Southampton City NHS
Primary Care Trust

Primary Care Trust Policy Document

Serial Number: **SCPCT/Policy/IMT/03 – Version 2**

Issue Date: **February 2005**

Operative Date: **February 2005**

Review Date: **February 2007**

DATA PROTECTION, CALDICOTT & CONFIDENTIALITY POLICY & PROCEDURES

Purpose of Agreement:

This document describes the Southampton City Primary Care Trusts (SCPCT) policy on Data Protection and Caldicott, and employees' responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and on computers.

For action by:

All staff via Directorate Leads

Further details and Additional Copies from:

Information Security Team
ICT Services
Oakley Road

Responsibility for dissemination to new staff:

All Departmental Heads

Amendments Summary:

Amend No	Issued	Page	Subject	Action Date

Review Log
Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes

Routes of Ratification
Policy Steering Group 9th May 2005
Chair – Rachel Goldsworthy

Policy Written By

Information Security Team
ICT Services

Supporting Documents	
ACCESS TO PERSONAL AND HEALTH RECORDS PROCEDURE	
INFORMATION SHARING POLICY	
RESEARCH PROCEDURE (in development)	
CONFIDENTIALITY: NHS CODE OF PRACTICE **http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4069253&chk=jftKB%2B**	

Table of Contents

1. Introduction

1.1 Guidance on the Data Protection Act 1998, the Access to Health Records Act 1990, the Caldicott Report 1997 and related legislation

This document describes the Southampton City Primary Care Trusts (SCPCT) policy on **Data Protection and Caldicott**, and employees' responsibilities for the safeguarding of **confidential** information held both manually (non-computer in a structured filing system) and on computers.

This policy applies to all directly and indirectly employed staff and other persons working within the Trust in line with Southampton City PCTs Equal Opportunities Policy.

This Trust holds and manages a great deal of personal and confidential information relating to patients, service users and carers, the public and employees of the NHS.

The **Data Protection Act 1998** (DPA 98) provides controls on the handling of personal identifiable information for all **living** individuals. Central to the Act is compliance with the eight data protection principles (see 2.1) designed to protect the rights of individuals about whom personal data is processed whether an electronic or a paper record.

The **Access to Health Records Act 1990** provides controls on the management and disclosure of health records for **deceased** patients. Thus the personal representative of the deceased or a person who might have a claim arising from the patient's death can apply to gain access to the files.

The **Caldicott Report 1997** provides guidance to the NHS on the use and protection of patient identifiable information, and emphasises the need for controls over the availability of such information and access to it. It makes a series of recommendations which led to the requirement for all NHS organisations to appoint a Caldicott Guardian who is responsible for compliance with the 6 Caldicott confidentiality principles. (see 2.2)

The **Common Law Duty of Confidentiality** prohibits use and disclosure of information, provided in confidence unless there is a statutory or court order requirement to do so. Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example, to protect the vital interests of the data subjects or another person, or for the prevention or detection of a serious crime.

1.2 Note on Terminology

Throughout this document the term "patient" is used. This term includes those people who are also known as "Service Users", and "Clients"

Similarly the terms "clinician" and "health professional" are used, but should be interpreted as encompassing social care staff and NHS practitioners.

1.3 Review and Maintenance

The Information Security Team, Southampton ICT Shared Services, maintain this policy on behalf of SCPCT.

This policy may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed after twelve months and thereafter on a bi-annual basis

Forms referred to in this policy are available from ICT Services.

Please consult your Manager or the Information Security Team if you have any queries.

The latest version can be found on the Trust Intranet.

2. Principles and Practices to ensure compliance with Data Protection and Confidentiality

(See Appendix A for a summary of the Data Protection Act 1998)

2.1 Data Protection Act 1998 - Principles and Practices to ensure compliance

The Trust will put in place procedures to ensure the eight principles in the DPA 98 are met.

