UNIVERSITY OF LINCOLN

CLINICAL GOVERNANCE - STANDARD OPERATING PROCEDURE

DATA MANAGEMENT

CG-QMS SOP CGD2

Version Final 1.0 Date 01 May 2021

Effective Date: 01 August 2021

Next review: 2 years

Author:	**Elise Rowan** Data Manager (CaHRU)
Approved by: Signature:	UREC See original

Version History	**Reason for change**

NOTE: All SOPs are subject to regular review.

Please ensure that the version of this SOP is the most up-to-date.

OUT OF DATE DOCUMENTS MUST NOT BE USED AND HARD COPIES SHOULD BE DESTROYED

1 PURPOSE

This Standard Operating Procedure (SOP) describes the general procedures for accurate and secure data collection and management (on paper and/or using electronic data capture systems) for clinical and health-related studies and clinical trials at University of Lincoln, UK.

2 SCOPE

This SOP applies to all UoL sponsored clinical research or where LinCTU (Lincoln Clinical Trials Unit) are holding in data in databases for clinical studies and clinical trials.

3 BACKGROUND

2.1 The procedures outlined here are aimed to ensure that data is collected, quality-checked, and stored appropriately to maintain high scientific and ethical standards.

2.2 In addition to the principles of Good Clinical Practice (GCP) and the University of Lincoln Research Data Management Policy, clinical research/trial data and personal data shall be collected, recorded and managed in accordance with the UK Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

2.3 Sponsor: The sponsor will ensure that investigators maintain control of, and continuous access to, data throughout the study and request updates for regulatory purposes as required.

2.4 Chief Investigator (CI): The CI for each clinical study or trial will act on behalf of the sponsor to manage the data but may delegate data management tasks.

2.5 CRFs can be paper-based and/or electronic and the trial protocol, or other study document must specify which data is stored (whether paper based and/or electronic) and which elements of data are to be retained on archiving.

2.6 The number of personal data items stored shall be kept to the minimum required for conducting the study and for maintaining the safety of participants.

2.7 All computers used for entering and accessing study/trial data shall have appropriate security software installed in accordance with University ICT policy.

2.8 The number of personal data items stored shall be kept to the minimum required for conducting the study and for maintaining the safety of participants.

4 CROSS REFERENCES

4.1 CG-QMS CG09-RF01 Screening and Enrolment Log

4.2 CG-QMS Data Monitoring Committee

4.3 CG-QMS RF CG08-RF01 Study Delegation Log

4.4 CG-QMS SOP CG15 Archiving (Clinical Data)

4.5 CG-QMS SOP CGD1 Data Protection and Confidentiality

4.6 CG-QMS SOP CGS2 Statistical Analysis Plan

4.7 RG-QMS RG03 Document Control – (Study documents)

4.8 Trial / Study Case Report Form

4.9 University of Lincoln Data Protection Policy

University of Lincoln Record Retention and Disposal Policy

https://cpb-eu-w2.wpmucdn.com/blogs.lincoln.ac.uk/dist/8/8024/files/2014/04/Record-Retention-and-Disposal-Policy-v1-PDF.pdf

University of Lincoln Research Data Management Policy

https://cpb-eu-w2.wpmucdn.com/blogs.lincoln.ac.uk/dist/8/8024/files/2013/08/Research-Data-Management-Policy.pdf

4.10

5 PROCEDURE

COLLECTING DATA

5.1 The study/trial protocol, or other study document will specify all the data (both personal identifiers and research data) to be collected using Case Report Forms (CRFs) or in any other applicable format.

5.2 The study/trial team members shall be trained to complete the study CRFs (paper and/or electronic versions) prior to beginning their work on the study/trial. Only authorised members of staff are permitted to make entries onto a CRF as recorded on RF CG08-RF01 Study Delegation Log).

PROTECTION OF PERSONAL IDENTIFIERS

5.3 Each participant for whom data is collected must be pseudo-anonymised i.e., assigned a unique identifier (ID) which will be used in the research database/data storage/filing system(s).

5.4 The participant screening and enrolment log (CGXX-RF01) code or file linking participants' personal identifiers (i.e. participant full names, addresses, telephone, email and next of kin contact details) shall be kept secure and separate from the research/trial data which will be used for study analysis. This separation of personal identifiers could be achieved by either:

- Storing the personal identifiers in a completely separate physical or electronic location/file space or system to the main research/trial data.
- Storing the personal identifiers in a more restricted and encrypted section of the research/trial database (such an arrangement may be possible in some electronic data management systems).

