1. PURPOSE

This document describes the procedure used for Design, Development, Validation, Functional Testing, Management and Security of Databases for Clinical Studies in NHS Fife (as part of the East of Scotland (EoS) Node) and complies with the principles of Good Clinical Practice (GCP).

It is the responsibility of all researchers using this SOP to ensure they are using the latest version of it. The latest version is available via the R&D pages on the NHS Fife Intranet or, for guidance, contact the Research Governance Officer in the R&D Office, Queen Margaret Hospital, 01383 623623 (extension 20940).
2. APPLICABILITY

This document applies to CTIMPS and non-CTIMPs and is recommended for other types of studies sponsored or co-sponsored by NHS Fife.

This SOP is intended for use by anyone involved with the creation or management of databases for clinical studies, including trials.

In accordance with the principles of GCP, the Chief Investigator (CI) must ensure the accuracy, completeness, legibility, and timeliness of the data reported to the Sponsor in the Case Report Form (CRF) and in all required reports. These duties may be delegated by the CI to other personnel but they must be listed on the delegation log (see SOP28(Fife) Study Start Up In Clinical Trials Of Investigational Medicinal Products).

Where MS Excel is used as a data management system, the CI must adhere to the NHS Fife Guideline for data management using Excel: SOP37(Fife) – Data Management In CTIMPs Using Excel, and to the associated document with advice from TASC “When is Excel an acceptable data management system for a CTIMP?” (Doc Ref 097(TASC)). The Guideline is also recommended for non-CTIMPS.

3. POLICY

This version of the SOP has been adapted for use in NHS Fife from an equivalent Tayside Medical Science Centre (TASC) SOP and will be reviewed every two years unless changes in legislation or procedures require an earlier review. This NHS Fife SOP will be revised at its review date. Use of the adapted Fife version will take precedence over the equivalent TASC version.

Research data must be collected, recorded and managed in accordance with the Data Protection Act (1998) and the appropriate NHS Fife Information Statement policies, NHS Fife Freedom of Information policies and NHS Fife Removable media policy. In addition, data for all research involving the participation of human subjects must be handled according to the principles of GCP.

4. PROCEDURE

Database development for research studies must be undertaken in accordance with this SOP and according to any Data Management Plan (DMP) that there is for the study. The DMP typically details the data sources and how they will be integrated (i.e. the data flow) and the systems to be used. It refers to (or details) procedures to be used for database development and data handling plus any additional study specific instructions such as self-evident corrections.

The study delegation log must document who is responsible for database development and testing. The DMP will apportion responsibilities for management and security of the study database(s).

4.1 Design and Development
The database must meet the Sponsor’s established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. system validation). In practice this means that study data must be stored in a database with the following key characteristics:

- The system will store data as defined by the CRF for the number of participants defined in the protocol at visits defined by the protocol.
- There will be an unambiguous and unique identifying ID for each participant. The code for file linking participants’ names with their IDs must be kept secure and separate from the data used for analysis.
- The system will safeguard study blinding where this exists. Blinding must not be broken through the day-to-day use of the computerised system. The system must provide protection against unintentional unblinding but support, where appropriate, any trial specific unblinding procedures.
- There will be a security system that prevents unauthorized access to the data (see section 4.3 on Security of electronic databases to GCP). There must be role based access – some people can design, some can enter and change data.
- An audit trail will be maintained so that when data items are changed the original value is stored and it is recorded who changed what, when and why (ideally the system will prompt the user to enter why data items are being changed).
- To support data quality, it is advisable (although not essential) to have a system that generates a warning on entry of data items that are inconsistent or out of range for that patient group. These warnings may be “hard” i.e. suspect data is refused, or “soft” i.e. suspect data can be entered but is flagged by the system.
- It must be possible to distinguish in the database between data items that are missing, or not applicable, or zero. The system should have a built in function that supports this or it may be dealt with using a system of manually entered codes.

There must be documentation to prove that the data management system meets these requirements and that entered data will be stored and exported without alteration. This documentation will consist of:

- A specification which will centre on the protocol and CRF.
- Evidence that the system has undergone and passed validation as per section 4.2 below. This includes validation of the export process.
- User instructions and evidence of user training.
• Documented release of the system for “live” use. This will be explicitly contingent on the system having passed validation and been signed off by the developer and a member of the investigating team.

4.2 Validation and Functional Testing

In order to demonstrate that a computerised system is fit for purpose and performs consistently, it must pass a validation process and this must be documented.

