Standard Operating Procedure CCTU/SOP029

Data Transfer

1. Scope

This Standard Operating Procedure applies to staff of the Cambridge Clinical Trials Unit and trial teams working on Cambridge Sponsored CTIMPs or clinical trials led by the CCTU.

2. Purpose

The purpose of this SOP is to define the principles and practices of data transfer between the Cambridge Clinical Trials Unit and other institutions and/or personnel in accordance with Trust Policy, NHS England Confidentiality Policy, The Data Protection Act and The Information Commissioners' Office

Both electronic and paper data are considered in this SOP.

For each type of data transfer, methods and practices must be followed to ensure:

- The security of the data
- The maintenance of participant anonymity
- The utility of the data
- Successful transfer and receipt of data

3. Definitions and Abbreviations

The headings below contain the definitions of terms and meaning of abbreviations used within the document.

3.1. Definitions

Term	Definition
Cambridge Sponsored	Sponsored by Cambridge University Hospitals NHS Foundation Trust (CUH); or the University of Cambridge (UoC); or jointly by CUH and UoC or Cambridgeshire & Peterborough NHS Foundation Trust (CPFT) or CPFT jointly with the University of Cambridge

3.2. Abbreviations

Abbreviation	Meaning
CCTU	Cambridge Clinical Trials Unit
CRF	Case Report Form
CSV	Comma Separated Variable File
CTIMP	Clinical Trial of Investigational Medicinal Product
GDPR	General Data Protection Regulations
R	Statistical Package

R&D	Research and Development
SAE	Serious Adverse Event
SAS	Statistical Package
Stata	Statistical Package
TMF	Trial Master File
PID	Personal Identifiable Data

4. Undertaken by

Staff of the Cambridge Clinical Trials Unit, Chief Investigators and their trial teams.

5. Items Required

NA

6. Summary of Significant Changes

Clarification to data transfer of trial related documents in section 7.6.1, and questionnaire procedures 7.7.5

Addition of action to be taken if the CCTU receives unauthorised PID in section 7.9

7. Method

The following sections provide a description of the processes to be followed when implementing this document's procedures.

7.1. Responsibilities

- Staff must have attended The Trust induction programme, signed the Information Governance Code of Conduct for new starters, and be compliant with mandatory corporate refresher training, which includes the information governance refresher
- Both the sender and the recipient are responsible for ensuring the successful transfer of data.

7.2. Data Classification

- The appropriate method is dependent on the classification of the data based on the identifiers used
- Any member of staff unsure about the classification of data should seek advice from the CCTU Data Management Team or the relevant R&D contact

7.3. Personal Identifiable Data (PID)

- Personal identifiable data are identifiers that can be linked to an individual if found by a member of the general public
- These consist of but are not restricted to:
    - Patient name

- Combination of Initials and DOB
- Postal address, phone numbers and email address
- Postcode
- NHS number
- Hospital number

7.3.1. Other Potential Identifiers

With coded/pseudo-anonymised (or 'pseudonymised') and unlinked anonymised data, there are occasions where it is possible to deduce an individual's identity through combinations of information.

The most important potential identifiers are:

- Rare disease or treatment, especially if an easily noticed illness/disability is involved
- Partial post-code or partial address
- Place of treatment or health professional responsible for care
- Rare occupation or place of work
- Combinations of birth date, ethnicity, and date of death

To protect the identity of any individual participating in research, extra precautions should in place before transferring and publishing information.

7.3.2. Coded or Pseudo-anonymised Data

- Coded data is where PID is concealed within a code and can only be 'decoded' by the person receiving/holding the data (e.g. co-ordinating site)
- Pseudo-anonymised data is defined by UK GDPR as data resulting from 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'
- It is important that by removing as many identifiers as possible, the utility of the data is not unduly compromised
- Routinely three identifiers are used. This way, if one identifier is compromised or unclear, a deduction of the correct trial subject ID is still possible, so data can be used
- Examples of coded and pseudo-anonymised data in clinical research include but are not restricted to:
  - Trial number
  - Barcode Number (coded)
  - A combination of initials and trial number and date of birth (pseudo-anonymised)

7.3.3. Unlinked Anonymised Data

Unlinked anonymised data cannot identify the individual by any means.

As a minimum, it must not contain any of the following, or codes of the following:

- Name, address, phone number, e-mail address, full postcode
- NHS number, any other identifying reference number
- Photograph or names of relatives

7.3.4. Non-personal Data

Public divulgence of non-personal data should present no risk to confidentiality.

Non-personal data is not directly related to an individual (for example, cumulative recruitment figures).

7.4. Research Sensitive Data

The data itself may be sensitive to the research, for example:

- Safety and efficacy data not in the public domain (i.e. annual safety report, DMEC report by treatment arm)
- Paper case report forms
- Raw statistical datasets (e.g. outputs from SAS, R, Stata)
- Files downloaded from the trial database (e.g. CSV files)

7.5. Consent

The transfer of personal data must be conducted in compliance with the General Data Protection Regulation (GDPR). Before transferring personal identifiable or coded/pseudo-anonymised data, appropriate informed consent must be obtained or data must meet the relevant exemption criteria set out in section 7.8.

