brighton and sussex medical school

Brighton and Sussex University Hospitals NHS Trust

This is a controlled document
Any printed versions of this document will be classed as uncontrolled
Data Management

SOP Reference:	**SOP/RD/017**
Version Number	**Final V 2.0**
Date:	**26th April 2016**
Effective Date:	30th July 2016
Review by:	29th July 2018

Author: Justine Boles **Designation:** Senior Trial Manager Brighton & Sussex University Hospitals NHS Trust	**Signature**	**Date** 30 June 2016
Authorised By: Scott Harfield **Designation: Head of** Research and Development Brighton and Sussex University Hospitals NHS Trust.		30/6/16

Version	Date	Reason for Change
2.0	26th April 2016	This SOP now refers to non-CTIMP studies. Reference to Research Governance Framework guidelines added. Microsoft Access usage recommendation added to section 4.2. Additional details added to section 4.6

1.0 Purpose

The purpose of this Standard Operating Procedure (SOP) is to describe the procedures for data management for BSUH (Brighton and Sussex University Hospital NHS Trust) sponsored research studies other than CTIMPs (Clinical Trial of Investigational Medicinal Product). All CTIMP studies sponsored by BSUH that are set up from the date of this SOP onwards will be managed by the Brighton and Sussex Clinical Trials Unit (BSCTU) and all CTU SOPs will be followed.

2.0 Introduction

To ensure that the data produced from a research study is accurate and captured in accordance with the protocol, data management processes are required. The aim of any data management process is to get the highest quality dataset suitable for statistical analysis at the end of the study.

International Conference on Harmonisation Good Clinical Practice (ICH GCP) guidelines state that 'All clinical trial information should be recorded, handled and stored in a way that allows accurate reporting, interpretation and verification'. The Research Governance Framework states that 'procedures are kept in place to ensure collection of high quality, accurate data and the integrity and confidentiality of data during processing and storage'. To ensure these principles are adhered to, this SOP provides guidance on how to manage research data for studies sponsored by BSUH.

3.0 Responsibilities

Sponsor
It is the responsibility of the sponsor to ensure data management personnel are appropriately trained.

Chief Investigator (CI)
The CI is responsible for finalising the data collection tool and database prior to recruitment commencing for the research study. The CI is responsible for ensuring any amendments made to the data collection tools are version controlled.

Principal Investigator (PI)
The PI is responsible for ensuring data is collected in accordance with ICH GCP and all data management procedures are carried out correctly at their research site.

4.0 Procedure

4.1 The Case Report Form

The CRF (Case Report Form) captures all of the clinical data for a research study. This will need to be finalised prior to the study starting and any changes to the CRF once the trial has begun must be version controlled. The CRF could be a simple paper form or an electronic CRF (eCRF). Data captured on an eCRF is known as electronic data capture (EDC), where data is transcribed from the source into a database such as a web-based computer application. The R&D team can offer advice as to what system would be most suitable for your research study. The R&D team recommends the use of a CRF for all research studies to ensure consistency of the data collected.

The design of the CRF will be based on the requirements of the protocol. It is recommended that advice is sought from the statistician during the design phase to ensure the relevant information is collected for statistical analysis. If surplus data is captured this increases resources unnecessarily, however, if too little data is collected this may affect what can be analysed at the end of the study.
The data collected on the CRF should be verifiable from the source data. Exceptions to this include where the CRF is source data itself e.g. patient completed questionnaires. It must be specified in the approved protocol if data is to be entered directly into the CRF.

4.2 The Database

The database needs to be secure with appropriate password protected access. The database should also be adequately backed up.

For most studies, Microsoft Access or equivalent is recommended as a minimum, unless otherwise justified to the sponsor when applying for support.

An online training course 'Access 2013 Essential Training' is available to medical school staff and students for free on the Lynda.com website.

