DATA PROTECTION, CALDICOTT

& CONFIDENTIALITY

POLICY & PROCEDURES

[VERSION 2]
Hampshire Partnership NHS Trust

POLICIES AND PROCEDURES PROFORMA

Subject and Version of Document: Data Protection, Caldicott & Confidentiality Policy and Procedure; Version 2

Author: Gordon Cheeseman, Information Governance Manager

Persons/Committees etc consulted whilst document in draft: Information Governance Group, P&PC, TMT, TB

Date agreed: Version 1: June 2004
Version 2: March 2007

By whom agreed: P&PC (March 04), TMT (June 04), TB

Date of next review/update and by whom: March 2010
Information Governance Group

Copy obtainable from: Website

Date document issued: Version 1: July 2004 – Update 9
Version 2: March 2007 – Update 22

Responsibility for dissemination to new staff: All Department Heads

Principal Target Audience: All staff who come into contact with personal identifiable information

Training Implications: Staff Awareness
Legal responsibilities covered in Organisational Induction.

Amendments Summary:

<table>
<thead>
<tr>
<th>Amend. No.</th>
<th>Issued</th>
<th>Page</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, Version 2</td>
<td>Nov 2006</td>
<td>All</td>
<td>Minor changes to update document</td>
</tr>
<tr>
<td>2. Version 2</td>
<td>Dec 2006</td>
<td>24 &amp; 30</td>
<td>Procedure for franked mail</td>
</tr>
<tr>
<td>4. Version 2</td>
<td>March 2007</td>
<td>24</td>
<td>NHSmail Guidance</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Introduction &amp; Relevant / Associated Legislation</td>
<td>4</td>
</tr>
<tr>
<td>1.1 Guidance on the Data Protection Act 1998, the Access to Health</td>
<td>4</td>
</tr>
<tr>
<td>Records Act 1990, the Caldicott Report 1997 and related legislation</td>
<td></td>
</tr>
<tr>
<td>1.2 Note on Terminology</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Review and Maintenance</td>
<td>5</td>
</tr>
<tr>
<td>2 Principles and Practices to ensure compliance with Data Protection</td>
<td>5</td>
</tr>
<tr>
<td>and Confidentiality</td>
<td></td>
</tr>
<tr>
<td>2.1 Data Protection Act 1998 - Principles and Practices to ensure</td>
<td>5</td>
</tr>
<tr>
<td>compliance</td>
<td></td>
</tr>
<tr>
<td>2.2 Caldicott Principles for handling person-identifiable data</td>
<td>7</td>
</tr>
<tr>
<td>3 Confidentiality</td>
<td>8</td>
</tr>
<tr>
<td>3.1 Patient Confidentiality</td>
<td>9</td>
</tr>
<tr>
<td>3.2 Staff Confidentiality</td>
<td>9</td>
</tr>
<tr>
<td>4 Exemptions to the Data Protection Act 1998</td>
<td>9</td>
</tr>
<tr>
<td>5 Roles &amp; Responsibilities</td>
<td>11</td>
</tr>
<tr>
<td>6 Performance Criteria</td>
<td>15</td>
</tr>
<tr>
<td>7 Staff Training and Awareness Programme</td>
<td>15</td>
</tr>
<tr>
<td>8 Health &amp; Safety Considerations</td>
<td>15</td>
</tr>
<tr>
<td>9 Conclusion</td>
<td>15</td>
</tr>
<tr>
<td>10 Sources of Information</td>
<td>16</td>
</tr>
<tr>
<td>11 Other Trust Policies and NHS Documents to be read in conjunction</td>
<td>16</td>
</tr>
<tr>
<td>with this policy</td>
<td></td>
</tr>
<tr>
<td>APPENDIX A Data Protection Act 1998 – A Summary</td>
<td>17</td>
</tr>
<tr>
<td>APPENDIX B Data Protection Act 1998 - The First Principle</td>
<td>18</td>
</tr>
<tr>
<td>APPENDIX C Information Sharing Leaflet</td>
<td>20/22</td>
</tr>
<tr>
<td>APPENDIX D Safe Haven Policy</td>
<td>23</td>
</tr>
<tr>
<td>APPENDIX E Posters for the transfer of information by phone, fax, post</td>
<td>27</td>
</tr>
<tr>
<td>and transport</td>
<td></td>
</tr>
<tr>
<td>APPENDIX F Procedure for franked mail</td>
<td>31</td>
</tr>
</tbody>
</table>

Author: Information Governance Manager
Version 2
March 2007
1. Introduction & Relevant / Associated Legislation


This document describes the Hampshire Partnership NHS Trust 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 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 request access to the files.