2.1.1 Personal data shall be processed fairly and lawfully

Compliance with Data Protection and Caldicott will be achieved by implementing the following measures:

- Complying with the common law duty of confidentiality; which is that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.
- Informing the individual who will be processing their data (usually via an information leaflet)
- Ensuring that certain conditions in Schedules 2 and 3 of the Act are met. (*see Appendix B for detail of the Data Protection Act 1998 - First Principle*)
- Informing the individual how the data will be processed. This means fully describing how the data will be used i.e. what will be done to the data; for what purposes it will be used, who it will be passed onto, how it will be processed, stored and destroyed. *(see Appendix C)*

2.1.2 To obtain personal data only for specified and lawful purposes and further process it only in a compatible manner.

The following must be adhered to:

- Personal data must only be processed for the purposes for which it was originally obtained.
- Protocols should be in place to ensure that personal data that is passed on is used only for the purposes for which it was originally obtained.

2.1.3 Personal data must be adequate, relevant and not excessive

This will be achieved by:

- Conducting routine audits as part of good data management practice.

- Ensuring that Health Service Circular (HSC) 1999/053 For the Record: Managing Records in NHS Trusts & Health Authorities, and professional guidelines, on taking and making of records, are adhered to.

2.1.4 Personal data must be accurate and up to date.

This will be achieved by:

- Data users recording information accurately and taking reasonable steps to check the accuracy of information they receive from data subjects or anyone else.

- Data users regularly checking all systems to destroy out-of-date information and correcting inaccurate information.

2.1.5 Personal data must be kept no longer then necessary.

This will be achieved by:

- Adherence to HSC 1999/053 For the Record: Managing Records in NHS Trusts & Health Authorities which is detailed in the Trusts Retention & Disposal of Records Policy.

- Staff working in joint team situations using the maximum retention period.

2.1.6 Personal data must be processed in accordance with the rights of the individual.

The Act gives seven rights to individuals, they are a:

- right of subject access (e.g. to see or have a copy of your medical records or staff files)
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- rights in relation to automated decision taking
- right to take action for compensation if the individual suffers damage
- right to take action to correct, block, erase or destroy inaccurate data
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The **ACCESS TO PERSONAL AND HEALTH RECORDS PROCEDURE**, details the actions to process a request for Subject Access.

Should an individual make a request to prevent processing then depending on the individual circumstances, the Trust would have to make a judgement based on the risk to the individual or others whether it was right to provide a service.

2.1.7 Personal data must be kept secure.

Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of personal data and against accidental loss or destruction.
Compliance will be achieved through the Information Security Policy and by following the Safehaven Policy. *(See Appendix D)*

2.1.8 Personal data shall not be transferred to a country outside the European Economic Area unless that country can ensure adequate level of protection.

To ensure compliance protocols must be in place for the transfer of personal data outside the European Economic Area unless that country can ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.2 Caldicott Principles for handling person-identifiable data

2.2.1 Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2.2.2 Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

2.2.3 Use the minimum necessary patient-identifiable information

Where the use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

2.2.4 Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

2.2.5 Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

2.2.6 Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

3. Confidentiality

3.1 Patient Confidentiality

- Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

- On admission or on first contact with the service for a particular matter, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or those they specifically do not give permission to receive information.

- In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

- The patient should be encouraged to be very explicit if there is anyone that they do not want to be given information. In the event of the patient being unable to give permission a person must be identified to act on behalf of the patient and permission obtained from him/her.

In all cases, the wishes expressed must be appropriately documented in the Health Records or patient notes.

3.2 Staff Confidentiality

- All Staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

- Confidential information must not be disclosed to unauthorised parties without prior Trust authorisation by a senior manager. Staff must not process any personal information in contravention of the Data Protection Act 1998.

- Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

- All staff have a confidentiality clause in their contract of employment. The Trust has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

4. Exemptions to the Data Protection Act 1998

4.1 In certain circumstances personal information may be disclosed and this section details these. However it is vital in each case, that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason.

4.2 Disclosing information against the subject's wishes

- The responsibility of whether or not information should be withheld or disclosed without the subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.
- Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:
- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Child abuse and vulnerable adults
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.