Prior to use, validation of the database should occur. This will demonstrate whether the database is fit for purpose and ensure that what is entered into the database is exported as expected. User acceptance testing is recommended. This is where test data is entered into the database. Edit check testing should be performed to ensure any programmed edit checks fire when appropriate (e.g. programmed local lab ranges for each site). If a fax machine or scanner is being used to send paper CRFs to a coordinating centre, this process must be tested prior to sending trial data to ensure it works effectively. The whole testing process must be fully documented and this documentation should be stored within the trial master file.

4.3 Data Entry & Query Management

To assist with entry of data onto paper or electronic CRFs, completion guidelines should be developed. Data entry should be done by an appropriately trained member of staff, delegated this role on the delegation log.

If CRFs are being transferred to the coordinating centre, a copy of the CRF should remain at the investigator site. The copy kept at the investigator site and the copy at the coordinating centre should contain the same information. This means that if the values are updated as a result of queries, the changes must be annotated on both copies. Data queries will either be generated on a data clarification form or via the eCRF. Any change to paper CRFs should be initialled, dated and explained if necessary. This provides an audit trail. The same applies to eCRFs. The system used should be able to track the user

making the changes, all previous & current entries visible and all actions date/time stamped.

The coordinating centre should keep a log of all CRFs received. Paper CRFs should be stored in a secure place e.g. a locked filing cabinet for protection against environmental damage as well as theft.
To reduce the risk of errors when transcribing data from a paper CRF into a database, data can either be single or double data entered as a form of quality control.

1) Single data entry: Once the data has been entered once, a visual check is performed on what is entered on the database against what is on the paper CRF
2) Double data entry: The same data is entered by two people independently. Depending on the software used this could mean that the two independent people enter data on separate files which are then compared for accuracy.

The method use will depend upon the size of the study and the resources available.

4.4 Data Back Up

All data must be stored on computer systems which are centrally backed up on a secure server.

Whatever the format of database software used, there must be back up systems in place to protect against loss of data (see IT Back Up and Disaster Recovery Plan for storing data on the R&D shared drive).

4.5 Data Protection

Throughout all data management processes it is essential that data is dealt with in line with the Data Protection Act 1998. Participant confidentiality must be maintained at all times. Participants should be identified using a study number rather than name, hospital number or address. All study documentation should be kept in a secure location with authorised individual access only. Any electronic transfer of CRFs for data entry should be via a secure system.

The Subject Identification Log, which links the patient's identity to the study number, should be kept separately from the data used for analysis.

4.6 Transfer of data

Staff should take appropriate security measures to ensure that data are not lost or does not fall into the wrong hands during transfer. Personal/sensitive personal data should never be sent through the regular mail or using unencrypted email messages.

If data is being transferred from one organisation to another a secure encrypted format must be used.

If it is necessary to transfer data using removable media e.g. Universal Serial Bus (USB) stick or memory cards, this must be a copy of the data, and the original version kept on the secure computer system.

Data sent on removable media should be password-protected and encrypted; it is not sufficient to use password protection alone.

Identifiable data must not be transferred by email unless the email has been encrypted. BSUH email is not encrypted by default therefore queries /information should not contain any identifiable data except the participant's unique study number.

In general, NHS net to NHS net email (which ends with nhs.net) is secure as it stays behind the firewall. However, before performing this type of transfer it is recommended that this is checked with the Information Governance team.

If the study involves the sharing of personal data between BSUH and another organisation, check to see if an agreement has been signed. If unsure, please contact Martin Gibson, Information Governance Manager – martin.gibson@bsuh.nhs.uk.

5.0 Training

This is a 'read and understand' SOP. Please note that the R&D department discourages the retention of hard copies of SOPs and can only guarantee that the most up-to-date version is on the Trust website.

6.0 Cross Referenced SOPs

IT Back Up and Disaster Recovery Policy

7.0 References

ICH GCP (1996) Section 5.5

Statutory Instrument 1928 (2006), 31A: Trial Master File & Archiving

Data Protection Act 1998

Research Governance Framework for Health and Social Care Second Edition, 2005