MANCHESTER 1824
The University of Manchester

**Standard Operating Procedure**

| | | | |
|---|---|---|---|
| **Number:** | UoMCTSOP17/ 2026 / v7.0 | | |
| **Title:** | Data Management | | |
| **Version:** | 7.0 | **Effective Date:** | 13 May 2026 |
| **Author:** | Lubica Stasinkova | **Review Date:** | 13 May 2028 |
| **Reviewed by:** | Mohammed Zubair | **Approved by:** | Professor Adrian Parry-Jones |
| **Position:** | Research Governance, Ethics and Integrity Manager | **Position** | Deputy Chair of Clinical Trials Management Group |
| **Signature:** |  | **Signature:** | Via email |

| Version | Date | Summary of changes |
|---|---|---|
| 2.0 | January 2013 | Update of weblinks and office details |
| 2.1 | May 2014 | Addition of version control statement for SOP |
| 3.0 | October 2015 | Update of weblinks and office details |
| 4.0 | August 2016 | Update of weblinks and office details |
| 5.0 | March 2018 | Review and update |
| 6.0 | November 2020 | Update in line with GDPR, updated MHRA guidance, and sponsor processes. |
| 7.0 | April 2026 | Updated all regulatory references to align with the UK Clinical Trials Regulations 2026 |

## 1 Background

All clinical trial activities conducted under this SOP are in line with the applicable UK legislation governing clinical trials of investigational medicinal products and/or medical devices. This includes, but is not limited to, the Medicines for Human Use (Clinical Trials) Regulations 2004 and any subsequent amendments or replacement legislation, such as the Medicines for Human Use (Clinical Trials) (Amendment) Regulations 2025, effective from 28 April 2026. All procedures must be carried out in accordance with current guidance issued by the Medicines and Healthcare products Regulatory Agency (MHRA), the Health Research Authority (HRA), and relevant Research Ethics Committees (RECs). This SOP will be reviewed annually or upon significant changes to the regulatory framework to ensure continued compliance.

With the continued evolution of available technologies and methods to support data management, the Medicines and Healthcare Products Regulatory Agency (MHRA) released Data Integrity Guidance and Definitions in 2018 to provide updated expectations for Good Clinical Practice (GxP) in relation to data management for clinical trials (see references). However, the underlying regulatory requirements remain the same. Regulatory requirements for data management of Clinical Trials of Investigational Medicinal Products (CTIMPs) also apply to medical device trials and trials of Advanced Therapy Investigational Medicinal Products (ATIMPs).

## 2 Purpose and Scope

This Standard Operating Procedure (SOP) describes the requirements and expectations for the management of trial data for RGEIT Clinical trials sponsored by The University of Manchester, and it outlines the processes by which the University maintains oversight of data management activities when these are delegated to third parties.

This SOP applies to such trials in conjunction with all applicable University policies and procedures (for UoM employees) and the policies and procedures of the relevant NHS Trust and/or contracted vendor.

## 3 Definitions

**Data Management System (DMS):** A Data Management System is the system used to store, manage, and process clinical trial data captured via the Case Report Form (CRF). A DMS may be paper-based or, more commonly, electronic (e.g., software platform or database). The type, size, and complexity of the system should be proportionate to the needs of the trial and may range from a simple spreadsheet to a fully validated, custom-designed clinical database. A DMS must be fit for purpose and support data integrity in line with MHRA GxP expectations.

**Database:**

The database is the structured data repository within the DMS where trial data are stored. The database alone does not constitute a full Data Management System**.**

**Source data**:
Source data are the original records where trial-related information is first captured (e.g. hospital records, laboratory notes, subjects' diaries, x-rays). Documents that record source data are classified as "essential documents" that allow evaluation of the trial and ensure the quality of data. They are essential for the purposes of ensuring compliance with GCP and regulatory requirements. Source data must be attributable, legible, contemporaneous, original, and accurate (ALCOA).

**Case Report Form (CRF)**:
A printed or electronic form designed to record all the protocol-required information. CRFs are used to document data that will be entered into the trial's Data Management System.

**Special category data**: Special category data refers to personal data that are more sensitive and require additional protection under UK GDPR. This includes health data, genetic data, biometric data, and any information that could identify an individual or cause harm or distress if disclosed. In clinical trials, this typically includes patient identifiable information received from the NHS. Processing of special category data requires an appropriate lawful basis and condition for processing under UK GDPR.

