Data Protection, Caldicott and Confidentiality Policy

This document describes the Trusts’ policy on Data Protection and Caldicott requirements, and employees’ responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and electronically.

| Key Words: | Data Protection Act; Caldicott Guardian; principles; confidentiality; information governance; information security; Information Asset owners; Information Asset Administrators |
| Version: | V1 Final |
| Adopted by: | Quality Assurance Committee |
| Date Adopted: | 21/1/15 |
| Name of author: (owner of policy): | Records Transformation & Information Governance Manager |
| Name of responsible committee: | Records and Information Governance Group |
| Date issued for publication: | January 2015 |
| Review date: | May 2016 |
| Expiry date: | November 2016 |
| Target audience: | All Staff |
| Type of Policy (tick appropriate box): | Clinical ✓ | Non Clinical ✓ |
CONTRIBUTION LIST

Key individuals involved in developing the document

<table>
<thead>
<tr>
<th>Name</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary Stait</td>
<td>Information Governance Compliance Manager</td>
</tr>
<tr>
<td>Fern Barrell</td>
<td></td>
</tr>
<tr>
<td>Lesley Tooley</td>
<td></td>
</tr>
</tbody>
</table>

Circulated to the following individuals for comments

<table>
<thead>
<tr>
<th>Name</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr Satheesh Kumar</td>
<td>Medical Director (Caldicott Guardian)</td>
</tr>
<tr>
<td>Adrian Childs</td>
<td>Chief Nurse/Deputy Chief Executive (SIRO)</td>
</tr>
<tr>
<td>Members of Records and Information Governance Group</td>
<td></td>
</tr>
<tr>
<td>Members of Clinical Effectiveness Group</td>
<td></td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equality statement</td>
<td>5</td>
</tr>
<tr>
<td>Due Regard</td>
<td>6</td>
</tr>
<tr>
<td>NHS Constitution</td>
<td>6</td>
</tr>
<tr>
<td>Definitions</td>
<td>7</td>
</tr>
<tr>
<td>1.0 Summary</td>
<td>9</td>
</tr>
<tr>
<td>2.0 Introduction</td>
<td>9</td>
</tr>
<tr>
<td>3.0 Purpose</td>
<td>10</td>
</tr>
<tr>
<td>4.0 Duties within the Organisation</td>
<td>11</td>
</tr>
<tr>
<td>5.0 Main Policy Content</td>
<td>13</td>
</tr>
<tr>
<td>5.1 Data Protection Act 1998 – Principles and Practice to ensure compliance</td>
<td>13</td>
</tr>
<tr>
<td>5.2 Caldicott Principles for Handling Personal Confidential Data (PCD)</td>
<td>16</td>
</tr>
<tr>
<td>5.3 Confidentiality</td>
<td>17</td>
</tr>
<tr>
<td>5.3.1 Patient Confidentiality</td>
<td>18</td>
</tr>
<tr>
<td>5.3.2 Staff Confidentiality</td>
<td>19</td>
</tr>
<tr>
<td>5.4 Exemptions To The Data Protection Act 1998</td>
<td>19</td>
</tr>
<tr>
<td>5.4.1 Disclosing Information against an Individuals’ Wishes</td>
<td>19</td>
</tr>
<tr>
<td>5.4.2 Non-Disclosure of Personal Information held in a Health Record</td>
<td>20</td>
</tr>
<tr>
<td>5.4.3 Personal Identifiable Data In Medical Research</td>
<td>21</td>
</tr>
<tr>
<td>5.5 Privacy Impact Assessment Procedure and Template</td>
<td>22</td>
</tr>
<tr>
<td>6.0 Safe Haven Requirements</td>
<td>22</td>
</tr>
<tr>
<td>6.1 Communication by Post</td>
<td>22</td>
</tr>
<tr>
<td>6.1.1 Internal Post</td>
<td>22</td>
</tr>
<tr>
<td>6.1.2 External Post</td>
<td>22</td>
</tr>
<tr>
<td>6.2 Verbal Communication</td>
<td>23</td>
</tr>
<tr>
<td>6.3 Communication by Faxes</td>
<td>23</td>
</tr>
<tr>
<td>6.4 Computers and electronic storage devices</td>
<td>24</td>
</tr>
<tr>
<td>6.4.1 Encrypting personal confidential data on CD’s and DVDs</td>
<td>24</td>
</tr>
<tr>
<td>6.5 Whiteboards/Noticeboards</td>
<td>24</td>
</tr>
<tr>
<td>7.0 Pseudonymisation</td>
<td>24</td>
</tr>
<tr>
<td>8.0 De-identification</td>
<td>25</td>
</tr>
<tr>
<td>9.0 Confidentiality Audit Approach</td>
<td>25</td>
</tr>
<tr>
<td>10.0 Sharing Information with other Organisations</td>
<td>26</td>
</tr>
<tr>
<td>11.0 Training</td>
<td>26</td>
</tr>
<tr>
<td>12.0 Dissemination</td>
<td>27</td>
</tr>
<tr>
<td>13.0 Monitoring and Compliance</td>
<td>27</td>
</tr>
<tr>
<td>13.1 Data Protection Act 1998 Compliance</td>
<td>28</td>
</tr>
<tr>
<td>14.0 Links to Performance Indicators</td>
<td>28</td>
</tr>
<tr>
<td>15.0 Review</td>
<td>28</td>
</tr>
<tr>
<td>15.1 Archiving</td>
<td>28</td>
</tr>
<tr>
<td>16.0 References and Associated Documents</td>
<td>28</td>
</tr>
<tr>
<td>APPENDICES</td>
<td>28</td>
</tr>
<tr>
<td>Appendix 1 Caldicott Approval Procedure</td>
<td>29</td>
</tr>
<tr>
<td>Appendix 2 Privacy Notice</td>
<td>35</td>
</tr>
<tr>
<td>Appendix 3 Checklist for Procedural documents</td>
<td>37</td>
</tr>
<tr>
<td>Appendix 4 Training Requirements Checklist</td>
<td>39</td>
</tr>
<tr>
<td>Appendix 5</td>
<td>Policy Monitoring Chart</td>
</tr>
</tbody>
</table>

Version Control and Summary of Changes
For further information contact:

Records Transformation & Information Governance Manager 0116 2950997

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all.