The Caldicott Report 1997 provides guidance to the NHS on the use and protection of patient identifiable information (PII), 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 requirement or court order 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

This policy will be subject to regular review and, if revised, all staff will be alerted to the new version. Forms referred to in this policy are available from Southampton ICT Shared Services.

The Information Security Team, Southampton ICT Shared Services, maintain this policy on behalf of Hampshire Partnership NHS Trust.

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

The latest version can be found on the Trust Website.

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:

- Ensuring the Trust’s Data Protection Notification is kept up to date.

- Complying with the common law duty of confidentiality; 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.

- 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. (Confidentiality and Information Sharing Policy (CP 12.1 and NCP 5.1))

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 Records Policy and Procedures (CP 21 and NCP 8) and professional guidelines, on taking and making of records, are adhered to, see Data Quality Policy (NCP 28.3).

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 Health Records Policy and Procedures (CP 21 and NCP 8);

• 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.

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 (IG2) 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**

The organisation must 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. The Caldicott Guardian, Director of Information and Estates, is responsible for ensuring that the organisation complies with legal requirements.

3. **Confidentiality**

The 'Confidentiality: NHS Code of Practice' has been published by the Department of Health following a major public consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

This document is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

For the purposes of this document, the term ‘staff ’ is used as a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health. This includes private and voluntary sector staff.

This document

- a. introduces the concept of confidentiality;
- b. describes what a confidential service should look like;
- c. provides a high level description of the main legal requirements;
- d. recommends a generic decision support tool for sharing/disclosing information;
- e. lists examples of particular information disclosure scenarios.

A summary of the key confidentiality issues can be gained by reading the main body of the document (pages 1-12), while the supporting Annexes provide detailed advice and guidance on the delivery of a confidential service.

3.1 **Patient Confidentiality**

3.1.1 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.

3.1.2 On admission and/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, and those they specifically do not give permission to receive information. A ‘consent to share’ form is available from Interagency Policy on Confidentiality and the Management of Service User Information CP 12.1 Appendix 2.

3.1.3 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.

3.1.4 In the event of the patient being unable to give permission a person must be identified to act in the best interests of the patient and permission obtained from him/her.

> In all cases, the wishes expressed must be appropriately documented in the patient’s Health Records.

3.2 **Staff Confidentiality**

3.2.1 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.

3.2.2 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.

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

3.2.4 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 guidance is below. 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

4.2.1 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.

4.2.2 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
- 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

4.2.3 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 at Work Act 1974
- Terminations - Abortion Regulations 1991
- Offenders thought to be mentally disordered – Mental Health Act 1983
- Child abuse - Children’s Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime eg terrorism, murder - The Crime and Disorder Act 1998

4.2.4 If in doubt, staff should seek guidance, in confidence, from the senior Clinician or the appropriate Senior Manager or the Information Governance Manager or the Litigation Manager or the Caldicott Guardian.

Hampshire Partnership NHS Trust 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 provided the identity of the third party is not revealed. The DPA 98 suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous.

Further guidance is available from the Litigation Manager or the Records Advisor or the Information Governance Manager.

4.3.2 The Trust is not required to supply copies of health 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 health 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.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf) 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

The Hampshire Partnership NHS Trust has established 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 Confidentiality: NHS Code of Practice.

- 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 Andrew Clapper, Director Information & Estates. 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 annual Information Governance Toolkit assessment. To assist with the volume and diversity of this task the Guardian is supported by the Information Security Team, the Litigation Manager, the Records Manager, the Information and Performance Manager and the Data Custodians.

5.3 Data Protection Officer

The Data Protection Officer is Andrew Clapper, Director Information & Estates. 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

5.3.1 To support the Data Protection Officer and Caldicott Guardian the following roles have been identified as recommended in 'Introduction to Data Protection V1.0 NHS Executive.'
5.4 Records Manager

One task of the Records Manager is to facilitate all the Data Protection and Caldicott functions within the Trust. The Records Manager liaises closely with the Data Custodians (see 5.7) and the Information Security Team in Southampton ICT Shared Services.