5.5 Paper documents with participants personal identifiers (e.g. names address, email, phone numbers) shall always be stored in locked cabinets in locked offices. Electronic files containing personal identifiers shall be password protected.

5.6 In any event, access to personally identifying information must be restricted to only those members of the research team who need the personal information for the purpose of organising the study

5.7 On publication of research data, it is essential that participants are not identified. Special care must be taken to preserve the identity of individuals and careful anonymisation/masking measures shall be utilised when publishing quotations from individuals and/or using digital media (e.g. photographic images, voice recordings and video data).

BLINDING / UNBLINDING

5.8 Where a study/trial protocol requires blinding, data management systems/processes must be in place to facilitate the safeguarding of this and avoid inadvertently breaking the blind. Protocols shall clearly outline how investigators can obtain support from data managers in emergency circumstances where the blind must be broken in order to protect the well-being, and facilitate the medical management, of individual participants.

DATA RETENTION

5.9 Identifiable data shall not be retained for longer than is necessary to meet the requirements described in the study protocol and to meet any requirements set by the grant-awarding body, Research Ethics Committee (REC) and regulatory authorities.

5.10 All Clinical Trials of Investigational Medicinal Products (CTIMPS), Medical Devices, and surgical studies sponsored by University of Lincoln shall be archived in accordance SOP CG15 Archiving (Clinical Data) for a minimum 25 years unless subject to any other third-party obligations (e.g. funder's terms and conditions and legal requirements).

5.11 All other clinical research studies shall be archived in accordance with SOP CG15 Archiving (Clinical Data) for the duration as stated in the protocol, or Sponsor's institutional guidelines.

5.12 Careful consideration and planning must be given to the process of data destruction; whilst electronic data files can be deleted, physical destruction may also be necessary especially where data has been collected by paper records, or other media such as tapes, videos, film and CDs for example.

Trial/study teams should adhere to the University's Record Retention and disposal policy for all data (including personal data) they hold and ensure it is destroyed when no longer required.

The retention periods specified within privacy notices should be reflective of the University Records Retention Schedule, which is contained within the University's Records Management Policy. Further guidance about record retention schedules is available from the Information Compliance Team.

On destruction, personal data in paper form must be shredded and/or sealed in the confidential waste bags provided by the University.

Personal data in electronic form should be deleted. Portable devices that hold personal data may be destroyed by the ICT department if office shredders do not include this capability.

There should be a formal documentation within the research group/LincTU of when any clinical trial/study records are destroyed and this should be notified to the sponsor.

DATA PROTECTION AND SECURITY

5.13 All person-identifiable data must be treated in a confidential manner by the research team members who have access to it. The CI must ensure that the team members understand this before starting the study/trial.

5.14 Paper or computer records containing personal-identifiable data must be accessible by the minimum number of people required for the most efficient and secure administration/management of the study/trial.

5.15 All electronic research data shall be securely backed-up and/or replicated on a regular basis.

5.16 Where data is stored in files on removable media, stand-alone computers, laptops and mobile devices or on tape recorders and cameras then it shall be regularly copied/backed-up/uploaded to another secure central storage location (for example cloud based One Drive or server-based storage). N.B. OneDrive is the current solution for this at University of Lincoln and it is recommended that Microsoft Teams is used to create project specific file spaces with restricted access by research team members.

5.17 All lap-tops and mobile devices shall be encrypted and password protected and stored securely when not in use. All laptops and mobile devices shall be maintained in accordance with CGXX Information Security.

5.18 Data used for study/trial analysis must be pseudonymised (see 5.3-5.7).

5.19 Personally identifying data (e.g. participant names, addresses, telephone, email and next of kin contact details) shall be stored separately from the data used in the study /trial analysis (also see 5.4) and can be used for study/trial administration and day to day management (e.g. contacting participants, arranging assessments) Access to study/trial data shall be limited to authorised personnel in accordance with SOP CG08 Trial Initiation as recorded on the RF CG08-RF01 Study Delegation Log.

PERSONAL DATA TRANSFER

5.20 Clear processes for transfer of personal data within trial/study management teams and between collaborating sites must be agreed before starting a trial/study. Data shall not be transmitted in a way that could cause loss of data or allow access by unauthorised parties.

