

Standard Operating Procedure

Title: DATA PROTECTION		
REF: SOP 005	Version: 04	Issue No: 1
Template Source: Merseyside & Cheshire Cancer Research Network		Date: 18/02/05
Reviewed by: Professor Rod Owen		Date: 05/11/2009
Approved by: Dr M J Maxwell		Date: 21/05/07
Due for Revision		Date: 05/11/2012
This SOP is effective from:		Replaces: Version 03 (21/05/07)

1. BACKGROUND

The Data Protection Act of 1998 listed 8 principles of data protection. The act came into force in March 2000, and has implications for research centres and employees.

The eight principles are:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purpose(s) and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Personal data shall be accurate and where necessary kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction.

DATA PROTECTION	
REF: SOP 005	VERSION: 03

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. PURPOSE

To ensure that personal data relating to research subjects is handled and maintained in such a way as to satisfy the requirements of the 1998 Data Protection Act.

3. OTHER RELATED PROCEDURES

SOP 006 Study Files and Filing
SOP 009 Case Report Form (CRF) Completion
SOP 013 Archiving

4. WHEN

This SOP is applicable at all times when dealing with patient/subject identifiable data of any kind (i.e. electronic records, paper notes etc).

5. WHO

Every individual involved in the retrieval, handling and storing of patient/subject data should practice in accordance with this SOP.

Extra responsibility for data protection issues lies with the Trust's Information Governance Officer and the Caldicott Guardian.

6. HOW

All study patient identifiable data should be stored in a secure room.

All study patient identifiable data must be locked away if unattended.

No one should access study patient identifiable data unless authorised to do so by members of the research team or the Caldicott Guardian.

Patient confidentiality should be supported by use of initials/numbers only on research material.

Electronic data must be password protected

Personal data that has the potential to identify research subjects should be kept in a secure place, separate from the study files and case report forms, with the exception of essential study documents required to be kept as part of the study site file e.g. signed consent forms.

DATA PROTECTION	
REF: SOP 005	VERSION: 03

All staff should be familiar with the local NHS Trust data protection policies and attend information governance training.

Medical notes should be stored in accordance with local NHS Trust policy.

6.1. Non-Medical Information covered by the Act.

Information such as personal data held by the department must be stored safely in secure computerised systems or locked away. All data must be treated with care.

Note: Source documents and trial-related data from clinical trials with investigational medicinal products (CTIMP) or medical devices must be stored for a minimum of 15 years (See SOP 013: Archiving) and for all other studies, at least 10 years.

Care **must** be taken to ensure that such data are stored safely and in accordance with the requirements of the Data Protection Act and this SOP.