**Data Validation:** The process of checking data for such things as consistency, protocol compliance, and missing, incorrect or implausible data. The specific checks that are done as part of data validation must be documented, usually in a validation specification in the Data Management Plan. Data validation processes ensure that the trial data are accurate and reliable for analysis. Validation activities must be risk-proportionate and documented.

## 4 Roles and Responsibilities

The Chief Investigator (CI) is responsible for the data management of the trial; however, this may be delegated to an external vendor (usually a UKCRC registered Clinical Trials Unit). Where the role of data management is delegated to an external vendor, the vendor's own data management processes may be followed, however they must be reviewed by the Sponsor at the point of vendor assessment for compliance minimum data management requirements, regulatory expectations, and UoM standards, as outlined in this SOP.

The Chief Investigator (CI):

- Has overall responsibility for the conduct and management of the trial in accordance with the protocol, GCP, and applicable regulations.
- Ensures data collected are accurate, complete, and verifiable from source.
- Approves the Data Management Plan (DMP) and key data-related documents.
- Ensures CRFs and data collection tools are appropriate and align with the protocol.
- Ensures timely resolution of data queries.
- Ensures delegated staff are qualified, trained, and documented on the delegation log.
- Ensures essential data management documents are maintained in the TMF.

- Oversees any delegated data management activities and escalates issues to the Sponsor when required.

The UoM as the sponsor of trials

- Ensures that data are collected, handled, and stored in accordance with the approved protocol, regulatory requirements, and Good Clinical Practice (GCP).
- Ensures that appropriate systems and processes are in place to ensure data accuracy, completeness, and reliability.
- Ensures that any delegation of data management activities is clearly documented, risk-assessed, and subject to appropriate oversight.

The Sponsor provides oversight of all data management activities conducted on behalf of the Sponsor. Responsibilities include:

- Ensuring data management processes comply with applicable regulations, GCP, GDPR and UoM requirements
- Oversight of delegated data management activities, including monitoring vendor performance
- Reviewing and approving external vendor data management processes and quality systems during vendor assessment
- Reviewing and approving key data management documentation (e.g., Data Management Plan, validation documentation, database specifications)
- Ensuring roles, responsibilities and oversight mechanisms are clearly defined and documented
- Ensuring proportionate oversight in line with the UK Clinical Trials Regulations reform (effective 28 April 2026)

CTU / Data Management Team

- Develops and maintains Data Management Plan (DMP).
- Designs Case Report Forms (CRFs) and validation rules.
- Manages database build, testing, and lock.
- Conducts data cleaning and query management.
- Implements data integrity controls in accordance with MHRA GxP Data Integrity Guidance.

Vendors

- Provide validated systems and maintain data integrity.
- Comply with Sponsor oversight requirements.
- Ensure their data management processes meet applicable regulatory standards and are documented within their quality management system.

## 5 Related Documents

| Reference Number | Document Title |
|---|---|

| | |
|---|---|
| UoMCTSOP14 | Independent Data Monitoring Committee and Trial Steering Committee |
| UoMCTSOP20 | Archiving |
| UoMCTSOP23 | CRF |
| UoMCTSOP17 | Data Management Appendix 1 |
| NA | Greenlight Checklist (Current version) |

# 6 Procedure

## 6.1 Development of the Data Management System (DMS)

Chief Investigators (or their designated delegate with responsibility for data management), should seek expert advice on the design, build, testing, and deployment of an appropriate Data Management System (DMS), unless they are already suitably experienced or qualified. This should take place well in advance of the planned trial start date.

All electronic data must be stored securely on systems that comply with the University's IT and IG Security Policies and processes. If a vendor intends to use a database that has not previously been used for a UoM sponsored trial, the RGEI team should send the vendor's data management SOPs and the data compliance details described in the vendor assessment to the UoM Information Governance (IG) team at information.governance@manchester.ac.uk. The IG team will confirm whether the arrangements are in accordance with UoM requirements.

For DMSs developed internally by University of Manchester staff within the University IT infrastructure, the study team must ensure the DMS complies with University IT Standard Operating Procedures (see references), and an information governance risk review may be required. The RGEI team should contact the IG team to clarify this and confirm compliance.

