South Eastern Health and Social Care Trust

# Standard Operating Procedures (SOP) Research and Development Office

| | |
|---|---|
| **Title of SOP:** | Principles of Data Collection and Storage |
| **SOP Number:** | 8 |
| **Version Number:** | 2.0 |
| **Supercedes:** | 1.0 |
| **Effective date:** | August 2013 |
| **Review date:** | August 2015 |

| | |
|---|---|
| Author: | Alison Murphy, Research Manager<br>Endorsed by Paul Carlin |
| Approved by: | Dr David Hill |
| Signed: |  |
| Date: | 01 August 2015 |

| Version No. | Date | Author | Reason for Change |
|---|---|---|---|
| 1.0 | Oct 2007 | Paul Carlin | N/A |
| 2.0 | Aug 2011 | Paul Carlin | Regional SOP |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Table of contents**

## 1. INTRODUCTION

Information Governance sets standards for all HSC/NHS Trusts on how information is held, obtained, recorded, used and shared. Information Governance ensures compliance with the Data Protection Act 1998, Freedom of Information Act 2000 and the Department of Health's Code of Confidentiality and the Caldicott Principles.

The majority of research projects carried out within South Eastern Health and Social Care Trust involve the use of personal data to some extent. There is much confusion over exactly what counts as personal data, and therefore what is covered by the Data Protection Act. The Act defines personal data as any data that can be attributable to a living individual, and does **not** have to include name, address, date of birth or sex. For example, research projects often identify participants using their hospital number or using a code - this still counts as personal information. It is recommended that you store your research data in coded form, using a key only known to yourself.

The appropriate use and protection of patient data is paramount. As researchers working within the Trust you must abide by the Data Protection Act 1998 and the Trust Data Protection Policy.

## 2. OBJECTIVE

The objective of this Standard Operating Procedure (SOP) is to provide a guide to Researchers on the Data Protection Act 1998, ensuring that they are aware of their legal and ethical duties.

## 3. SCOPE

Within the context of this SOP are instructions and guidelines for collection, storage and transfer of data and results collected for **all** research within the South Eastern Health and Social Care Trust.

## 4. PROCESS

### 4.1 General Guidelines

The following information provides the legislative guidelines and associated procedures relating to data collection and storage of data for research purposes.

- The identity of the trial subject must be restricted to essential site staff only. This can include the Principal Investigator, research nurse, dispensing pharmacist and any other site staff deemed necessary by the principal investigator.

- The Subject Identification Log must be stored in a locked restricted access location separately from the source documents and case report forms.

- Any data collected with the subjects name included e.g. clinical laboratory reports/X-ray reports/Dexa scan reports must be photocopied and anonymised prior to being placed in the source document notebook for monitoring.

- Source documents and Case report forms must be stored in a locked area with restricted access to essential study personnel only.

- Principal Investigators must ensure the Site Delegation Log is completed and maintained in the Site Master File.

- All study personnel must have current and documented Good Clinical Practice Training.

- The SEHSCT retention schedule states that primary research data should be retained for a minimum period of 5 years following completion of the study. This refers to all forms of research and not just clinical trials. Medical notes of participants in clinical trials must be retained for 15 years.

### 4.2 Information Governance

Information Governance is a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards.

Information governance incorporates legislation and codes of practice, including:

| | |
|---|---|
| Data Protection Act 1998 | Information Quality Assurance |
| Caldicott Principles | Records Management |
| Confidentiality Code of Practice | Freedom of Information Act 2000 |
| Information Security | |

"… *the appropriate use and protection of patient data is paramount. All those involved in research must be aware of their legal and ethical duties in this respect. Particular attention must be given to systems for ensuring confidentiality of personal information and to security systems."* – The Department of Health Research Governance Framework for Health and Social Care, 2nd Edition, 2005

### 4.3 Principles of Data Protection

The Data Protection Act of 1998 embraces all **personal data** of living individuals. The personal data can be paper or electronic, including images, which can identify, in isolation or in combination with other data, a living person.