This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

In carrying out its functions, LPT must have due regard to the different needs of different protected equality groups in their area.

This applies to all the activities for which LPT is responsible, including policy development and review.
Due Regard

The Trusts commitment to equality means that this policy has been screened in relation to paying due regard to the Public Sector Equality Duty as set out in the Equality Act 2010 to eliminate unlawful discrimination, harassment, victimisation; advance equality of opportunity and foster good relations.

A due regard review found the activity outlined in the document to be equality neutral because the principles of the Data Protection Act 1998 and Caldicott are universal and provide the basis upon which the handling of personal and personal sensitive information is required to be processed.

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay.

The NHS will provide a comprehensive range of services

| Shape its services around the needs and preferences of individual patients, their families and their carers | ✓ |
| Respond to different needs of different sectors of the population | ✓ |
| Work continuously to improve quality services and to minimise errors | ✓ |
| Support and value its staff | ✓ |
| Work together with others to ensure a seamless service for patients | ✓ |
| Help keep people healthy and work to reduce health inequalities | ☐ |
| Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance | ✓ |
## Definitions that apply to this Policy

| **Caldicott Report** | Provides guidance to the NHS on the use and protection of personal confidential information (PCD), and emphasises the need for controls over the availability and access to such information. It made a series of recommendations which led to the requirement for all NHS organisations to appoint a Caldicott Guardian, who is responsible ensuring compliance with the 6 (original) Caldicott confidentiality principles.  
| **Databases** | Are any collections of personal information that can be processed by automated means. A few examples are detailed below:  
- Patient/personal records (names and addresses etc) for appointments  
- Patient/personal information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this can be an Excel spreadsheet  
- Patient/personal details used for prescribing drugs  
- Staff records held on Excel or other locally developed databases, to monitor annual leave and sickness |
| **Data Controller** | Is the body/organisation and/or individual person who controls how the personal data shall be processed. The data controller can be either an organisation, a group of people who share control or an individual member of staff. |
| **Data Processing** | Any operation performed on data. The main examples are collection, retention, deletion, use and disclosure. |
| **Data Subject** | Is the individual to whom the personal data relates. |
| **Disclosure** | The passing of information from the Data Controller to another organisation / individual |
| **Personal Data** | Is information about a living, identifiable individual. This will include any opinion expressed about an individual. It need not be particularly sensitive information, and can be as little as a name and address. |
| **Primary uses** | Information used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare services |
## Safe Haven

Term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure personal confidential information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post, email, telephone or other means. Any members of staff handling confidential information must adhere to safe haven principles.

## Sensitive Personal Data

Is defined as any of the following classes of data:

a) The racial or ethnic origin of the data subject,
b) Their political opinions,
c) Their religious beliefs or other beliefs of a similar nature,
d) Whether they are a member of a trade union,
e) Their physical or mental health or condition,
f) Their sexual life,
g) The commission or alleged commission by them of any offence, or
h) Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

## Secondary uses

For non-healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When personal confidential data is used for secondary purposes this should, where appropriate, be limited and de-identified so that the secondary use process is confidential.
1.0 Summary

Personal information held by the Leicestershire Partnership NHS Trust (hereafter referred to as ‘the Trust’, is an important and valuable asset. The Trust recognises that the lawful and correct treatment of personal data is very important in delivering an effective health service and maintaining confidence with our clients.

Sharing personal information between service area and partner agencies is vital for the provision of co-ordinated and seamless care of individuals. Legislation does not prevent the sharing of information between agencies but places important rules and safeguards that must be observed.

The Trust has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, other advisory groups to the NHS and guidance issued by professional bodies.

This document describes the Trusts' policy on Data Protection and Caldicott requirements, and employees’ responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and electronically.

2.0 Introduction

The 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.

Data protection law exists to strike a balance between the rights of individuals to privacy and the ability of the organisation 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, in deed 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:

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.

3.0 Purpose

The purpose of this policy provides the framework to ensure that the Trust complies with the requirements of the Data Protection Act 1998, Caldicott Principles and the NHS Code of Confidentiality.

3.1 This policy covers all identifiable information created, processed and stored on living individuals, patients and staff. Throughout this document the term “patient” is used to refer to an individual who is receiving a service from the Trust, and this term includes those people who are also known as “Service Users”, and “Clients”. Similarly the terms “clinician” and “healthcare professional” are used, but should be interpreted as encompassing social care staff and NHS practitioners.

3.2 This policy applies to all employees of the Trust, any staff who are seconded to them, contract and agency staff and volunteers.

3.3 All employees are responsible for maintaining patient confidentiality. The duty of confidentiality is written into employment contracts. Breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence, which could result in dismissal and/or prosecution.

3.4 Patients expect that information about them will be treated as confidential and are given that assurance in the NHS Constitution for England. Patients who feel that confidence has been breached may issue a complaint under the NHS complaints procedure or they could take legal action.

ALL STAFF HAVE A LEGAL DUTY TO PROTECT THE PRIVACY OF INFORMATION ABOUT INDIVIDUALS
4.0 Duties within the Organisation

4.1 The Trust Board has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

4.2. The Chief Executive has a duty to ensure that:

- Staff are aware of the need to comply with the Data Protection Act 1998, in particular with the rights of patients wishing to access personal information and/or their health records
- Staff are aware of the requirements of the common law duty of confidence as set out in the Confidentiality: NHS Code of Practice
- Arrangements with third parties who access 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 Data Protection Act 1998 and how it applies to the use of data for research purposes.