  Reference: Confidentiality NHS Code of Practice, Common Law and disclosure in the Public Interest

- The following are examples where disclosure without consent is required:

  Births and deaths - National Health Service Act 1977
  Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
  Poisonings and serious accidents at the work place - Health & Safety Act
  Terminations - Abortion Regulations 1991, duty to inform
  Offenders thought to be mentally disordered – Mental Health Act
  Child abuse – duty to disclose following Child Protection Procedures
  Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
  Road traffic accidents - Road Traffic Act
  Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

  If in doubt, staff should seek guidance, in confidence, from the Senior Clinician or the appropriate Senior Manager or the Caldicott Guardian.

SCPCT will support any member of staff who, using careful consideration, professional judgement and has sought guidance from their manager, can satisfactorily justify any decision to disclose or withhold information against a patient's wishes.

4.3 Non–Disclosure of personal information contained in a Health record.

4.3.1 An individual requesting access to their health records may be refused access to parts of the information if an appropriate Clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure should be documented. Where access would disclose information relating to or provided by a third party, consent for release must be given by the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care. Where the third party does not consent, the information may be disclosed providing the identity of the third party is not revealed. The DPA 98 suggests that this might be done by omitting names and particulars from the records. Care should be taken to ensure that the information, if released is genuinely anonymous.

Further guidance is available from the Records Manager.

4.3.2 The Trust is not required to supply copies of medical records if the individual requesting the information has

- not provided enough supporting information in order for the information to be located
- not supplied the appropriate fee
- not supplied the necessary evidence of identity

or

- the retrieval of the medical records requires disproportionate effort

4.3.3 The Information Commissioner has released guidance on issues of law concerning the right of access to personal data. See **Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division), decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003 (http://www.informationcommissioner.gov.uk/eventual.aspx?id=5152)** which gives guidance on

- what makes “data” “personal” within the meaning of “personal data”
- what is meant by a “relevant filing system”
- upon what basis should a data controller consider it “reasonable in all the circumstances” to comply with the request even though the personal data includes information about another and that other has not consented to disclosure

5. Roles & Responsibilities

SCPCT will establish a structure to deliver information governance, to meet the requirements of data protection and confidentiality.

5.1 The Chief Executive

The Chief Executive has a duty to ensure that:

- staff are aware of the need to comply with the DPA 98, in particular with the rights of patients wishing to access personal information and or their health records.

- staff are aware of requirements of the common law duty of confidence as set out in

NHS Code of Confidentiality

- arrangements with third parties who process personal data on behalf of the Trust are subject to a written contract which stipulates appropriate security and confidentiality.

- Local Research Ethics Committees and researchers are aware of the DPA 98 and how it applies to the use of data for research purposes.

5.2 Caldicott Guardian

The Trust's Caldicott Guardian is the Medical Director. The Guardian is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of patient-identifiable information across the Trust and supporting agencies. The Guardian is also responsible for the return of the Information Governance Toolkit assessment. To assist with the volume and diversity of this task the Guardian is supported by the Records Manager and the Data Custodians.

5.3 Data Protection Officer

The Data Protection Officer is the Records Manager. The Data Protection Officer has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance throughout the Trust with the DPA 98.

The Data Protection Officer has these tasks:

- To promote awareness of the Act and Procedures contained in this policy
- To be responsible for compliance with the DPA 98 and the eight data protection principles.
- To ensure Trust compliance of Notification requirements with the Information Commissioner's Office
- To monitor changes to working practices, and where any such changes are found to come within the remit of the DPA 98, to take appropriate action
- To liaise closely with the Data Custodians (see 5.5) and the Information Security Office in Southampton ICT Shared Services.
- Organise the Data Custodian Exchange Forums.
- To help maintain the Trust Data Protection inventory by recording all service/local changes to the systems (both computerised and manual) inventory.
- Oversee applications for Subject Access and maintain appropriate files.

5.4 The Information Security Team is a shared service provided by Southampton ICT Shared Services, contact number 023 8072 5556, and consists of the following staff;

5.4.1 Information Security Manager

The main responsibility is the implementation of the Trust's IT Security Policy which details further safeguards for data held in Trust's systems.