The following key elements (not exhaustive) must be considered during DMS development:

- Data collection tools (case report forms)
- user requirements for data entry, processing and reporting
- measures to ensure data integrity (risks documented in the study risk assessment)
- system and data auditing functionality to log access and track changes/corrections
- security of the DMS and the trial data, especially if network connected systems
- access control (authentication) and appropriate authorisation levels
- change control (for patches, upgrades, modifications)
- data storage arrangements
- process for reconciliation with external or separate databases (e.g. pharmacovigilance)
- database lock (including requirements before database lock)
- backup policy, system procedure, system and plan, including regular testing
- archiving policy, system and procedure, including digital preservation considerations

### 6.2 Case Report Form (CRF) Design

Only data that is essential for the purposes of the study should be collected. Statistical input should be sought during trial design.
Consideration should be given as to whether CRF completion instructions are required, or the procedures for completing CRFs may be detailed in the DMP.
The final CRF must be reviewed and approved by the Chief Investigator (CI). A copy of the approved CRF should be provided to the Sponsor prior to the start of the trial.

### 6.3 Database Design and Testing

RGEIT must receive confirmation that any computer systems used for trial data management have been validated. This confirmation forms part of the checks completed prior to granting Sponsor green light for the trial to begin.
The trial-specific database should be developed to reflect the data captured in the CRF. The complexity of the database may vary depending on the complexity of the trial, but simpler databases must be justified based on risk to data integrity.
The database must be tested before it is finalised (for example, against the database design specification), and this testing and any resulting corrections to the database must be documented.
Once testing has been carried out and the database confirmed fit for use, the CI must provide their approval for the finalised database before it is activated for trial use.
Any changes made to the database after activation must be controlled, re-tested, and validated to ensure continued data integrity and compliance with the approved design.

**Sponsor Greenlight Requirements**
Before the database can be activated for trial use, the study team must compile and submit the following documentation to the Sponsor. The Sponsor will review these materials to confirm that the database is complete, validated, and compliant with protocol and regulatory expectations.

**1. Chief Investigator (CI) Approval**
Purpose: Confirms CI review and approval of the final database.
Acceptable formats:
- Signed approval form
- Email confirmation from the CI
- Approval recorded in an electronic workflow system

**2. Database Specification (Design and Build)**
Purpose: Provides the full technical description of the database.
Acceptable formats:
- Database Design Specification (DDS) document (Word or PDF)
- System-generated specification report
- Version-controlled design document stored in the trial master file

**3. Validation Documentation (User Acceptance Testing / UAT)**


SOP is a controlled document. Any printed version of this document may not be current.
It is the responsibility of colleagues to ensure that the most recent version of the document is accessed, and the procedures stated within the document followed.

Purpose: Demonstrates that the database functions as intended.
Acceptable formats:

- UAT summary memo
- Completed UAT test scripts (Word, PDF, or exported system report)
- Defect log (Excel or system-generated)
- UAT completion certificate or sign-off form

A short UAT completion memo is often preferred because it summarises the testing performed, issues identified, and confirmation that all critical findings were resolved.

**4. Security Documentation (Access and Audit Controls)**
Purpose: Confirms that appropriate security measures are in place.
Acceptable formats:

- System security overview document
- Role and permission matrix (Excel or PDF)
- Screenshot or export of audit trail functionality
- System validation summary (if applicable)

**5. Data Entry Instructions**
Purpose: Ensures consistent and accurate data entry across sites.
Acceptable formats:

- Data Entry Guidelines (Word or PDF)
- Site user manual
- System-generated help guide
- Training slide deck (PDF)

**6. Backup and Data Recovery Information**
Purpose: Confirms that data protection and recovery processes are in place.
Acceptable formats:

- System backup policy
- Vendor-provided backup and disaster recovery summary
- IT-issued confirmation memo
- Extract from system validation documentation

### 6.4 Data Management Plan (DMP)

Good Clinical Practice (GCP) requires that quality control is maintained at every stage of data handling—including data entry, processing, and validation—to ensure that trial data are reliable, accurate, and processed consistently. To support this, a trial-specific Data Management Plan (DMP) must be developed using either the University of Manchester online DMP system or another Sponsor-approved DMP template. The chosen template must contain sufficient detail to meet GCP requirements and fully describe all data management processes for the trial.