4.3 The Caldicott Guardian (Medical Director) is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of personal confidential data across the Trust and supporting agencies. To assist with the volume and diversity of this task the Caldicott Guardian is supported by the Records Transformation and Information Governance Manager, Divisional IG Leads and Information Asset Owners (who act as Data Custodians).

4.4 Records Transformation and Information Governance Manager (Data Protection Officer) has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the Data Protection Act 1998, throughout the Trust

Main Tasks

- To promote awareness of the Act and Procedures contained in this policy
- To be responsible for compliance with the Data Protection Act 1998 and the eight principles
- To ensure Trust compliance with Notification requirements with the Information Commissioners Office
- To monitor changes to working practices, and where any such changes are found to come within the remit of the Data Protection Act 1998, take appropriate action
- Facilitate all the data protection and Caldicott functions within the Trust
- Advise and update the Trust in relation to directives/guidance from the Information Commissioner and the Department of Health
- Via the Information Governance Framework, ensure that the Caldicott Guardian and SIRO are informed of relevant issues and decisions are recorded
- Responsible for co-ordinating the return of the annual Information Governance Toolkit assessment
- Working with the Information Governance Compliance Manager to develop
and support the Information Request process, especially in relation to subject access requests

4.5 Information Asset owners undertake the role and responsibility of Data Custodians, as referred to in the Data Protection Act 1998 and are responsible for ensuring that the Data Protection and Caldicott principles are fully observed and complied with by staff within their Division/Service/Department. Working with Team/Service Managers, Information Asset Owners are required to ensure that all data flows and processing of data complies with all current Data Protection policies, working closely with the Records Transformation & Information Governance Manager as appropriate.

- Promote Data Protection and Caldicott Principles on an on-going basis
- Ensure that all staff know the procedure for reporting IG and IT security incidents
- Carry out an annual review of the Information Asset Register to enable an assessment of compliance with Data Protection and Caldicott Principles
- Have systems in place to enable the above to be managed effectively within the service

4.6 Managers will ensure that all staff:

- are aware of the Data Protection Policy and updates in regard to any changes in the Policy,
- undertake appropriate training including the annual mandatory IG training
- have access to all relevant systems and procedures to support the Policy,
- know how to deal with requests for personal/patient identifiable information,
- know how to access and store personal/patient identifiable information, both manual and electronic records,
- Report actual and potential breaches and issues and seek advice where necessary
- register databases with the Information Management and Technology Operations Group via their Divisional representative, who will maintain a log of databases and nominated application/system managers

4.7 All staff must be aware of the underlying principle that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised persons include NHS staff who are not involved in either the clinical care of the patient or the associated administration processes.

Staff who become patients do not have an automatic right to view their own information. Equally, staff do not have an automatic right to view or access information about their family, friends or work colleagues, Subject Access Requests must be made using the Trust's Access to Personal Information Policy.

Staff whose duties require them to have access to patient information will receive specific guidance and instruction from their direct line manager.
Staff need to be aware that inappropriate use or loss of information is a potentially serious and reportable incident, and should be reported in accordance with the Trust Incident Reporting Policy.

All staff are expected to:

- adhere to this Policy and all related systems and processes to implement the Act,
- undertake training as appropriate, including their annual IG training
- ensure that all patient/personal identifiable information is accurate, relevant, up to date and used appropriately, both electronic and manual including the use of databases,
- ensure that all patient/personal identifiable information is kept secure at all times.
- ensure that patient information is recorded accurately
- inform patients how their information will be used and ensure that they understand. The patient should understand that the information given will be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided.
- provide choice and allow patients to decide whether their information can be recorded, disclosed or used in particular ways. People have very different needs and values – they must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information.
- improve ways and always look for better ways to safeguard information
- be aware of the issues surrounding confidentiality, and seeking training or support where uncertain in order to deal with patients’ information appropriately.
- report possible breaches or risks of breaches to patient confidentiality.

5.0 Main policy content

This policy sets out the framework to ensure that the trust complies with the law.

5.1 Data Protection Act 1998 – Principles and Practice to ensure compliance

The Trust will put in place procedures to ensure that the eight principles in the Data Protection Act 1998 are met.

Principle 1 – Personal data shall be processed fairly and lawfully

Compliance 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. However the law recognises that research which does not directly lead to decisions about a person should have a special freedom to use information in ways not foreseen when it was collected but these uses must be fair and lawful (Taken directly from MRC Executive Summary – Personal Information in Medical Research)

- Ensuring that certain conditions in Schedules 2 and 3 of the Act are met (see Appendix 2 for detail of the Data Protection Act 1998 – Principle 1)
- Informing the individual how their information will be processed. This means fully describing how the information will be used i.e. what will be done with the information; for what reason will it be used; who will it be passed on to; how will it get there, stored and destroyed.

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 shared is only used for the purposes for which it was originally obtained
- Those involved in research must develop procedures for making patients aware that their information may sometimes be used for research, and explaining the reasons and safeguards. Any objections from patients must be respected (MRC Executive Summary – Personal Information in Medical Research)

This will be achieved by:

- Conducting routine audits as part of good data management practice
- Ensuring that relevant records policies and professional guidelines, i.e. information lifecycle, are adhered to

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
This will be achieved by:

- Adherence to Information Governance Policies (i.e. information lifecycle)
- Staff working in joint team situations using the maximum retention period
- Compliance with the Department of Health’s Records Management: NHS Code of Practice, Part 2 provides a comprehensive retention schedule, which is reflected in the information lifecycle and records management policy

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

- Right of access (e.g. to see or have a copy of your health 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 making
- Right to take action for compensation if the individual suffers damage
- Right to take action to correct, block, erase or destroy inaccurate information
- 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 Information Policy details the process to be followed to manage a Subject Access Request

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 in relation to whether it has a right to provide a service. This decision can only be made by the Caldicott Guardian

The following principles must be adhered to:

**Principle 5** – Personal data must be kept no longer than necessary

**Principle 6** – Personal data must be processed in accordance with the rights of the individual

**Principle 7** – Personal data must be kept secure

**Principle 8** – Personal data shall not be transferred to a country outside the European Economic Area unless that country can ensure adequate levels 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 individuals in relation to the processing of personal data.