The tasks are to:

- Provide an advisory service on Information Governance, through the Information Security Team.
- Monitor and report on the state of Information Management & Technology (IM&T) security within the organisation.
- Ensure that the Information Security Policy is implemented throughout the organisation,
- Develop and enforce detailed procedures to maintain security,
- Ensure compliance with relevant legislation,
- Ensure that the organisation's personnel are aware of their responsibilities and accountability for information security,
- Monitor for actual or potential information security breaches,
- Maintain an up-to-date IT Security Policy

5.4.2 Information Governance Officer

The main task is to provide a source of up-to-date expertise on information governance issues. The Information Governance Officer provides support to the Data Protection Officer, the Caldicott Guardian and the Data Protection Co-ordinator / Information Governance Support; to ensure the correct data protection notification is achieved.

The tasks are to:

- Be the first point of contact within the Trust for data protection and Caldicott issues.
- Advise and update the Trust in relation to directives/guidance from the Information Commissioner and the Department of Health.
- Provide effective training for all staff in the requirements of Data Protection legislation and the Caldicott principles.
- Maintain an up to date Notification under the Data Protection Act 1998.
- Carry out Data Protection and Caldicott compliance checks in the Trust's departments, as required.
- Liaison with Information Commissioner's Office.

The above posts are supported by an Information Security Support Officer who provides administration and training support for the Information Security office

5.5 Data Custodians

Data Custodians, identified within each department of the Trust, are responsible for ensuring that the Data Protection and Caldicott principles are fully observed and complied with by staff within their department. Data Custodians are required to ensure that all data flows and processing of data complies with all current Data Protection policies, working closely with the Data Protection Officer and Information Governance Officer as appropriate.

Their tasks are to:

- Promote Data Protection & Caldicott Principles on an on-going basis, including posters, articles and local briefings.
- Promote local induction and ensure that all new starters, before they access any information system, are given instruction on the Data Protection Act and Caldicott, as part of their first day/week induction programme.

- Ensure that all new staff attends the Corporate Induction session as soon as they are able.
- Ensure all staff have access to current information on Data Protection Act and Caldicott requirements.
- Ensure that all staff are aware of the Data Custodian for their area and the contact details for the Information Security Team.
- Ensure that all staff know the procedure for reporting security incidents
- Carry out an annual Data Protection inventory (using the compliance proforma) to enable an assessment of compliance with the Data Protection and Caldicott principles within the service or area.
- Ensure applications for access to systems within the department are processed following the agreed procedures and with appropriate authorisation.
- Have systems in place to enable the above to be managed effectively within the service. Maintain close liaison with the Data Protection Officer regarding any changes within the department.

6. Performance Criteria

6.1 Information Governance Toolkit

The NHSIA released the Information Governance Toolkit in November 2003 which contained ten information governance initiatives and aims to deliver an integrated approach to the risk assessment and continuous improvement processes involved in a number of related areas. The Toolkit was amended in July 2004 and comprises the following initiatives: -

- Confidentiality Code of Practice
- Data Protection
- Freedom of Information
- Health records
- Information Governance Management
- Information Quality Assurance(Data Accreditation)
- Information Security
- National Programme

6.2 Data Protection Act 1998 Compliance

Compliance with the Data Protection Act is mandatory and the Trust will ensure that it keeps an up to date register of all purposes for processing personal data and makes the required notification with the Information Commissioners Officer.

7. Staff Training and Awareness Programme

The Trust will ensure that training courses/presentations support this policy. The training will ensure general awareness of the Data Protection and Caldicott principles with more specific training for Data Custodians.

All new staff will receive local and corporate induction on Information Security, Data

Protection and Caldicott and will be given appropriate training material as part of their induction pack. This will be fully explained by their Manager or Data Custodian.

8. Conclusion

Compliance with Data Protection and Caldicott principles is a shared responsibility for all members of staff. By adhering to the principles, staff will help promote a secure environment where patients feel confident that their personal information is dealt with professionally and in accordance with the law.