There are **Eight Principles of Data Protection** that must be complied with when processing personal data. They are that personal data must be:

1. Processed fairly and lawfully;

2. Obtained only for one or more specified and lawful purposes;

3. Adequate, relevant and not excessive for the purpose.

4. Accurate and, where necessary, kept up to date;

5. Kept no longer than necessary for the purpose;

6. Processed in accordance with the rights of the data subject.

7. Kept secure, and appropriate measures taken against unauthorised or unlawful processing of data, including accidental loss or destruction;

8. Not transferred to countries outside the European Economic Area unless the country ensures adequate protection for the individual in relation to the processing of their data. Personal data can be transferred outside the EEA for legal reasons.

### 4.4 Principles of Good Clinical Practice

GCP is an international ethical and scientific quality standard for the design, conduct and recording of research involving humans. Comprised of 13 core principles, GCP applies to all clinical investigations that could affect the safety and well-being of human participants (in particular, clinical trials of medicinal products).

GCP was developed by the regulatory authorities of the EU, Japan and US in a steering group termed the Tripartite International Conference on Harmonisation (ICH) and provides international assurance that:

- Data and reported results of clinical investigations are credible and accurate, and
- Rights, safety and confidentiality of participants in clinical research are respected and protected

It was finalised in 1996 and became effective in 1997. When first expounded, it was an internationally recognised as best practice, but was not enforceable by law. However, with the advent of the Medicines for Human Use (Clinical Trials) Regulations 2004 and the EU Directive on Good Clinical Practice, compliance with GCP is now a legal obligation in the UK/Europe for all trials of investigational medicinal products .

GCP - 13 Principles

1. Clinical trials should be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki, and that are consistent with GCP and the applicable regulatory requirement(s).

2. Before a trial is initiated, foreseeable risks and inconveniences should be weighed against the anticipated benefit for the individual trial subject and society. A trial should be initiated and continued only if the anticipated benefits justify the risks.

3. The rights, safety, and well-being of the trial subjects are the most important considerations and should prevail over interests of science and society.

4. The available nonclinical and clinical information on an investigational product should be adequate to support the proposed clinical trial.

5. Clinical trials should be scientifically sound, and described in a clear, detailed protocol.

6. A trial should be conducted in compliance with the protocol that has received prior institutional review board (IRB)/independent ethics committee (IEC) approval/favourable opinion.

7. The medical care given to, and medical decisions made on behalf of, subjects should always be the responsibility of a qualified physician or, when appropriate, of a qualified dentist.

8. Each individual involved in conducting a trial should be qualified by education, training, and experience to perform his or her respective task(s).

9. Freely given informed consent should be obtained from every subject prior to clinical trial participation.

10. All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification.

11. The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).

12. Investigational products should be manufactured, handled, and stored in accordance with applicable good manufacturing practice (GMP). They should be used in accordance with the approved protocol.

13. Systems with procedures that assure the quality of every aspect of the trial should be implemented.

### 4.5 Fair Processing of Personal Information

At the time of data collection you must inform research participants of:

- The identity of those who will have access to the data;
- What will happen to the data, ie how it will be processed, intended disclosures or retention periods;
- The purpose for which the personal data is to be processed; Intention to further process the data;
- Intention to further process the data;
- The security of the data being collected;
- Any other relevant information demonstrating how their data will be processed fairly and lawfully

This information should form part of the consent process.

### 4.6 Consent for Processing of Personal Data

The informed consent of research participants must be sought for the processing of their personal data, wherever practically possible:

- The data subject must know the proposed uses/disclosures of personal data.
- The subject must be given a choice.
- There should be some indication that consent has been gained.

### 4.7 Data Protection and Research

Use of personal identifiable information

Personal data should be "coded", such that all information that might be used to identify a person is removed at the earliest opportunity. Codes should be kept separate from the original data set and access should be restricted to a limited number of designated persons.

**Anonymised data** are data prepared from personal identifiable information, but from which the person cannot be identified by those who receive the data. Permission for this data to be used in future research should be requested at the time of initial consent to registration or research.