5.2 Caldicott Principles for handling personal confidential data (PCD):

1 – Justify the Purpose

Every proposed use or transfer of personal confidential data within or from and organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate Guardian.

2 – Don’t use personal confidential data unless absolutely necessary

Personal confidential data 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)

3 – Use the minimum amount of personal confidential data necessary

Where the use of personal confidential data 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 necessary for a given function to be carried out.

4 – Access to personal confidential data should be on a strict need-to-know basis

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

5 – Everyone with access to personal confidential data should be aware of their responsibilities

The organisation must ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality

6 – Understand and comply with the law

Every use of personal confidential data must be lawful. The Caldicott Guardian, Medical Director, is responsible for ensuring that the organisation complies with legal requirements

7 – The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share
information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers; regulators and professional bodies [Refer to the Information Sharing Policy]

Where there is a request to access or to share information outside of a regular flow of information, staff are expected to follow the Caldicott approval process (Appendix 1).

5.3 Confidentiality

The ‘Confidentiality: NHS Code of Practice’ was published by the Department of Health following major consultation in 2002/03. 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.

The Code of Practice 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. This document uses the term ‘staff’ 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 services. This includes local authority staff working in integrated teams and private and voluntary sector staff.

This document:

1. Introduces the concept of confidentiality
2. Describes what a confidential service should look like
3. Provides a high level description of the main legal requirements
4. Recommends a generic decision support tool for sharing/disclosing information
5. 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.

The full document can be accessed from

To compliment this document a ‘Supplementary Guidance: Public Interest Disclosures published in November 2010 is available for NHS staff in making what are often difficult decisions on whether a breach of confidentiality can be justified in the public interest


Following the publication of the Caldicott Review in March 2013, the Health and Social Care Information Centre (HSCIC) published ‘ A guide to confidentiality in
health and social care’ which identified five rules for treating confidential information with respect:

Rule 1 – Confidential information about service users or patients should be treated confidentially and respectfully

Rule 2 – Members of a care team should share confidential information when it is needed for the safe and effective care of an individual

Rule 3 – Information that is shared for the benefit of the community should be anonymised

Rule 4 – An individual’s right to object to the sharing of confidential information about them should be respected

Rule 5 – Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

The full document which contains other helpful guidance can be found:


5.3.1 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 be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

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. This information must be recorded in the clinical record – either an electronic patient record system or paper health record.

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.

For further guidance – please refer to the Information Sharing Policy

As a research active organisation staff might screen patients’ records to identify any potential research participants with the Consultants permission. Patients may also be approached by staff regarding participation in a particular research study in order to obtain consent.
In the event of the patient being unable to give permission, the Mental Capacity Act 2005 must be followed. Staff should refer to the Mental Capacity Act Policy for detail.

**In all cases, the wishes expressed must be appropriately documented in the patients’ clinical record**

5.3.2 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 discussion and confirmation with a senior manager in the Trust. 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 approved Data Protection and Confidentiality clauses on all contracts with 3rd party contractors and suppliers who process personal information.

5.4 Exemptions to the Data Protection Act 1998

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.

5.4.1 Disclosing information against an individuals’ wishes

The responsibility to withhold or disclose information without the individuals’ consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

Circumstances where an individuals’ right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the individuals’ life may be in danger, or cases in which they may not be capable of forming an appropriate decision
- Where there is a serious danger to other people, where the rights of others may supersede those of the individual, 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.
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 in the work place – Health & Safety at Work Act 1974
- Terminations – Abortion Regulations 1991
- Child Abuse – Childrens 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 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 manager or the Information Governance lead or the Caldicott Guardian

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

5.4.2 Non-Disclosure of personal information held in a health record

An individual requesting access to their health records may be refused access to parts of the information is an appropriate clinician deems exposure to that information could cause physical or mental harm to the individual 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 must be documented.

Where access would disclose information relating to or provided by a third party, consent for release must be sought from 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 a third party does not consent, the information may be disclosed provided that the identity of the third party is not revealed. The DPA 1998 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 Information Request Team – email: LPT-SARRequests@leicspart.nhs.uk

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

- Not provided enough information in order for the information to be located
- Not supplied with the appropriate fee
- Not supplied the necessary evidence of identity
Or

- The retrieval of the health records requires disproportionate effort

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 Justice Auld, Mummery and Buxton dated 8 September 2003 (http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx)

- 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 the other individual has not consented to disclosure.

5.4.3 Personal Identifiable Data in Medical Research

In order to ensure the key principles of Data Protection Act are adhered to, the Medical Research Council (MRC) published guidelines on Personal Information in Medical Research (2000). It clearly states that the law assumes that whenever people give personal information to health professionals caring for them, it is confidential as long as it remains personally identifiable. Frequently during medical research personal information is obtained from surveys, medical records, scientific tests and interviews. This information is confidential and any failure to control they ways in which it is used could be potentially harmful to a person’s sense of security and self-confidence, the doctor-patient relationship or lead to unfair discrimination.