9. Sources of Information:

The Data Protection Act 1998 An Introduction - The Information Commissioner's Office

Data Protection – Everybody's Business by the British Computer Society

Data Protection - Implementing the Legislation, A Practical guide for professionals and business Managers by the British Computer Society

The Caldicott Manual – Department of Health

The Use of Personal Data in Employer and employee relationships - UK Information Commissioners Office website http://www.informationcommissioner.gov.uk/

Salisbury Health Care NHS Trust – Data Protection and Confidentiality Policy

Hampshire Partnership NHS Trust – Access to Health Records Procedure

NFPCT

SCPCT

Other Trust Policies to be read in conjunction with this policy

Information Security Policy
Disciplinary Policy
Retention & Disposal of Records Policy
Web Services Policy
Health & Safety Policy

Appendix A

Data Protection Act 1998 – A Summary

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate business purposes.

The Data Protection Act 1998 which came into force on 1st March 2000 is concerned with "personal data" about living, identifiable individuals which is "automatically processed or manually stored as part of a relevant filing system or accessible record". It need not be particularly sensitive information, indeed it can be as little as name and address.

The Act works in two ways, giving individuals certain rights whilst requiring those who record and use personal information certain responsibilities. The Act incorporates 8 data protection principles which are binding for all organisations processing data,

All Staff are required to abide by the 8 principles of the Data Protection Act:

1. Personal data shall be processed fairly and lawfully

2. Personal data shall be obtained only for one or more specified and lawful purposes

3. Personal data shall be adequate, relevant and not excessive

4. Personal data shall be accurate and kept up to date

5. Personal data processed for any purpose must not be kept longer than necessary

6. Personal data shall be processed in accordance with the rights of data subjects under this Act

7. Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of personal data and against accidental loss or destruction

8. Personal data shall not be transferred to a country outside the European Economic Area unless that country can ensure adequate level of protection.

Everyone in the workplace has a legal duty to protect the privacy of information about individuals.

Appendix B

Data Protection Act 1998 - The First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Schedule 2 conditions

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):-

- The data subject has given their consent.
- For the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The process is necessary to protect the vital interests of the data subject.
- For the exercise of any other functions of a public nature exercised in the public interest.
- To pursue legitimate interests of the controller unless prejudicial to interests of the data subject.

Schedule 3 conditions for Processing Sensitive Data

- The data subject has given their explicit consent to the processing of the personal data.

- To comply with employers legal duty.

- In order to protect the vital interests of the data subject or another person, in a case where:-

    - Consent cannot be given by or on behalf of the data subject, or
    - The data controller cannot reasonably be expected to obtain the consent of the data subject, or
    - In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- The processing is carried out in the course of its legitimate activities by anybody or association which exists for political, philosophical, religious or trade-union purposes, and which is not established or conducted for profit, and is carried out with appropriate safeguards for the rights and freedoms of data subjects, and does not involve disclosure of the personal data to a third party without the consent of the data subject.

- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

- The processing is necessary for the purpose of, or in connection with, any legal proceedings

(including prospective legal proceedings).

- The processing is necessary for the purpose of obtaining legal advice, or

- The processing is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

- The processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by:-

  a) A health professional (as defined in the Act), or
  b) A person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

- The processing is of sensitive personal data consisting of information as to racial or ethnic origin, and the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality enabling such equality to be promoted or maintained, and the processing is carried out with the appropriate safeguards for the rights and freedoms of data subjects. The Secretary of State may by order, specify circumstances in which such processing is, or is not, to be taken to be carried out with the appropriate safeguards for the rights and freedoms of data subjects.

Interpretation

Personal data is not to be treated as being processed fairly unless the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made available to him at least:-

- The identify of the data controller;
- The purpose(s) for which data will be processed
- Any further information necessary.

Appendix C

DATA PROTECTION NOTICE FOR PATIENTS

- We *ask* you for information about yourself so that you can receive proper care and treatment
- We *keep* this information, together with details of your care, because it may be needed if we see you again.
- You have a right of access to a copy of your health records.
- We *may* use some of this information for other reasons: for example, to help us protect the health of the public generally and to see that the NHS runs efficiently, plans for the future, trains its staff, pays its bills and can account for its actions. Information may also be needed to help educate tomorrow's clinical staff and to carry out medical and other health research for the benefit of everyone.
- Sometimes the law requires us to *pass on* information: for example, to notify a birth.