The main tasks are to:

- 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 and reporting these to the Information Governance Manager.

5.5 Litigation Manager & Records Advisor to provide training and support to teams who are responsible for ensuring Subject Access Requests are handled in accordance with procedures.

5.6 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:

5.6.1 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

5.6.2 Information Governance Manager

The main task is to provide a source of up-to-date expertise on information governance issues. The Information Governance Manager provides support to the Data Protection Officer and the Caldicott Guardian; 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.
- Liaise with the 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

5.7 Managers

Managers are responsible for ensuring that policies are complied with, and breaches and issues raised by staff are acted upon. Managers are also responsible for ensuring that Data Custodians are appointed.

5.8 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 Records Manager and Information Governance Manager 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 Organisational 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.
6. **Performance Criteria**

6.1 **Information Governance Toolkit**

Connecting for Health released Version 4 of the Information Governance Toolkit in October 2006 which contains six information governance initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

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 Office.

7. **Staff Training and Awareness Programme**

7.1 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.

7.2 All new staff will receive local and organisational 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. **Health & Safety Considerations**

Staff must follow H&S requirements when handling and storing manual and paper records. In particular staff must not:

- block fire exits and escape routes
- that records are not stored at unsafe heights
- the placement of records minimises the risk of fire.

9. **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.
10. **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 – NHS Executive
- The Use of Personal Data in Employer and employee relationships - UK Information Commissioners Office website [http://www.ico.gov.uk/](http://www.ico.gov.uk/)
- Salisbury Health Care NHS Trust – Data Protection and Confidentiality Policy
- HPT – Access to Health Records Procedure (NCP 17)
- NFPCT and SCPCT

11. **Other Trust Policies and NHS Documents to be read in conjunction with this policy**

Information Security Policy – IG 2
Disciplinary Procedure – PP7
Health Records Policy and Procedure– CP 21
Internet & Email Acceptable Use Policy – IG 1
Access to Health Records Procedure – NCP 17
Inter-agency Policy on Confidentiality and the Management of Service user Information – CP12.1
Confidentiality: NHS Code of Practice
NHSmail Acceptable Use Policy – IG 7
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 health professional (as defined in the Act), or
- 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.
Your rights

You have a right to see all the records we hold about you both on paper or computer except for information that

☐ has been provided about you by someone else if they haven’t given permission for you to see it or
☐ relates to criminal offences or
☐ is being used to detect or prevent crime or
☐ could cause physical or mental harm to you or someone else

We will obtain your consent to share information with others as you receive services from us.

Further information is available on how we use the information we keep about you and how you can see your records. This can be obtained through your care co-ordinator.

We hope this leaflet addresses some of your concerns about the use and confidentiality of your records but if you have any further questions you can speak directly to your care co-ordinator or their manager.

The government is developing a national care record for NHS patients in England. This will change the way your records are stored on computer and who will have access to them. This is being phased in over the next few years and we will inform you through your care coordinator when this is likely to affect you. If you want to obtain further details this is available through www.connectingforhealth.nhs.uk

Hampshire Health Authority has also developed a local electronic care record system upon which your details will be held. You have the right to withdraw from this. If you wish to do so, please telephone 023 8072 5500.
Making your records work for you

Your records are used to guide and record the treatment and care you receive. Your records are vital in helping to ensure you receive good quality and timely care. Keeping records means that:

- We have all the information necessary for assessing your needs and the type and quality of care you require
- Your concerns can be properly investigated if you need to complain
- Full and accurate information about you is available if you
  - move to another area
  - need to use another service
  - see a different healthcare professional
- Professionals involved in your care have accurate and up-to-date information

How your records are used to help us

As well as ensuring you receive the right care, your records can also provide us with an important source of information when we need to:

- Review the care we provide to ensure it is of the highest standard
- Investigate complaints, legal claims or untoward incidents
- Prepare statistics about services
- Audit accounts and services
- Conduct research and development to help us look after the health of the general public and to make sure our services can meet future demand
- Teach and train health and social care professionals

Unless we are investigating a complaint you have made, the records we use for these purposes will not include any of your personal details.