**Linked anonymised data** is anonymous to the people who receive and hold it (eg the research team), but contains information and codes that would allow others (eg those responsible for an individual's care) to identify the data subject.

**Unlinked anonymised data** contains no information that could reasonable be used, by anyone, to identify people: the link between the data and the person to whom it refers has been irreversibly broken.

### 4.8 The "Research Exemption"

Where certain conditions are met, ie:

a) The data are not processed to support measure or decisions relating to particular individuals, and

b) The data are nor processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject,

Certain exemptions apply and data obtained for "medical purposes" can be used for research and, as such:

- **Exemption from Principle 2**. Identifiable data that have been obtained for routine medical care can be further processed for medical research purposes so long as the relevant conditions are met.

- **Exemption from Principle 5.** Researchers are able to hold the information for longer than may otherwise be necessary.

- **Exemption from Principle 6**. The right of the individual to access their data does not apply provided that the person cannot be identified from the results of the research.

Even where a researcher properly applies the exemptions, (s)he is still required to comply with the rest of the Act, including the first and second principles. Therefore, at the time data are collected the data subject should be made fully aware of how the data will be processed and whether further processing of the data is intended in the future.

### 4.9 Research Using Identifiable Personal Information

Investigators must inform participants of the intended uses of their data and gain consent for this.

If the patient was not informed at the time of data collection that their information could be used for research, then for:

1. **Research using current records:** If the patient is still undergoing treatment, there is ample opportunity to explain to the individual that the records may be used for research purposes and consent should be sought.

2. **Research using records of patients no longer being treated:** If it is considered impracticable to obtain consent, for example, due to excessive numbers involved in establishing disease registers, then an investigator can apply for an exemption under Section 60 of the Health & Social Care Act (2001) from the National Information Governance Board (NIGB), however this legislation does not apply in Northern Ireland. In these instances, in the South Eastern Trust approval must be sought from the Trust Data Guardian and a Data Access Agreement put in place if the data is being transferred outside the Trust.

### 4.10 Caldicott Principles

Together with the Data Protection Act 1998, the Caldicott principles form the basis of best practice in information management in the Health and Social Care sectors. They allow for the secure transfer of confidential information amongst professionals within these sectors and, where authorised, across the NHS, social care and University boundaries.

The six Caldicott principles:

**1.** Justify the purpose(s) for using personally-identifying information.

**2.** Only use personally-identifying information if it is absolutely necessary.

**3.** Use the minimum necessary personally-identifying information.

**4.** Access to personally-identifying information should be on a strict need to know basis.

**5.** Everyone should be aware of their responsibilities and obligations to respect personal confidentiality.

**6.** Everyone should understand and comply with the law.

### 4.11 Data Security

For any instance where personal identifiable information is being processed, a "data controller" or "custodian" should be identified. Ultimately, the data controller is the Trust or organisation who will have overall responsibility for the processing of the data. Individuals in custody of personal identifiable information should establish procedures for the following:

#### 4.11.1 Computer storage of personal data

- Restrict and document the number of computers on which data is stored.
- Personal data should not be stored on hard drives unless adequately protected using suitable encryption tools and passwords.
- Maximise the security of computer-based data by storing data on a secure server (NHS or University) rather than the hard drive.
- Restrict and document access to data through use of passwords.
- Minimise the storage of personal identifiable information through coding and restrict and document access to codes.
- Never store personal identifiable information on portable computers, or data storage devices, unless appropriately encrypted in accordance with Trust procedures.

#### 4.11.2 Hard-copy storage of personal data

- Store documentation that contains personal identifiable information securely.
- Restrict access to documentation to designated persons.
- Audit access to documentation.

#### 4.11.3 Electronic transfer of data

- Transfer of data via email is only secure over NHSnet servers.
- University email systems offer some degree of security, but coded data should be used.

- Web-based email and the internet is not secure and should never be used for transfer of personal identifiable information.

### 4.11.4 Destruction of data

All data and records relating to this study should be kept at the investigational site or an alternative storage facility for the appropriate period in accordance with Trust procedures or sponsor requirements. Any alternative storage facilities should meet current legislative requirements.