Since the Data Protection Act (DPA) 1998 (EU Data Protection Directive 95/46/EC) became law in 2000, researchers must also ensure their work is consistent with the law. However, the law recognises that research which does not directly lead to decisions about a person should have special freedom to use information in ways not foreseen when it was collected but these uses must be fair and lawful.

All research within the Trust must comply with the Data Protection & Caldicott Principles as set out in this policy, be registered by the Research and Development Department.

The Information Governance Lead for the Trust will maintain a database of all the DPA approval requests as evidence for compliance with the DPA 1998 registration and Information Governance Toolkit.
5.5 Privacy Impact Assessment Procedure and Template

All projects and processes that involve personal information or intrusive technologies give rise to potential privacy issues and concerns. To enable the Trust to address the privacy concerns and risks a technique referred to as Privacy Impact Assessment (PIA) must be used. This process ensures that the Trust complies with the Data Protection Act: Principle 1 – “Personal Data should be processed fairly and lawfully” and Principle 2 – “Personal Data shall be processed for a specific purpose”. Refer to the Trust Privacy Impact Assessment Policy and Procedure for more details.

6.0 Requirements for Safe Havens

We hold large amounts of personal confidential data about our service users and staff. **Staff must ensure that they have done everything possible to protect this information**, and comply with the Caldicott and Data Protection principles.

6.1 Communication by post

6.1.1 Internal post

This is considered secure and can be used for personal information as long as multiple letters/documents are contained in sealed and secure envelopes/bags or boxes, so that they cannot simply fall out

Health records or other personal confidential information for transportation between sites/departments must be enclosed in sealed bags/envelopes/boxes and labelled appropriately i.e. ‘Confidential’, and if relevant, marked ‘to be opened by addressee only’. Guidelines for the transporting of health records are available on the intranet, and from the Information Governance Team on IGTeam@leicspart.nhs.uk

6.1.2 External post

Written communications containing sensitive/personal information (e.g. referral letters, appointment letters and test results) should be transferred in a sealed envelope, addressed to the named recipient and clearly marked ‘Private and Confidential’.

Constant care must be taken to ensure only the correct documents are placed inside the envelope. Confidentiality breaches often occur when more than one patient’s correspondence is placed in an envelope.

Always check that address details are correct by confirming them with the destination and always include the post code, even when using the internal mail service.

If appropriate, a designated person should be informed that the information has been sent and arrangements made within their location to ensure that the envelope is received within the expected timescales.
For situations where proof of posting and confirmation of receipt are required, either Recorded Delivery or Special Delivery services must be used.

6.2 Verbal Communication

A considerable amount of information sharing takes place verbally, often on an informal basis, and care should be taken to ensure that confidentiality is maintained in such discussions.

If information is to be shared by phone, then steps need to be taken to ensure that the recipient is properly identified. This can be done by taking the relevant phone number, double checking that it is the correct number for that individual/organisation and then calling the recipient back.

Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard by other staff who do not have a 'need to know'.

Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts etc.

Messages containing personal information should not be left on answer machines unless a password is required to access them. They should also not be stored on communal systems.

6.3 Communication by fax machines

One of the most common breaches of confidentiality occurs when documents that contain personal confidential data are sent by fax machine. Many fax machines are in corridors or open plan offices and are used by several different departments. People come and go collecting faxes but do not always check that all the pages belong to them; this increases the risk of information being seen by unauthorised persons.

To combat this, many NHS organisations have designated fax machines as 'safe haven' machines. These are located in a secure area and are used to receive documents of a private and confidential nature. Staff should:

- Telephone the recipient of the fax to let them know that you are about to send a fax containing personal confidential data
- Ask if they will wait by the fax machine whilst you send the document
- Ask if they will acknowledge the receipt of the fax
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential
- Check the fax number you have dialled and check again that it is correct before sending
- Request a report sheet to confirm that the transmission was received
6.4 Computers and electronic storage devices

Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data.

PCs or laptops should be locked or switched off when you are away from the desk for any length of time.

Information should be held on the organisations’ network servers, not stored on local hard drives.

All personal confidential data sent by email must be sent via the secure email contact list for those on the LHIS network or via NHSmail (nhs.net) to other secure government networks (gsi.gov.uk; gcsx.gov.uk or pnn.police).

In the rare event where a situation arises where it is not possible, a risk assessment should be undertaken in conjunction with the Information Security Manager/Information Governance Team and under advice from the Caldicott Guardian; and the attachment encrypted.

6.4.1 Encrypting personal confidential data on CD’s and DVD’s

Personal confidential data should never be written to CD’s or DVD’s without encryption. A number of organisations have been fined by the Information Commissioner when staff have failed to do this. Further information and guidance on how to secure data for CD’s and DVDs can be sought from the Leicestershire Health Informatics Service through the service desk.

6.5 Whiteboards/Notice Boards

Whiteboards that are placed in areas accessed by the public (wards, treatment rooms etc) should only contain sufficient detail to locate the patient, so as not to disclose patient related confidential information.

7.0 Pseudonymisation

A fundamental principle of the Data Protection Act 1998 is to use the minimum amount of personal information to satisfy a purpose and the strip out information relating to a data subject (individual) that is not necessary for the particular processing being undertaken.

Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. This allows patient linking analysis needed within secondary uses. Pseudonymisation is a core element of Secondary Uses Services (SUS) and should be applied across the Trust.

All business processes within the Trust must be documented. Business processes can include, but not limited to:

- The process of using patient data for primary uses (appointment booking,
management of waiting lists etc)
- The process for using patient data for secondary uses
- The use of Patient Confidential Data (PCD) for a combination of primary and secondary uses.

8.0 De-Identification

Staff only have access to the data that is necessary for the completion of the business activity that they are involved in. By de-identification users are able to make use of patient data for a range of secondary purposes without having to access the identifiable data items. The aim of de-identification is to obscure the identifier data items within the patient records sufficiently that the risk of potential identification of the individual is minimised to acceptable levels, providing effective anonymisation. Although risk identification can not be fully removed this can be minimised with the use of multiple pseudonyms.

