Tayside Medical Science Centre
UoD	University of Dundee

6. ASSOCIATED DOCUMENTS & REFERENCES

None.

7. DOCUMENT HISTORY

History prior to 2021 is in the archived SOPs available from TASC Quality Assurance Dept.

Version Number:	Reviewed By (Job Title):	Effective Date:	Details of editions made:

5	Emma McKenzie (Clinical Trial Information Systems Manager)	22/09/2021	Additional information on use of eCRFs, ePROs and data reconciliation/import between systems. Section 4.3 updated to comply with GDPR with regard to Date of Birth.
6	Marcus Achison (Database Manager)	25/08/2023	Visual Verification no longer mandatory. Updates to text.
7	Yusra Fatima (Data Manager)	25/08/2025	Minor changes to text. Vocabulary changed in line with ICH-GCP R3 updated terms.
8	Marcus Achison (Database Manager)	28/04/2026	Updated in accordance with the new Medicines for Human Use (Clinical Trials) (Amendment) Regulations 2025.

8. APPROVALS

Approved by:	**Date:**
Dr Steve McSwiggan, Senior R&D Manager NHS Tayside	23 Mar 2026
Dr Valerie Godfrey, TASC Quality Assurance Manager, on behalf of TASC Clinical Research Guidelines Committee	20 Mar 2026