Sometimes, for statistical, research or training purposes it is helpful to have more personal details as this can help us to identify particular trends or needs. However we will only use your personal information in this way if you give us your consent.

When other people need information about you

Everyone working in Health and Social Services has a legal duty to keep information about you confidential. Anyone who receives information from us is also under a legal duty to keep it confidential.

From time to time we may need to share information with other professionals and services concerned in your care. This may be for instance, when your care co-ordinator needs to discuss your case with other professionals (who may not be in the same team) in order to plan your care. We do this in order to provide the most appropriate treatment and support for you and your carers, or when the welfare of other people is involved. We will only share information in this way if we have your permission and it is considered necessary.

There may be other circumstances when we must share information with other agencies. In these rare circumstances we are not required to seek your consent. Examples of this are:

- If there is a concern that you are putting yourself at risk of serious harm
- If there is concern that you are putting another person at risk of serious harm
- If we have been instructed to do so by a Court
- If the information is essential for the investigation of a serious crime
- If you are subject to the Mental Health Act (1983), there are circumstances in which your “nearest relative” must receive information even if you object.

The records we keep about your health and care may include:

- Basic details that you have given us, such as address and next of kin
- Notes and reports about your health and any treatment, care or support you need and receive
- Results of your tests
- Relevant information from other professionals, relatives or those who care for you or know you well
- any contacts you have with us such as visits or outpatient appointments

If you have concerns about the information that you share with a professional providing care please discuss with them how it is kept and what will be shared with others.

The law protects your right to confidentiality and we will ensure your records are kept confidential at all times.

Why we collect information about you

The NHS and Social Services work together and share information to ensure the care you receive is effective, of a good quality and meets your needs.

Health and Social Care professionals working with you - such as doctors, nurses, psychologists, occupational therapists and social workers - keep records about your health and any care and treatment you receive. These records may be written (usually called ‘casenotes’) and are held by the care co-ordinator you see or by other professionals involved in your care. Some or all of your records may be held on a computer system. The computer system may be a Social Services and/or a NHS system.

The NHS and Social Services work together and share information to ensure the care you receive is effective, of a good quality and meets your needs.

Health and Social Care professionals working with you - such as doctors, nurses, psychologists, occupational therapists and social workers - keep records about your health and any care and treatment you receive. These records may be written (usually called ‘casenotes’) and are held by the care co-ordinator you see or by other professionals involved in your care. Some or all of your records may be held on a computer system. The computer system may be a Social Services and/or a NHS system.
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 Hampshire Partnership NHS Trust and has been written with the approval of the Hampshire Partnership NHS Trust Caldicott Guardian.

All members of staff at Hampshire Partnership NHS Trust 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 (Appendix E)

- 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 Hampshire Partnership NHS Trust 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** (Appendix E)

- 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.
- Assess whether information needs to be divulged. If in doubt ask for clarification in writing, email or fax.

**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** (Appendix E)
- If posting information, confirm the name and address of the recipient.
- When posting internally; 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 person concerned will see that it is private and who it is meant for by the inner address.
- When communicating by post with patients or colleagues using external mail, you must put an External Return Address (ERA) on all franked mail. This is to ensure that should it be undeliverable then the Royal Mail will be able to return it to the sender. Consider making the ERA as anonymous as possible to avoid any unnecessary disclosure of who the sending organisation is. This can be achieved by putting the originator’s post code plus a room number or identifying team initials. See further guidance from the Royal Mail at Appendix F.

Transporting Personal Information - See Poster (Appendix E)

- 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.
- 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.(see NHSmail Acceptable Use Policy (IG 7))
- 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.

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 regularly reviewed.

**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.
Guidance for sharing personal information by FAX

Follow steps 1-6

1. Telephone the recipient of the fax (or their representative) to let them know you are going to send confidential information.

2. Ask them to acknowledge receipt of the fax.

3. Double check the fax number.

4. Use pre-programmed numbers wherever possible.

5. Make sure your fax cover sheet states who the information is for, and mark it “Private and Confidential.”

6. If appropriate, request a report sheet to confirm that transmission was OK.

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

If you are faxing to a known Safe Haven/Secure fax you do need to follow these guidelines. The patient’s name must not be faxed with clinical details. Unless agreed by your Manager.
Guidance for sharing personal information by PHONE

1. Confirm the name, job title, department and organisation of the person requesting the information.

2. Confirm the reason for the information request if appropriate.

3. Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient’s name, job title, organisation and telephone number.

4. Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.

5. Provide the information only to the person who has requested it (do not leave messages).

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

Take a contact telephone number e.g. main switchboard number (never a direct line or mobile telephone number) To ensure requestor is at a recognised base

Information Security and Confidentiality

Information Security Team
ICT Services
Guidance for sharing personal information by POST

1. Confirm the name, department and address of the recipient.

2. Seal the information in a robust envelope.

3. Mark the envelope “Private & Confidential-To be opened by Addressee Only.”

4. When appropriate, send the information by Recorded Delivery.

5. When necessary, ask the recipient to confirm receipt.

If information is time critical, ensure addressee is aware of urgency and is available to act on information sent.

If intended addressee is not available, ensure that you identify a person to act on the information you are sending.

This guidance relates to Data Protection Principles 6 and 7 and Caldicott Principle 4

Information Security and Confidentiality

Information Security Team
ICT Services
Guidance for TRANSPORTING personal information

1. Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.

2. Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.

3. Information must be transported in a sealed container.


5. Ensure the information is returned back on site as soon as possible.

6. Record that the information has been returned.

This guidance relates to Data Protection Principle 7 and Caldicott Principles 4 and 6

Information Security Team
ICT Services
UNDELIVERABLE FRANKED MAIL – NEW PROCEDURE FROM ROYAL MAIL

Overview

Every year, we handle 21 million franked items that are undeliverable or marked ‘return to sender’ with no return address on the outside. 14 million of these are eventually destroyed.

Think how much that is costing you in wasted postage and lost business. You could be sending to ‘false’ addresses, as you can’t determine whether your customers are actually receiving your mail. If they do not respond to your mailing is it because they are not interested in your product or because they have changed address?

Key features

By including an External Return Address (ERA) on your franked mail, we can quickly return all your undelivered items at no extra cost, so you will know you have only ‘live’ customers on your database. This saves you wasted postage and gives you better results from your mailings.

From 4th October 2004, if you want your undeliverable franked mail to be returned to you, you must include an ERA. From then, we will be ending our return service for undelivered franked mail without an ERA, so those items will be disposed of.

Undeliverable means:

- an item is impracticable or unreasonable to deliver
- the delivery address is unsafe
- the delivery address is not permanently occupied
- the item does not have a complete, correct or legible address
- any reason concerning health and safety of staff
- any other reason

Product instructions

The best place to put your ERA is on the back of your mail (in the middle at the top, no bigger than 70mm x 30mm), which means your stationery must be pre-printed.

Alternatively, you can put it in the slogan block in your franking impression (ask your supplier who will automatically apply Royal Mail’s ‘Return Address Guidelines’ issued to them).

If you wish your company to remain anonymous, you can have a PO Box address as your ERA. Please call 08457 950 950 to arrange this.
Pricing

Costs for pre-printed stationery and new franking marks for slogan blocks must be met by the customer. Prices will vary depending on your printing supplier, your franking machine supplier and the type of your franking machine.

What to do next

- If you want your undeliverable franked mail returned to you, you will need to incorporate an ERA on your mail.
- Pre-print your stationery – you may already have your stationery pre-printed with your Brand or logo, check with your printer so they can advise on how to incorporate an ERA on your envelopes in the correct place (as stated above).
- If you post very small volumes you may wish to use a hand-stamp to put an ERA on the back of your envelopes once sealed. Hand-stamps are a cheap and effective method of placing an ERA on smaller volumes.
- If you already use a franking machine to frank your mail, why not ask your supplier if you can incorporate an ERA in to your franking impression, this is an efficient method of ensuring all your mail includes an ERA.

More information

For more information on External Return Addresses, and for changes to our franking terms and conditions, please call your Royal Mail Sales Centre on 08457 950 950.

To contact your franking machine supplier, please call:

Pitney Bowes – 08705 25 25 25
SECAP Ltd (a wholly owned subsidiary of Pitney Bowes) – 08705 023 023
Neopost Ltd – 01708 738 344
Frama UK Ltd – 01992 451 125
Francotyp Postalia Ltd – 0500 223 56