De-identification can be achieved by:

- Removing patient identifiers
- The use of the identifier for example; value ranges instead of age
- By using a pseudonym

9.0 Confidentiality Audit Approach

With advances in the electronic management of health and employment information, the requirement to monitor access to such confidential information has become increasingly important.

With the move to using more electronic systems, it is imperative that access is strictly monitored and controlled. The movement of confidential information via these methods poses the threat of information falling into the hands of individuals who do not have a legitimate right of access to it.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented may result in a breach of that confidentiality, therefore contravening the requirements of Caldicott, the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

The SIRO is responsible for ensuring that audits of security and access arrangements within each area are conducted on a regular basis. Audit should focus on:

- Failed attempts to access confidential information
- Repeated attempts to access confidential information
- Access to confidential by unauthorised persons
- Evidence of shared login sessions/passwords
- Staff awareness of Trust policies and guidelines concerning confidentiality and understanding their responsibilities with regard to confidentiality
- Appropriate use of smartcards
• Appropriate allocation of access rights to systems which contain confidential information
• Appropriate staff access to physical areas
• Storage of and access to filed hard copy patient notes and information
• Security of confidential fax handling
• Confidential information sent or received via email, security applied and email system used
• Information removed from the workplace – has authorisation been gained either for long term or short term removal?
• Security applied to laptops and portable devices
• Evidence of secure waste disposal
• Use of whiteboards for confidential information
• Information flows of confidential information
• Appropriate transfer and sharing arrangements are in place
• Security and arrangements for recording access applied to manual files both live and archived e.g. storage in locked cabinets/locked rooms

9.1 Confidentiality audits can be carried out in a number of ways:

• Interviews with staff using structured questionnaires
• Notified audit visits with structured questionnaires
• Spot checks at random work areas
• Audit carried out by the Data Owners on electronic records
• Registration Authority (smartcard usage) enhanced reporting facilities
• As part of an investigation into a potential breach of confidentiality/data loss
• Investigation of reports/Caldicott log
• Monitoring of reported incidents

Confidentiality audit results will be collected on a standard template and recorded for analysis and future reporting. Reporting will be to the Records and Information Governance Group and will highlight any areas for improvement and learning.

If a breach or any risks of breaches of PCD are identified from the audits, matters will be reported and investigated through the Trusts Incident Reporting Policy and Procedure and Disciplinary where appropriate.

The Records and Information Governance Group is tasked with developing an annual confidentiality audit plan, and will identify appropriate staff to undertake the audits.

10.0 Sharing Information with other organisations

Staff sharing personal information with other agencies should be aware of information sharing agreements between LPT and other agencies. Information sharing agreements provide assurance that these agencies are able to comply with safe haven ethos ad meet legislative and related guidance requirements. Further guidance can be found in the Trusts’ Information Sharing Policy.

Information Sharing Agreements are published on the intranet, or alternatively
through contact with the Trusts Information Governance lead who can provide a list.

11.0 Training

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory training. The course directory e-source link below will identify: who the training applies to, delivery method, the update frequency, learning outcomes and a list of available dates to access the training.


A record of the event will be recorded on staff ULearn record

The governance group responsible for monitoring the training is Records and Information Governance Group

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 Information Asset Owners/Administrators (see Information Risk Policy for more details).

All new staff will receive local and organisational induction on Information Governance which will include confidentiality and records management. This will be fully explained by their manager.

All staff will complete the required Information Governance Training using on-line learning modules:

- New Staff – Beginner or Introduction depending the role being undertaken
- Annually – Refresher module.

12.0 Dissemination

Copies of this Policy will be made available to all staff via the Policy Files found on the intranet

All staff will be notified of a new or reviewed Policy via the eSource

This document will be included in the Trust Publication Scheme in compliance with the Freedom of Information Act 2000.

13.0 Monitoring Compliance and Effectiveness

13.1 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.
13.2 Information Governance Toolkit

The Trust is required to complete an annual review of Information Governance compliance by completing the online HSCIC IG Toolkit. The toolkit comprises of the following indicators:

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

The Trust is required to ensure that all permanent staff complete the relevant IG online training module and monthly reports are provided to operational managers to ensure compliance, and this will be monitored through the Divisional Scorecard.

14.0 Links to Standards/Performance Indicators

<table>
<thead>
<tr>
<th>TARGET/STANDARDS</th>
<th>KEY PERFORMANCE INDICATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance Toolkit standard 112 – IG Training</td>
<td>95% of all staff have undertaken IG Training each year</td>
</tr>
</tbody>
</table>

15.0 Review

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced), and the old policy stored in the corporate document management system.

15.1 Archiving

The Trust Secretary is responsible for ensuring that superseded versions of policies and procedures are retained in accordance with the Records Management: NHS Code of Practice 2006

16.0 References and Associated Documentation

- Information Risk Policy
- Information Sharing Policy
- Privacy Impact Assessment Policy and Procedure
- Information Lifecycle and Records Management Policy
Appendix 1

Caldicott Approval Process Flowchart

Information request requiring patient identifiable information, received by the Health Informatics team.