A description for the computerised system to be used in a CTIMP must be produced and retained in the Trial Master File (TMF), or other appropriate file.

The validation and functional testing of the computerised system must be undertaken against the documented description for the computerised system.

The process of validation and functional testing must be recorded each time that it is carried out. Evidence of such testing must be retained in the TMF or other appropriate file.

As modifications to the system are made, these must be functionally tested and validated. If necessary, updates to the application description document and validation and functional testing regimes must be carried out. The trial database must be version controlled. There must be a log detailing the changes made for each version and the date it went live.

Note 1: It is important that the CI makes adequate provision for validating computerised systems (and support of these systems after release) in the funding arrangements for CTIMPs.

Note 2: The document Guidance on functional testing and validation of computerised systems (Doc Ref 50-001) gives some guidance on how investigators can implement this SOP.

4.3 Security of electronic databases to GCP

All persons dealing with personal data are responsible for ensuring the security and safety of these data. Data used for analysis must be anonymised. Data used for study management must use the minimum number of personal identifiers necessary to conduct the study and ensure patient safety.

Physical location of servers

Servers holding data for clinical studies must be in secure data centres to which physical access is restricted to authorised personnel. The server room must be temperature controlled using a calibrated system and should have rodent control measures in place.

Backup
Electronic data must only be stored on devices that are backed up in a secure and timely (e.g. daily) manner. Data will be backed up onto remote and/or removable disk storage but only using devices approved in accordance with NHS Fife IT policy. Such backup remote and/or removable disks are to be placed into a secure fire safe. Data must not be held on devices that do not participate in a backup regime. If in doubt contact the NHS Fife IT department to confirm that the server upon which the clinical trial database is stored is appropriately backed up.

The process of restoring from backup must be tested regularly, e.g. quarterly, and logs kept of this procedure.

**Updates**
Any machines used to enter or access study data must have up-to-date operating system patches installed together with appropriate security software (e.g. antivirus, anti-spyware, firewall).

**Authorisation**
Access to the data must be limited to authorised personnel and each user of the system must have an individual account. A record must be kept of authorised users and the access levels that apply to each user. The list of authorised users must be kept in the study documentation with dates granted and revoked. Access must be revoked when a user is no longer working on the study. Access to electronic data must require a unique password which complies with the NHS Fife policy on passwords available on the NHS Fife Intranet. Accounts must never be shared, nor should there be ‘guest’ accounts. Individual users must login with their own usernames and passwords and must not login so as to provide access to another user.

**Data transfer**
Datasets containing identifiable personal data must be encrypted prior to transmission, or transfer (e.g. on CD), using an industry-standard encryption mechanism (e.g. Advanced Encryption Standard (AES-128) (see [http://aesencryption.net/](http://aesencryption.net/)). Software such as Truecrypt is suitable for this.

**Note 3:** The NHS Fife management of its networked drives is consistent with the above guidance on location of servers, backup, updates and authorisation. Therefore storing study data on NHS Fife networked drives (NB not hard drives or laptops) will ensure the data are secure, are backed up, with restricted access controls in place and appropriate updates to the operating system and security software. Note that only users with a need to access the data will be allowed access. Hence, a specific drive will have to be arranged and/or the data files password protected. Also arrangements will also have to be made to encrypt any data that are to be transferred outside the organisation.

**4.4 Third party provision of data management services**
The development and hosting of the study database may be out sourced to an external third party such as a Clinical Trials Unit, by arrangement. In this case, the provision of data management services must be covered by an agreement confirming
that the service provider is able to meet the requirements of the Sponsor as set out in this and other relevant SOPs.

5 ASSOCIATED DOCUMENTS

Doc Ref 10-001 Guidance on functional testing and validation of computerised systems

6. DEFINITIONS

CD Compact Disc
CI Chief Investigator
CRF Case Report Form
CTIMP Clinical Trial of Investigational Medicinal Product
GCP Good Clinical Practice
DMP Data Management Plan
R&D Research and Development
SOP A Standard Operating Procedure (SOP) is a written instruction and written record of procedure agreed and adopted by individual study teams. SOPs achieve uniformity of the performance of specific functions and set out the way practice and procedures should be performed.
TASC Tayside Medical Science Centre
TMF Trial master File

7. REFERENCES

WORLD MEDICAL ASSOCIATION DECLARATION OF HELSINKI Ethical Principles for Medical Research Involving Human Subjects. (http://www.wma.net/en/30publications/10policies/b3/)

It is assumed that by referencing the principal regulations, all subsequent amendments made to the principal regulations are included in this citation.