UNIVERSITY OF LINCOLN

CLINICAL GOVERNANCE - STANDARD OPERATING PROCEDURE

DATA PROTECTION AND CONFIDENTIALITY

CG-QMS SOP CGD1

Version Final 1.0 Date 01 May 2021

Effective Date: 01 August 2021

Next review: 2 years

Author:	Sam Lewis Research Governance Manager
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OUT OF DATE DOCUMENTS MUST NOT BE USED AND HARD COPIES SHOULD BE DESTROYED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

To ensure personal data collected during the course of a clinical trial (including trial management) is in accordance with legal requirements and University of Lincoln Policy.

2. SCOPE

This SOP applies to all UoL sponsored clinical research or where Lincoln Clinical Trials Unit (LinCTU) are handling personal data of trial participants or trial staff.

3. BACKGROUND

3.1 Data protection legislation (GDPR and the Data Protection Act 2018) provides a framework for organisations (known as “controllers” which is defined as body which, alone or jointly with others, determines the purposes and means of the processing of personal data.). This ensures personal data is handled properly, as well as providing legal rights to individuals on which their personal data is being used (known as “data subjects”).

3.2 The legislation works in two ways: (i) it states anyone who processes personal data must comply with the data protection principles, as defined by the relevant data protection legislation (ii) it provides individuals with important rights, including the right to find out what personal data is held in both digital and paper records.

3.3 Personal data should only be processed for the specific purpose contained in the relevant privacy notice which was provided when the data was collected.

3.4 A privacy notice should identify who the data controller is, with contact details for its Data Protection Officer. It should also explain the purposes for which personal data are collected and used, how the data are used and disclosed, how long it is kept, and the controller's legal basis for processing.

Clinical Trial Data

3.5 This is information as numerical or text values found within paper and electronic records including images and sound

Examples include:

- Trial reports
- Case report forms
- Electronically transferred documents including emails and attachments
- Trial databases
- Photographs
- x-rays

Personal data

3.6 Personal data is any information relating to an individual who can be directly or indirectly identified, by reference to an identifier, such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Examples of categories of personal data in clinical trials include:

- Name
- Date of birth
- Address
- NHS / Hospital Number

Special Category Data

3.7 Special Category (formerly known as sensitive personal) data is a subset of personal data and means personal data consisting of information relating to;

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,

- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- Genetic data (used for identifying an individual),
- Biometric data (used for identifying an individual),
- Data concerning an individual's health,
- An individual's sex life or sexual orientation.

Personal data breach

3.8 A personal data breach may arise from

- a theft
- a deliberate attack on University / Clinical Trials systems
- unauthorised use of personal data
- accidental loss
- by disclosure (including emails, containing personal data being sent to the wrong recipient)
- equipment failure

Anonymised Data

3.9 Data for which it is impossible to identify the participant from the information or any other information held.

Pseudonymised data

3.10 Trial participants are given an identifier by which they are known in a system (e.g. in a Case Record Form or in a computer database), which is typically a number or other unique identifier. One master list with the identifier and participants' details must be kept separately in order to link the participant to their data. GDPR makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR (known as Recital 26 of GDPR).

Sponsor

3.11 The Sponsor has overall accountability for handling and maintaining personal clinical research data in such a way as to satisfy legal and University requirements for security and privacy. This may be delegated in a written agreement. The Sponsor is also responsible for reporting a data breach to the University's Information Compliance Office. Where the data breach involves another organisation, this shall be reported in accordance with any local organisation requirements.

Chief Investigator (CI) / Principal Investigator (PI) / Lincoln Clinical Trial Unit (LinCTU)

3.12 The CI, PI or the Director of LinCTU are responsible for data confidentiality and security within a clinical research study including ensuring all clinical research staff are appropriately trained, equipped and made aware of their individual legal and ethical responsibilities.

All Clinical Research Staff

3.13 Clinical research staff are responsible for handling all data in accordance with their individual legal and ethical responsibilities.

4. CROSS REFERENCES

4.1 CG-QMS CG04 Protocol Development

4.2 CG-QMS CGD2 Data Management

4.3 Data Protection Act 2018

4.4 GDPR – General Data Protection Regulations

4.5 University of Lincoln Policies:

University of Lincoln Data Protection Policy

ICT Information Security Policy

Information Systems Acceptable Use Policy

How to send Personal Data, Special Category Personal Data and Non-Public Information

5. PROCEDURE

TRIAL PROTOCOL, PARTICIPANT INFORMATION SHEETS (PIS) AND INFORMED CONSENT FORMS (ICF)

5.1 Protocols should be developed in accordance with SOP CGXX Protocol Development.

5.2 Arrangements for data protection and security should be clearly described in the trial protocol and should be in accordance with Annexe 2 of the University's Data Protection Policy (University of Lincoln Data Protection Policy).

5.3 Participant Information Sheets and Informed Consent Forms should contain information on:

- the items of personal data to be collected, including whether participants could be identified
- the lawful basis for the processing of that data
- how the data will be used
- details of any organisation that will collect, store and process the data
- details of any data transfers
- the intended duration of data retention.

5.4 Clinical research data should be classified and handled according to how critical and sensitive they are.

DATA SECURITY (PAPER OR ELECTRONIC DATA)

5.5 As with all clinical research data, personal data should be stored securely and retained for only as long as is necessary. Access to the data must be restricted to relevant members of staff, authorised by the Sponsor, CI, PI or host organisation. Staff should be granted access to data where access is restricted to only those resources absolutely required to perform routine, legitimate activities (often referred to as "least-privilege basis").

5.6 All IT systems and/or third-party organisations used to store, process or transmit any clinical research data must be compliant with the University's Information Security Policy and baseline IT security requirements.

TRANSFER OF PERSONAL DATA

5.7 Any transfer of personal data must be done securely and in line with the University's Information Systems Acceptable Use Policy, and the Sharing Personal and Special Category Data Guidance document. Personal data should be encrypted in accordance with ICT How to send Personal Data, Special Category Personal Data and Non-Public Information. See also Section 4.5 and 4.6 of the University' Data Protection Policy.

PERSONAL DATA BREACHES

5.8 Potential personal data breaches should be reported to the University's Information Compliance Team and the ICT Helpdesk as soon as possible so mitigation techniques can be implemented quickly to limit any potential repercussions.

5.9 See Section 5 of the University's Data Protection Policy.

6. FLOW CHART

Not required.