Information request requiring patient identifiable information received by the Information Governance Team

Send Caldicott information request form to applicant

Return to Information Governance Manager for checking

Log on Caldicott Issue Log

Completed form forwarded to Caldicott Guardian with recommendations for consideration

Not Approved

Approved

Form signed and returned to Information Governance Manager who logs decision in the Caldicott log

Information Governance Manager informs the applicant of the decision

Information request/ request for Caldicott approval relating to patient identifiable information received by Caldicott Guardian

Pass to Information Governance Manager to enter into Caldicott Log

Discusses changes with applicant
Caldicott Approval Form

Caldicott Approval Form – for use or release of service user identifiable data
(Please print clearly)

<table>
<thead>
<tr>
<th>Title:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description of proposal:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Indicate which data items have been requested:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forename: □</td>
</tr>
<tr>
<td>Address: □</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of organisation receiving data:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Person responsible for release of data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Person responsible for receipt of data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>For what time period is data transfer required:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start date</td>
</tr>
</tbody>
</table>

Please state regularity e.g. monthly ..............................................................

<table>
<thead>
<tr>
<th>Contact details in relation to this form:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Address:</td>
</tr>
<tr>
<td>Telephone:</td>
</tr>
<tr>
<td>E-mail:</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>How will the data be transferred?</strong></td>
</tr>
<tr>
<td>Paper records</td>
</tr>
<tr>
<td>Computer records</td>
</tr>
<tr>
<td>(Note – patient/user identifiable data must not be transferred via e-mail)</td>
</tr>
<tr>
<td><strong>Who else will have access to the data?</strong></td>
</tr>
<tr>
<td>(If data recipients are not employed by the NHS please state whether NHS honorary contracts are in place. If not – detail confidentiality agreements)</td>
</tr>
<tr>
<td><strong>How will the service users be contacted?</strong></td>
</tr>
<tr>
<td><strong>How will service users consent be obtained?</strong></td>
</tr>
<tr>
<td>If no consent being obtained, please detail the reason why not e.g. exemption under section 60 of the Health and Social Care Act 2001</td>
</tr>
<tr>
<td><strong>Where will the data be stored?</strong></td>
</tr>
<tr>
<td><strong>How will the data be protected?</strong> (Please detail security measures to be taken)</td>
</tr>
<tr>
<td>If the data is on a computer is there access via a network?</td>
</tr>
<tr>
<td><strong>How long will the data be stored?</strong></td>
</tr>
<tr>
<td><strong>At the end of this period, how will the data be disposed of?</strong></td>
</tr>
</tbody>
</table>
Who will be responsible for ensuring that the data is disposed of in a confidential manner?

You must address the 7 Caldicott Principles – please give a brief description under each of the following headings

**Principle 1 – Justify the purpose(s)**
Every proposed use or transfer of service user identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2 – Don’t use service user-identifiable information unless it is absolutely necessary**
Service user-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for service users to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3 – Use the minimum necessary service user-identifiable information**
Where use of service user-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.

**Principle 4 – Access to service user-identifiable information should be on a strictly need-to-know basis**
Only those individuals who need access to service user-identifiable information should have access to it, and they should 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.
**Principle 5 – Everyone with access to service user-identifiable information should be aware of their responsibilities**
Action should be taken to ensure that those handling service user-identifiable information – both clinical and non-clinical staff – are made aware of their responsibilities and obligations to respect service user confidentiality.

**Principle 6 – Understand and comply with the law**
Every use of service user-identifiable information must be lawful. Someone in each organisation handling service user information should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality**
Judgements about the sharing and/or disclosure of personal confidential data should be recorded clearly, to demonstrate the risk based considerations.

**Other supporting information e.g. Ethics approval, correspondence etc**

I confirm that the data will be held and used according to the condition and information given as described within this approval form.

Name…………………………………………….    Title……………………………………
Signature……………………………………………………….   Date……………………..
Please return to:
Information Governance Team
Lakeside House
4 Smith Way
Grove Park
Enderby
LE19 1SX
Or via email to IGTTeam@leicspart.nhs.uk

For Office Use Only
The release and use of data as described above: Approved / Not Approved

Caldicott Guardian/Deputy

Date:
Privacy Notice

Leicestershire Partnership NHS Trust (‘We’ or ‘LPT’) are committed to protecting and respecting your privacy. This notice (and any other documents referred to in it) sets out the basis on which any personal information we collect from you, or that you provide to use, will be processed by us. Please read the following carefully to understand our practices regarding your personal information and how we will deal with it, including:

- What personal confidential data of your is collected
- What organisation is collecting the information
- How the information is used
- What choices are available to you regarding collection, use and distribution of the information
- What kind of security procedures are in place to protect the loss, misuse or alteration of information under our control
- How you can correct any inaccuracies in the information

This notice only applies to how we process personal information. For the purpose of the Data Protection Act 1998 (the Act), the data controller is Leicestershire Partnership NHS Trust (Notification Number Z6769559)

Information we may collect from you

During the course of our activities, we may collect and process the following information about you:

- We will collect, store and process personal information about our patients and staff. All personal and personal health information obtained about patients or staff treated as confidential, along with all corporate information
- Through the provision of our healthcare services, including: inpatient rehabilitation and intermediate care; mental health and learning disability services; community services; and childrens and young persons services.
- Through research, whether market or clinical (we may ask you to complete surveys that we use for research purposes, although you do not have to respond to them)
- Details of current, past and prospective employees
- If you are suppliers, or others that we communicate with
- If you contact us, we may keep a record of that correspondence
- Through CCTV monitoring at our premises

Uses made of the information

We use information held about you in the following ways:

- To allow us to provide health services and to carry out our obligations to you
• Anonymised findings from our research
• For education and training
• To notify you about changes to our services
• To enable us to comply with our obligations under relevant legislation
• If we are under a duty to disclose or share your personal information in order to comply with any legislation or to protect the rights, property, or safety of Leicestershire Partnership NHS Trust, our patients or others
• We will not disclose your details to anybody outside of the NHS without your permission, unless we have a lawful reason to do so, for example where disclosure is necessary for crime prevention or safeguarding purposes. We also undertake to only hold your information for as long as is necessary for providing a service to you.