This is separate and in addition to the data management plan which is completed as part of the PURE system at the funding application stage, which does not contain the level of information required for clinical trials and cannot replace the trial-specific DMP.

DMPs may vary in complexity but may include:

- Map of the data flow from data collection through to final archiving
- Identification of data validation points throughout the data lifecycle
- procedure for data entry, edit checks and system level validation
- procedure for post data entry review and validation
- data protection considerations, including data classification and handling requirements
- backup and data recovery procedures

**Data Management Planning**

For low-risk non-CTIMP trials where the use of a validated database is not planned, a **Data Capture Risk Assessment** (Appendix 1) must be completed to assess the suitability of using alternative data capture methods (e.g., Excel)
The outcome of the assessment must be recorded within the DMP, along with justification for the chosen data capture method. For CTIMPs, a validated database is required. For non-CTIMP studies, Excel may only be used where the risk assessment demonstrates that data integrity, security, and auditability can be maintained.
The completed assessment must be reviewed and approved by the CI and Sponsor before data collection begins.

The DMP should be reviewed and approved by the CI and statistician at a minimum, and final versions sent to the Sponsor, for oversight and confirmation that data management processes are appropriate for the trial.

As the DMP is a live document, any substantial amendments to the protocol, data collection tools, database structure, or other trial processes must include an assessment of whether the DMP requires updating. Where updates are necessary, a revised version must be prepared, reviewed, approved, and re-submitted to the Sponsor.

### 6.6 Data Entry

The CI (or delegated data manager/individual with delegated responsibility for data management) must ensure a process is in place **to receipt, review, coding, and entry** of trial data.

This process must include:

- Receipt of data via Case Report Forms (CRFs) or other approved data collection tools
- Review of submitted data to identify missing, incomplete, inconsistent, or out-of-range values
- Coding and entry of data into the Data Management System (DMS)
- Documentation and resolution of discrepancies, with queries raised to the CI/PI (or delegate) and responses recorded appropriately

On paper-based CRFs, correction fluid must not be used as this will obscure the original data. Any amendments must be made using a single line strike-through, with the correction initialled and

dated by the PI (or delegate) to maintain an audit trail. Coding and entry of data into the DMS should be undertaken by a delegated member of the research team working to a defined data entry process. A double-entry or verification process may be used where appropriate.

### 6.7 Data Processing

The following principles must be adhered to when processing clinical trial data to ensure accuracy, integrity, and compliance with GCP:

- all transactions (insert, change, delete) must have a clear and complete audit trail (less sophisticated electronic systems (e.g. spreadsheets) may require printing/dating of previous versions of the data).
- only authorised personnel should be able to process the data; access rights must be controlled and documented and personnel appropriately trained and delegated,
- authorised data processors are responsible for maintaining data integrity, availability, security and confidentiality.
- if data are transformed during processing, it must remain possible to compare original and derived data to allow reconciliation and verification.
- manual coding of data must be done through appropriate coding lists or dictionaries to ensure consistency and accuracy.

All the above points must be fully documented in the Data Management Plan. All data management risks, including mitigation, must be incorporated into the trial risk assessment to ensure appropriate oversight and proportional controls.

### 6.8 Data Validation

Data validation is undertaken to ensure that all trial data are accurate, complete, and suitable for statistical analysis. Data validation should take place at three stages:

- At CRF completion: Source data validation by cross-referencing CRF entries with source documents
- At data entry: Automatic checks within the DMS and documented manual checks.
- Post-entry: System-generated or manual queries to detect missing values, out-of-range values, and anomalies.

Where algorithms, applications, or digital tools are used, they must undergo appropriate validation with periodic review to ensure continued accuracy and reliability.
Validation checks must continue until all missing values and inconsistencies are identified and corrected. All validation procedures and responsibilities must be documented within the Data Management Plan (DMP).

### 6.9 Data Monitoring

The extent and intensity of data monitoring required during the trial must be determined by the trial's risk assessment. This assessment should define the level of source data verification (SDV) required and identify any critical data or processes that must be verified as a minimum.
Data monitoring procedures are usually described in the Monitoring Plan. If no standalone plan exists, the monitoring strategy must be documented in the protocol or risk assessment.
For large, complex, higher-risk trials, an Independent Data Monitoring Committee (IDMC) should be established.
See UoM SOP14 "Independent Data Monitoring Committee and Trial Steering Committee" for further details.