The NHS Central Register for England & Wales contains basic personal details of all patients registered with a general practitioner. This Register does not contain clinical information and is not used to make any decisions about the treatment or care that you receive from your hospital or GP.
Should there be any further uses of this information there are strict controls by the NHS Information Authority and an independent body called the Security and Confidentiality Advisory Group who report to the Government Chief Medical Officer.

EVERYONE WORKING FOR THE NHS HAS A LEGAL DUTY TO KEEP INFORMATION ABOUT YOU CONFIDENTIAL.

You may be receiving care from other people as well as the NHS. So that we can all work together for your benefit we may need to share some information about you.
We only ever use or pass on information about you if people have a genuine need for it in your and everyone's interests. Whenever we can we shall remove details which identify you. Law strictly controls the sharing of some types of very sensitive personal information.
Anyone who receives information from us is also under a legal duty to keep it confidential.

THE MAIN REASONS FOR WHICH YOUR INFORMATION MAY BE NEEDED ARE:

- giving you health care and treatment
- looking after the health of the general public
- managing and planning the NHS. For example:
- making sure that our services can meet patient needs in the future
- paying your doctor, nurse, dentist, or other staff, and the hospital which treats you for the care they provide
- auditing accounts
- preparing statistics on NHS performance and activity (where steps will to be taken to ensure you cannot be identified)
- investigating complaints or legal claims
- helping staff to review the care they provide to make sure it is of the highest standard
- training and educating staff (but you can choose whether or not to be involved personally in

research approved by the Local Research Ethics Committee. You will not be identified in any published results without your agreement).

If you agree, your relatives, friends or carers will be kept up to date with the progress of your treatment.

If at any time you would like to know more about how we use your information you can speak to the person in charge of your care or to the Trust's Data Protection Officer.

Appendix D

Safe Haven Policy

Introduction

The term "Safe Haven" was originally implemented to support contracting procedures. Today a safe haven is an agreed set of administrative procedures to ensure the safety and secure handling of confidential personal information between organisations or sites. The term was initially meant to describe the transfer of facsimile messages, but should now cover the data held and used with:

- Fax machines
- Answer-phones
- Phones
- Photocopiers
- Computer Screens
- Message Books
- Post Trays
- Unopened Post
- Visitor Books
- Dictation Machinery
- Photographic / Video media

When information is transferred via a designated safe-haven point to an equivalent point in another organisation, staff can be confident that agreed protocols will govern the use of the information from that point on.

Terms of the Policy

This policy covers the Safe Haven procedures at Southampton City Primary Care Trust and has been written with the approval of the SCPCTs Caldicott Guardian.

All members of staff at SCPCT are aware of the confidential nature of their employment and the sensitive information they may come across during their working day. All staff are in possession of a Contract of Employment and have received training on General Confidentiality and Data Security requirements of their employment.

The overall responsibility for the safe transfer of patient identifiable information lies with the organisations Caldicott Guardian, but all Trust employees are responsible and will comply with the following procedures:

Facsimile Machines – See Poster http://nww.healthenet.nhs.uk/ICT/LGG/fax_poster.pdf

- Facsimile machines are sited in areas where the general public does not have physical access.
- A list of all known safe haven fax machines should be available for all users to see.
- Any other fax machines within the department/office should not be used to transmit patient identifiable information.
- Arrangement must be made for the confidential handling of transmitted data / information which may be received outside of normal working hours. This can either be addressed by the fax machine storing information overnight without it being printed out, or a designated member of staff being responsible of checking the machine each morning.

- Frequently used numbers should be identified and programmed into the fax machine “memory dial” facility to reduce risk of misdialling.
- For any external transmissions always seek confirmation from the intended recipient that the fax has been received.
- All faxes containing patient identifiable information must be transmitted using a “front” sheet which should precede the information being sent.
- The wording on the “front” sheet must make it clear that information contained in the fax is confidential and should only be read by the intended recipient.
- When patient identifiable information is transmitted every effort must be made to transmit the clinical information separately from the personal details.
- All procedures must include instructions for the process of handling misdirected facsimile information. A paragraph should appear at the bottom of the fax cover sheet which should contain text similar to:

  “The information contained in this facsimile is of a confidential nature. If you are not the intended recipient of this facsimile transmission please contact the sender as a matter of urgency.”