Access to Information

The Act gives you the right to access information held about you by making a Subject Access Request (as described in the Act). You can do this in writing to the Information Request Team, Suite P1, Bridge Park Plaza, Bridge Park Road, Thuramston, LE4 8BL or for advice by telephone: 0116 2253727 or via email LPT-SARRRequests@leicspart.nhs.uk
Checklist for the Review and Approval of Procedural Document

Checklist to be completed & attached to policy

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed: Data Protection, Caldicott and Confidentiality Policy</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the title clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is it clear whether the document is a guideline, policy, protocol or standard?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2. Key Points / Changes to the Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Rationale</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are reasons for development of the document stated?</td>
<td>Yes</td>
<td>Section 3.0</td>
</tr>
<tr>
<td>4. Development Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the front page include a sentence which summarises the contents of the policy?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is the method described in brief?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are people invited in the development identified?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is there evidence of consultation with stakeholders and users? (with representatives from all relevant protected characteristics)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>5. Content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the objective of the document clear?</td>
<td>Yes</td>
<td>Section 3.0</td>
</tr>
<tr>
<td>Is the target population clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are the relevant CQC outcomes identified?</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Are the intended outcomes described?</td>
<td>Yes</td>
<td>Section 4.0</td>
</tr>
<tr>
<td>Are the statements clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6. Evidence Base</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the type of evidence to support the document identified explicitly?</td>
<td>Yes</td>
<td>Section 5.0</td>
</tr>
<tr>
<td>Are key references cited?</td>
<td>Yes</td>
<td>Section 5.0</td>
</tr>
<tr>
<td>Are the references cited in full?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is there evidence to show that there has been due regard under the Equality Act 2011? (include equality analysis setting out summary of evidence to support public sector equality duty ‘due regard’ has</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>17.0</td>
<td>Are supporting documents referenced?</td>
<td>Yes</td>
</tr>
<tr>
<td>Appendix 6</td>
<td>Is there evidence to show NHS Constitution has been considered</td>
<td>Yes</td>
</tr>
<tr>
<td>7.</td>
<td>Approval</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the document identify which committee/group will approve it?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?</td>
<td>NA</td>
</tr>
<tr>
<td>8.</td>
<td>Dissemination and Implementation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is there an outline/plan to identify how this will be done?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Does the plan include the necessary training/support to ensure compliance?</td>
<td>Yes</td>
</tr>
<tr>
<td>9.</td>
<td>Document Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the document identify where it will be held?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Have archiving arrangements for superseded documents been addressed?</td>
<td>Yes</td>
</tr>
<tr>
<td>10.</td>
<td>Process to Monitor Compliance and Effectiveness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Is there a plan to review or audit compliance with the document?</td>
<td>Yes</td>
</tr>
<tr>
<td>11.</td>
<td>Review Date</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the review date identified?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Is the frequency of review identified? If so it is acceptable?</td>
<td>Yes</td>
</tr>
<tr>
<td>12.</td>
<td>Overall Responsibility for the Document</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Individual Approval**

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sam Kirkland</td>
<td></td>
<td>13 November 2014</td>
</tr>
</tbody>
</table>

**Committee Approval**

If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation’s database of approved documents.

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Policy Training Requirements

The purpose of this template is to provide assurance that any training implications have been considered.

<table>
<thead>
<tr>
<th>Training topic:</th>
<th>Information Governance Training</th>
</tr>
</thead>
</table>
| **Type of training:** | ✓ Mandatory (must be on mandatory training register)  
☐ Role specific  
☐ Personal development |
| **Division(s) to which the training is applicable:** | ✓ Adult Learning Disability Services  
✓ Adult Mental Health Services  
✓ Community Health Services  
✓ Enabling Services  
✓ Families Young People Children  
✓ Hosted Services |
| **Staff groups who require the training:** | All staff groups |
| **Update requirement:** | Annually |
| **Who is responsible for delivery of this training?** | eLearning through Learning and Development |
| **Have resources been identified?** | See Learning and Development Prospectus |
| **Has a training plan been agreed?** | See Learning and Development Prospectus |
| **Where will completion of this training be recorded?** | ✓ Trust learning management system  
☐ Other (please specify) |
| **How is this training going to be monitored?** | Monthly reports to managers |
NHSLA Policy Monitoring Section

NA

Duties outlined in this Policy will be evidenced through monitoring of the other minimum requirements

Where monitoring identifies any shortfall in compliance the group responsible for the Policy (as identified on the policy cover) shall be responsible for developing and monitoring any action plans to ensure future compliance

<table>
<thead>
<tr>
<th>Reference</th>
<th>Minimum Requirements</th>
<th>Self assessment evidence</th>
<th>Process for Monitoring</th>
<th>Responsible Individual / Group</th>
<th>Frequency of monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>Staff adhere to the requirements of the Data Protection Act 1998 and understand their obligations in relation to Caldicott and Confidentiality</td>
<td>Section 9.0 and Section 12.0</td>
<td>Confidentiality audits Information Governance Training compliance</td>
<td>Records &amp; Information Governance Group</td>
<td>As required Bi-Monthly</td>
</tr>
<tr>
<td>NA</td>
<td>Information Asset Owners undertake annual risk assessments of the assets under their responsibility</td>
<td>Section 4.5</td>
<td>Risk assessments provided to the SIRO for assurance</td>
<td>Records &amp; Information Governance Group</td>
<td>Annually</td>
</tr>
<tr>
<td>NA</td>
<td>Privacy Impact Assessments are undertaken where services redesigned/changes in processing/introduction of new technologies</td>
<td>Section 5.5 Privacy Impact Assessment Policy &amp; Procedure</td>
<td>PIA’s reviewed by IG Lead, SIRO and Caldicott Guardian</td>
<td>Records &amp; Information Governance Group</td>
<td>As required</td>
</tr>
</tbody>
</table>