7.6. Data Transfer

7.6.1. Trial Related Documents

Coded or sufficiently (pseudo-) anonymised trial related documents, like CRFs and SAE forms, can be sent to the data centre/coordination centre by email.

Trial documents containing PID often need to be sent to CCTU for the purpose of conducting participant follow up assessments centrally. Such PID containing trial documents are sent to CCTU via secure email (e.g. nhs to nhs or similar as per 7.7.4) and into a specific PID email inbox. Access to the PID inbox is restricted to staff who are delegated to manage PID and is separate to the general trial email inbox (where CRFs and other trial documents and communication are sent to).

7.7. Approved Data Transfer Methods

7.7.1. Standard Post

For unlinked (fully anonymised), coded and pseudo-anonymised only.

This method cannot be tracked or guaranteed, therefore no patient information which allows for the identification of an individual should be sent via this method.

7.7.2. Tracked and Signed Post

This method can be used for the transfer of all data groups; however it should only be used as a last resort. This includes:

- Courier services
- Royal Mail tracked and signed for service, which ensures that the parcel/package can be tracked at all times and that a signature of receipt is obtained

7.7.3. Egress Large File Transfer Service

This is an NHS approved service for the transfer of large files (up to a maximum combined file size of 5GB). An NHS.net account is required to send files (via the web form at https://lft.nhs.net/), but not to receive them. Further information about the service can be found on the NHSmail Knowledge Base (https://support.nhs.net/knowledge-base/egress-large-file-transfer-web-form/).

7.7.4. Email

- Documents containing information which potentially allows for the identification of the person can be sent via email, but this must be done using one of the following secure methods:
  - 7-Zip encryption:
    - This is in the form of an encrypted file using a 8 or more digit password containing upper & lower case and numerical characters
    - The encrypted file should be sent as an attachment to an email
    - The password should be sent in a separate email
  - NHS.net to NHS.net (or DCB1596 secure email standard) email accounts
    - A current list of organisations with DCB1596 accreditation can be found on the NHS England website
  - NHSMail secure service:
    - Include [secure] in the subject line when sending from an NHS.net email account
- Only professional email addresses shall be used for the transfer, and no data shall be sent to private accounts in accordance with trust policy
- Data should only be sent to a named individual or a named group such as a 'Data Monitoring Ethics Committee (DMEC)' or 'Trial Steering Committee (TSC)'
- Further information can be found with the Trust's Information Governance and Information Security policy

7.7.5. Questionnaires sent to Participants

Questionnaires should be coded or pseudo-anonymised before sending to participants. They must be sent via the REC approved process as detailed in the IRAS form.

7.7.6. SAE Reports

When reporting an SAE to an external organisation, all patient identifiers other than the patient trial number, initials, and date of birth must be removed before the report is emailed.

If an SAE form is received containing PID this must be obscured in either of the following ways:

- Using white sticky paper or marker pen and then photocopy
- Using the redact tool on Adobe Acrobat Pro DC

The original file should then be deleted, and any hard copies destroyed via confidential waste.

Breaches of confidentiality must be reported, as set out in section 7.10.

7.8. Additional Information

All data files sent should be stored in an appropriate study/trial specific folder within the secure electronic storage environment of the Trust (or the University of Cambridge, if applicable).

7.9. Receiving Data

Any personnel receiving data should acknowledge receipt of the data. This receipt may take any number of forms:

- Acknowledgement email; manually generated – for ad hoc data transfers
- Acknowledgement email; automated – for regular electronic data transfers

If requesting routine healthcare data from a national registry, the identifiable cohort file must only be provided to the registry via their secure file transfer website.

If we receive unauthorised PID from sites:

- Obscure the PID as per 7.7.6
- Delete or destroy the original copy
- Instruct the site to report as per their local policies

7.10. Breaches in Confidentiality or Data Protection

If a CUH Trust employee breaches confidentiality/data protection then a Datix report should be submitted in line with the Trust's Information Governance Incidents and Investigation policy. Additionally, the Regulatory team and Operations Director should be informed so that they can establish:

- If staff have current mandatory training status
- The facts around the breach by conducting an internal investigation
- If the incident should be escalated
- If the breach should be reported via the Trust Incident Process
- If any corrective and preventative actions are required and feedback to all staff

8. Monitoring Compliance with and the Effectiveness of this Document

a. Process for Monitoring Compliance and Effectiveness

As part of routine monitoring visits, audit and inspection

b. Standards/Key Performance Indicators

This process forms part of a quality management system and is reviewed according to CCTU procedures. Standard Operating Procedures are reviewed every two years.

9. References

1. MHRA, Good Clinical Practice "Grey Guide"
2. NHS England – Confidentiality Policy
3. Data Protection Act (2018)
4. Trust Data Protection Policy & Procedure
5. Trust Information Governance and Information Security Policy
6. Trust Information Governance Incidents and Investigation Policy
7. NHSmail Knowledge Base - Egress Large File Transfer Web Form

10. Associated Documents

NA

11. Equality and Diversity Statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

12. Disclaimer

It is the user's responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

Review date	2 years (or earlier in light of new evidence) from approval date
Owning department:	CCTU QA
Supersedes:	CCTU/SOP029 V4
Local reference:	CCTU/SOP029 V5