### 6.10 Database Lock

A process must be in place for locking of the database once data issues have been resolved and data is appropriately clean. Database lock prevents any further changes to the data and ensures the integrity of the dataset used for statistical analysis.
The point at which the trial database may be locked must be justified and documented. The statistical analysis plan for the trial must have been finalised before the database is locked.
A controlled process must also be in place for unlocking of the database, when necessary, for example if a data correction is required, however a database unlock, which should only occur for significant corrections that may influence results. The justification for the unlocking, process, access permissions, re-locking, and audit trial of the changes, must be documented. An audit trail of all changes made during the unlocked period must be maintained.
Any datasets produced before unlock must be retained for traceability.

### 6.11 Data Back-up

The DMS must have a robust back-up mechanism in place to guard against data loss, system failure or disaster scenarios, ensure that trial data remain secure, retrievable, and intact throughout the duration of the study.
The University of Manchester provides a range of storage facilities that provide a reliable means of automatically backing up data and recovery. A twin data centre operation is in place to provide resilience and disaster recovery. Customisable backup and recovery plans can be specified as part of the service design process.
Chief Investigators (CIs) should consult University IT Services for guidance on appropriate back-up arrangements and to ensure that the selected solution meets institutional and regulatory requirements. (http://www.itservices.manchester.ac.uk/research/).

### 6.12 Data Transfer

Any transfer of data must be justified, with appropriate agreements (e.g., Data Sharing Agreements, Data Processing Agreements, or contractual clauses).
The transfer process must be robustly designed, validated, and risk assessed to ensure that data integrity is maintained throughout.
This includes:

- secure and approved transfer methods, including encryption where appropriate

- verification procedures to confirm successful and complete transfer
- documentation of the transfer, including sender, recipient, date, and dataset version
- controls to prevent unauthorised access, corruption, or loss of data

Advice may be sought from the University IG Office on recommended procedures and approved technologies and secured data transfer mechanisms.

### 6.13 Data Archiving

It is a legal requirement that data from Clinical Trials is retained for at least 5 years after the trial has closed. For trials supporting a marketing authorisation, the retention is typically between 25–30 years. The required retention period must be confirmed during trial planning.

Consideration of appropriate archiving for trial data should take place during the trial design and costing phase. This includes identifying suitable storage solutions, ensuring long-term accessibility, and budgeting for secure archiving. (see UoM SOP on Archiving for further details).

*Chief Investigators should seek advice from the University's Information Governance Office for detailed guidance on archiving requirements and compliance. For electronic data, CIs should also consult University IT Services to ensure that archiving solutions meet institutional, technical, and regulatory standards.*

### 6.14 Data Protection

Throughout the data management process, it is essential that data is kept in accordance with GDPR (UK General Data Protection Regulations) and the Data Protection Act 2018. Compliance with data protection legislation is a legal requirement and applies to all stages of data collection, processing, storage, transfer, and archiving.
All special categories information (within the University's definition of the term) on paper must be kept physically secure with access restricted to authorised personnel only.
See the University's "Information security classification, ownership and secure information handling SOP" (in references) for further information.

## 7 References


- The Medicines for Human Use (Clinical Trials) Regulations 2004 (as amended) https://www.legislation.gov.uk/uksi/2004/1031/contents
- UK Clinical Trials Regulations 2026 (effective 28 April 2026)) https://www.legislation.gov.uk/ukdsi/2024/9780348267167
- ICH E6 (R3) Good Clinical Practice https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Step4_FinalGuideline_2025_0106.pdf
- University of Manchester DMP Online: https://dmponline.manchester.ac.uk/?perform_check=false
- University of Manchester Information Security Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525

- University of Manchester Information security classification, ownership and secure information handling SOP: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971
- University of Manchester Guide to Data Handling: http://documents.manchester.ac.uk/display.aspx?DocID=19941
- MHRA Data Integrity Guidance 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf
- UK GDPR and Data Protection Act 2018 https://www.gov.uk/data-protection

## 8 Appendices

Appendix 1

Data Capture Risk Assessment Form