- According to the type of fax cartridge, disposal must take place carefully. Some faxes have a cartridge which is covered in a thin film and the patients name can still be seen on the roll. Any departments with a fax such as described, must ensure that the cartridge is disposed confidentially.

Phones - See Poster http://nww.healthenet.nhs.uk/ICT/LGG/phone_poster.pdf

- Ensure that the person you are divulging the information to is who you believe them to be. If unsure:-
  - Ask for their phone number and phone them on the landline, to check they are from where you believe them to be.
- Always be as discreet as possible when speaking of person identifiable information.
- Only divulge minimum information.
- Consistently assess whether information needs to be divulged.

Post

- Post must be opened in an area away from patients and visitors.
- Post in and post out trays must be sited away from the general public and are stored in an area with controlled access.
- Patient identifiable information is never stored in an open office.

Sending Confidential Information by Post - See Poster
http://nww.healthenet.nhs.uk/ICT/LGG/post_poster.pdf

- If posting information, confirm the name and address of the recipient.
- Whether posting internally or externally; carry out the following measures:-
  - Place the data into a sealed envelope marked confidential and state the name of the recipient that it is intended for.
  - Place the sealed, clearly marked envelope into another, and clearly mark the envelope with the name and address of the recipient but do not label it with anything else i.e. private and confidential.

- This process will ensure the envelope attracts less attention but when the outer envelope is opened, the staff concerned will see that it is private and who it is meant for by the inner address.

Transporting Personal Information - **See Poster**
http://nww.healthenet.nhs.uk/ICT/LGG/transporting_poster.pdf

- Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.
- Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.
- Information must be transported in a sealed container where available.
- Never leave personal identifiable information unattended and should not be left visible in vehicles .
- Ensure the information is returned back on site as soon as possible.
- Record that the information has been returned.

Manual Records and Books

- Message Books, Appointment Books and other written records must be sited away from the general public and at the end of each session must be stored in a secure location.

Computers, E-Mail and Web Browsing

- Patient identifiable information must not be sent over the Internet or NHSnet unless NHS encryption software is installed or using NHSmail (Contact).
- Computer screens must be angled away from the sight of visitors and the general public. This includes views from ground floor windows.
- If web browsing software is used to access patient details, then computer terminals classed as Safe Havens should only be used to access such data. These machines/terminals must be assessed to provide adequate security.
- Screen savers should be activated when a machine is left unattended. These should also automatically activate if the machine has not been accessed for a set number of minutes. It is recommended that this is no more than a five-minute period. All screen savers should be password protected, i.e. a password is needed to reactivate the screen (speak to your colleagues or ICT about how to activate screen savers.
- Do not hold personal data on machines but store on central servers with access restricted to those who need access, wherever possible.

Other Electronic Media

- Dictation machines and tapes contain extremely sensitive information and should always be kept in a locked area when not in use. They should be cleared of all dictation when the communication has been completed.
- There must be an area available for staff to use the telephone away from the public areas. One telephone in the location should be designated the Safe Haven telephone.
- Photocopying machines should be sited in areas where the general public does not have physical access.
- Answer-phones receiving personal information must have the volume lowered so that the information is not being un-necessarily shared.

Policy Administration

- Regular training sessions regarding access to patent's confidential information and the requirements of the Data Protection Act 1998 should be introduced and documented.
- The Data Custodian should perform regular checks throughout the workplace to ensure that Safe Haven Procedures are in place and are followed.
- The Data Custodian will act as the local contact point for any Safe Haven enquiries from inside and outside the organisation.
- This policy will be reviewed annually.

Conclusion

The organisation and individual staff have the responsibility to ensure the confidential transfer of personal data between organisations. It is vital that we respect individual rights under the common law duty of confidentiality and be fully aware of any guidance relating to the management of confidential personal information.