Confidential documentation should be destroyed to secure their complete illegibility, preferably by shredding, pulping or incineration, in accordance with relevant Trust Destruction Policies.

When disposing of computers ALL data/programs must be removed from equipment prior to disposal, there should be no sensitive data/programs left on the equipment. Written agreements should be obtained from contractors regarding the treatment of confidential waste. Magnetic media, microfiche used as a backup, hard disks and so forth should be made unreadable prior to disposal. The relevant Trust policies should be adhered to. The Trust ICT Department can provide guidance on disposal.

### 4.12 Freedom of Information

The Freedom of Information Act (2000) provides individuals with the right to ask for and be provided with any recorded information held by public sector organisations, subject to specified exemptions including the following examples:

**Absolute exemptions**

- Personal Information
- Information reasonably accessible to the public by other means
- Information provided in confidence
- Environmental information (although this may still be covered by the Environmental Information Regulations 2004)

**Public interest exemptions**

- National security
- Commercially sensitive information
- Information intended for future publication

Information about research is subject to the Freedom of Information Act. However due to the sensitive nature of some research any of the above exemptions may apply prior to disclosure. It is worth noting that whilst research findings may be covered by the

information intended for future publication exemption, background data and statistics may not.

## 5. REGULATIONS, GUIDELINES, REFERENCES, SOP LINKS etc.

International Conference on Harmonisation (ICH) of Good clinical Practice.

Data Protection Act 1998.

Freedom of Information Act (2000)

The Department of Health Research Governance Framework for Health and Social Care, 2nd Edition, 2005

## 6. APPENDICES

6.1 Appendix 1: Frequently Asked Questions

**Appendix 1: Frequently Asked Questions**

| | |
|---|---|
| What is the difference between anonymised and pseudo-anonymised? | Anonymised data is data where all personal identifiers have been removed permanently. Pseudo-anonymised is removal of patient names, initials, address or postcode, date of birth, hospital number and NHS number. Pseudo-anonymised data would contain a link back to the identifiable data. |
| If I am obtaining data from another organisation to use in my research.<br>Who should anonymise that data? | Ideally the organisation from which the data came. |
| Will the removal of names and addresses from the dataset be sufficient? | Not always. More information in a data set increases the likelihood of identification. Even by removing the name and address, there may be other identifying details. Data is not fully anonymised if a key exists. |
| What does the Data Protection Act say about tissue and biological samples? | The Human Tissue Act provides a legislative framework for the removal, storage and use of human organs and tissue for scheduled purposes. |
| Do Data Protection rules apply if a researcher in the Trust is analysing data for a colleague from another institution? | Yes, unless the data is anonymous, it is unlawful to analyse the data unless the subject has consented. |
| Does the Data Protection Act apply to dead people? | DPA does not apply to dead people; however there may be genetic/hereditary information that may affect family. Consequently a duty of confidence to their family still applies. |
| Do I need consent to conduct an audit? | No. However a duty of confidence still applies. |
| Who should take consent? | A clinician who is known to the patient should take consent. |
| Can I use data collected for an audit for research? | No. Data collected for a specified purpose cannot be used for any other purpose. |
| Can you send data outside the European Economic Area? | Only if the specific consent of the data subject has been obtained, or if a contract with the third party exists that enforces the principles of data protection. |
| What is “sensitive data”? | Racial or ethnic origin, information on political affiliation; religious or other similar beliefs; trade union membership; information on mental or |

| | |
|---|---|
| | physical health; criminal convictions; and sexuality. NB Specific written permission is imperative to collect sensitive data, unless you have a legal requirement to process it. |
| Can I take data home? | You are responsible for any data. Personal data must not be stored on computers that are not owned by the Trust and which are linked to the internet. |
| I have been through the ethics approval process, doesn't that mean that I have covered all data protection issues. | No. Favourable ethical opinion does not necessarily indicate that research complies with the Data Protection Act; when in doubt seek advice from the Data Protection officer. |