5.21 Personally identifying data shall not be stored or transmitted on removable media or laptops without encryption. Datasets of this nature shall be encrypted before transfer or transmitted/shared securely using OneDrive or other systems approved by University of Lincoln and any collaborating NHS study partner organisations. Guidance on How to Send Personal and non-Public Information is available from ICT. for this using the University of Lincoln Office 365 Environment is given at:

DATA AUDIT, DATA QUERIES AND DATA LOCK

5.22 Where electronic data capture systems are used in studies/trials (see 5.27-5.31), these systems shall have an audit trail to record any changes to electronic data following initial data entry. The audit trail shall show who made the change, when it happened and, where appropriate, include a note explaining the reason for the change.

5.23 In any studies/trials where it has not been possible to use a modern electronic data capture system (as may be the case in studies with very limited resources and/or set up during the early development of the Lincoln Clinical Trials Unit), it is recommended that trial/data managers keep an email record of data queries raised with investigators/researchers and any associated responses. If paper records are kept and data entered centrally or retrospectively, we recommend the use of file notes and the practice of initialling and dating any amendments to paper records (see 5.32-5.42).

5.24 Data quality shall be reviewed regularly (including Source Data Verification (SDV). Data queries shall be raised as soon after data capture as possible. These may include missing, inconsistent or implausible data.

5.25 At the end of a trial or study, and once all data queries have been addressed as fully as possible, data shall be locked to prevent further additions or changes. In electronic data capture systems this can be facilitated using the system's file-locking facility. Otherwise, a "snapshot" of the finalised data shall be taken for analysis and all further access to the data denied to anyone except the data manager and/or statistician. The "snapshot" data file shall be clearly labelled and dated to indicate that it is the final locked dataset.

5.26 Data provided for analysis shall always be verifiable against source data

Note: a CRF may serve as source data but shall be clearly documented as such.

ELECTRONIC DATA CAPTURE (EDC)

5.27 Electronic data capture systems shall reflect the layout, design and content of data capture documents/proformas.

5.28 Electronic data capture systems shall allow data validation, range checks, consistency checks and employ the use of features such as input masks to ensure accurate and high-quality data entry.

5.29 Where data is captured at more than one time point for each participant, the system will have the flexibility to capture the name description of the scheduled study time-point (e.g. baseline, visit 1) as well as the actual date and if necessary, time that is was carried out.

5.30 If necessary, data entry checks or double data entry will be considered for critical data.

5.31 Data queries and data anomalies with be handled according to study specific guidelines.

PAPER CASE REPORT FORMS (CRFS)

5.32 Paper CRFs shall be version controlled, paginated and dated in accordance with RG-QMS RG03 Document Control – (Study documents).

5.33 Unique Participant ID will be documented at the top of each page.

5.34 Study ID (e.g. IRAS ref) and name shall be documented in the header/footer of each CRF page.

5.35 No personally identifiable information (as described in 5.3 above) shall be recorded in the CRFs

5.36 Paper CRFs shall capture all data and procedures to be carried out on each participant at each visit as defined by the study protocol. No additional information shall be collected above and beyond this.

5.37 Paper CRFs shall be completed in permanent ink.

5.38 Any errors shall be crossed through once, corrected then initialled and dated by the researcher. The original value/errors shall still be visible for reasons of audit/transparency. If necessary, file notes can be appended to the CRF to further explain edits/corrections.

5.39 All required fields shall be completed. If a procedure is not carried out, then this shall be noted.

5.40 CRFs shall clearly indicate units of measurement where appropriate.

5.41 Paper CRFs shall be designed to avoid the need for free-hand text as much as possible. This will facilitate more accurate data transfer into the study/trial database and coding prior to analysis.

SCANNED IMAGES

5.42 Scanned images must be at appropriate resolution so that when viewed at actual size on the screen (as per the original) the image is clear and legible. Post-scan adjustments to the image to increase legibility are acceptable, provided the limits of what may be undertaken is clearly specified in a formal procedure. It is not acceptable to utilise the scanning process to remove or add material to the image, for example, to remove the header a fax machine has added, or undertake physical 'cut and paste' or 'correction fluid' activities on the original paper record.

DATA ANALYSIS

5.43 Data must be analysed in accordance with a statistical analysis plan which shall be developed taking into account the guidance in the Statistical Analysis Plan SOP (see CG SOP 015 Statistical Analysis Plan).

5.44 Quality checks as described in the Statistical Analysis Plan shall include but not be limited to: checking for outliers, missing data, accuracy/plausibility of dates (particularly if used in calculations), and inconsistencies.

5.45 Data shall be exported into an appropriate format(s) for analysis as per the requirements of the study statistician.

5.46 When data are exported for analysis, the data shall be fully anonymised.

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

6. FLOW CHART

None required.