Standard Operating Procedure CCTU/SOP029

Data Transfer

1. Scope

This Standard Operating Procedure applies to staff of the Cambridge Clinical Trials Unit and Chief Investigators and their trial teams whether substantially employed or holding an honorary contract working on CTIMPs or clinical studies coordinated 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 (ico)

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.

Common abbreviations and definitions can be found in CCTU/INF001 Common Abbreviations and Definitions.

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

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

4. Undertaken by

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

5. Items Required

Safe haven fax

6. Summary of Significant Changes

Clarification of PID and anonymisation

7. Method

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

7.1. Data Classification

Any member of staff that is unsure about the classification of data should seek advice from the CCTU Data Management Team or the relevant R&D contact.

7.1.1. Personal Identifiable Data As defined by Data Protection Act 1998 or as amended

- Publicly 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
    - Postal address, phone numbers and email address
    - Postcode
    - NHS number
    - Hospital number

7.1.2. Other Potential Identifiers

- With coded/ pseudo-anonymised 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

7.1.3. Coded or Pseudo-anonymised Data

- Coded data is where personal identifiable data is concealed within a code and can only be 'decoded' by the person receiving and holding the data (e.g. co-ordinating office)
- Pseudo-anonymised data is prepared from elements of personal information (PID) in a combination that cannot identify an individual by anyone other than those responsible for that individual's care (e.g. site staff).In Clinical Trials this process is the commonly used to pseudo-anonymise documents
- 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
- This may consist of but is not restricted to:
    - Trial number
    - Barcode Number (coded)
    - A combination of initials and trial number and date of birth (pseudo-anonymised)

7.1.4. 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/fax number, e-mail address, full postcode
    - NHS number, any other identifying reference number
    - Photograph or names of relatives

7.1.5. 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

7.2. Research Sensitive Data

- The data itself may be sensitive to the research of the trial 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 (outputs from SAS, R, Stata etc)
    - CSV files downloaded from the trial database
    - Database downloads

7.3. Consent

- The transfer of personal data is covered by the Data Protection Act 1998
- Before transferring personal identifiable or coded/pseudo-anonymised data:
    - Appropriate consent must be obtained or
    - Data should meet relevant exemption criteria as in 7.5

7.4. Data Transfer

7.4.1. 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 secure fax and email
- The method of transfer for all trial related documents containing PID which allows a recipient to identify the actual person must only be sent through:
    - Secure fax
    - Tracked and signed post
    - No other method should be used in these circumstances

7.5. Approved Data Transfer Methods

7.5.1. Standard Post

- For unlinked (fully anonymised), coded and pseudo-anonymised only
- This method cannot be tracked or guaranteed, therefore no patient information which allows to identify an individual should be sent via this method

7.5.2. 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, this ensures that the parcel/package can be tracked at all times and ensures a signature of receipt is obtained

7.5.3. Fax

- Faxes containing personal identifiable or coded/pseudo-anonymised data should only be sent to a stated safe haven fax within a secure office

- Faxes to general fax machines should only contain unlinked and non-personal data
- For all faxes sent containing data of any type, a fax report/receipt will need to be produced and filed with the relevant data
- All recipients will need to be contacted after each fax has been sent to ensure delivery/receipt
- Refer to Trust Policy for further information regarding safe haven process

7.6. Exceptional Cases

7.6.1. Email

- All documents containing information which allows to identify the person through PID sent by email must have digital security
- 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
- For all other data sent by email a strong password should be used
- Only professional email addresses shall be used for the transfer and no data shall be sent to private accounts in accordance to trust policy
- All transfer of data via NHS.net to NHS.net email accounts is encrypted as referenced in the IT Internet and email use policy
- The 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)'
- The sender should request a read receipt for the data and file them within the TMF

7.6.2. Questionnaires sent to Participants

Questionnaires should be coded or pseudo-anonymised before sending to participants. This can be sent out via the standard postal system.

7.6.3. 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 faxed/emailed
- If a SAE is received with personal identifiable information this should be obscured
- Use white sticky paper or marker pen and then photocopy
- The original should then be destroyed via confidential waste
- Breaches of confidentiality as above must be reported as in 7.9

7.7. 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.

7.8. 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
    - Acknowledgement email on receipt of a fax

7.9. Breaches in Confidentiality or Data Protection

- Follow Trust Policy – always check the latest policies and procedures

  Inform the team lead who will:
    - Establish that staff have current mandatory training status
    - Conduct an internal investigation to gather the facts around the breach
    - Establish if the incident should be escalated
    - Establish if the breach should be reported via the Trust Incident Process
    - Identify any corrective and preventative actions and feedback to the rest of the 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. Documents are reviewed every two years

9. References

NHS England – Confidentiality Policy (Version 2.0, 2014)
Data Protection Act (1998)
Trust Data Protection Policy & Procedure
Trust Governance and Information Security Policy
MHRA Good Clinical Practice "Grey Guide" (2014)

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 V2
Local reference:	CCTU/SOP029 V3