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 working on Trust-Sponsored 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. Both electronic and paper data are considered in this SOP. For each type of data transfer, set methods and practices should be followed to ensure:

- the security of the data
- the maintenance of participant anonymity
- Successful sending 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
Trust-Sponsored	Sponsored by Cambridge University Hospitals NHS Foundation Trust (CUH) or sponsored by CUH jointly with The University of Cambridge

3.2. Abbreviations

Abbreviation	Meaning
CCTU	Cambridge Clinical Trials Unit
R&D	Research and Development
SAS	Statistical Package
R	Statistical Package
Stata	Statistical Package
CRF	Case Report Form
CSV	Comma Separated Variable File

TMF	Trial Master File
SAE	Serious Adverse Event
MHRA	Medicines and Healthcare products Regulatory Agency

4. Undertaken by

Both the sender and the recipient are responsible for ensuring the successful transfer of all data. The appropriate method is dependent on the classification of the data based on the identifiers used.

5. Items Required

Safe Haven Protocol

6. Summary of Significant Changes

New

7. Method

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

Precise details of data transfer for each individual study will be outlined in Trial Specific Data Management.

7.1. Data Classification

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, address, postcode, NHS Number etc.

7.1.2. 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 personal information but cannot be identified by anyone other than those responsible for that individual's care (e.g. site staff). This may consist of: Trial number, Barcode Number etc.

7.1.3. 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/fax number, e-mail address, full postcode
- NHS number, any other identifying reference number

- Photograph or names of relatives

7.1.4. Non-personal Data

Non-personal data is not directly related to an individual, for example cumulative recruitment figures.
Public divulgence of non-personal data should present no risk to confidentiality.

7.1.5. Other Potential Identifiers

However with both 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, special precautions should be taken when designing studies, before transferring and publishing information. The appropriate method of transfer should be detailed in the CCTU/TEM Trial Specific Data Management

7.1.6. Advice

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

7.1.7. Research Sensitive Data

The data itself may be sensitive to the research of the trial. Safety and efficacy data not in the public domain is regarded as Research Sensitive. (I.e. Annual Safety Report, DMEC report by treatment arm). Paper Case Report Forms are regarded as Research Sensitive.

Raw statistical datasets (outputs from SAS, R, Stata etc), CSV files or database downloads are also considered as Research Sensitive.

7.1.8. Consent

The transfer of personal data is covered by the Data Protection Act 1998. Therefore appropriate consent needs to have been obtained or the data should meet relevant exemption criteria, before transferring Personal Identifiable or Coded/Pseudo-Anonymised Data.

7.2. The only approved transfer methods are as follows:

7.2.1. Standard Post

This is for Unlinked and Non-Personal Data only. This method cannot be tracked or guaranteed, therefore no patient information should be sent via this method.

7.2.2. Tracked and Signed Post

This includes courier services as well as the 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.
This method is for the transfer of all groups, however should be used as a last resort where possible.

7.2.3. Fax

Faxes containing Personal Identifiable or Coded/Pseudo-Anonymised Data should only be sent to a stated fax within a secure office following Safe Haven protocol.
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.
Please refer to Connect website http://10.154.5.9/index.cfm?articleid=8560 for further information regarding Safe Haven process

7.2.4. Email

All Personal Identifiable or Coded/Pseudo-Anonymised Data sent by email must have digital security. This is to be in the form of an encrypted file using a secure 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. This should also be 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
http://10.154.5.9/media/pdf/r/s/IT_-_internet_and_email_use_policy_280207.ur.pdf
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.

7.3. Exceptional Cases:

7.3.1. Trial Related Documents

The method of transfer for all trial related documents containing Personal Identifiable data should be through secure fax or tracked and signed post. No other method should be used.

7.3.2. Questionnaires sent to participants

For all questionnaires sent to participants, these shall be sent out via the standard postal system to avoid disruption.

7.3.3. SAE Reports

When reporting an SAE to an external organisation, all patient identifiers other than trial number must be removed before the report is faxed/emailed.

7.3.4. Submission to the MHRA

The MHRA require that documentation is submitted on a CD-ROM containing no password protection.

7.4. 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

7.5. 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 emails may be generated on receipt of electronic data.
- Acknowledgement email on receipt of fax.

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

Department of Health.
Data Protection Act, (1998).
Use & Disclosure of Health Data, Information Commissioner's Office, 2002
NHS Code of Confidentiality
Trust Data Protection Policy & Procedure
Trust Internet and Email Use Policy

10. Associated Documents

The following is an excerpt from the Safe Haven protocol.

'Safe Havens: Transfer and Delivery of personal identifiable information

"INFORMATION
Paper: Place in a sealed envelope, addressed to a named individual & include box number. Sending sensitive/confidential information - mark the envelope as private and confidential
Case notes: must be delivered by hand or via medical records courier
Email: only send emails from and to Addenbrooke's email address
EXTERNAL TRANSFER OF INFORMATION
Fax: follow safe haven fax procedures
Post to Patients: Double check you are sending the right person the right information. Address envelope clearly. If sending a mobile device with identifiable data send by special delivery
To external organisations: Post: Must be placed in a sealed envelope, addressed to a named individual, if sending sensitive/confidential information - mark the envelope as private &confidential , consider using special delivery/courier. Mobile device: Must be encrypted and sent by special delivery or courier. Telephone: Request a fax on headed paper or phone back via the switchboard. Fax: use the safe haven fax procedures
Websites: Use secure sites (Https or Fttps), seek Information Governance approval
Case-notes: For outreach clinics must be sent by courier or carried in a locked box/bag
Email: NHS organisations: send from and to an NHS Mail email address Non NHS Organisations: Anonoymise the PID or encrypt an attachment to the email Patients: Consent is needed, if sending administration information verbal consent is required, if sending clinical information then written consent is required on the email consent form and this must be taken face to face March 2010 V1Author: Michelle Ellerbeck'

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:	New
Local reference:	CCTU/SOP029 V1