Northern Lincolnshire and Goole Hospitals NHS
NHS Foundation Trust

Directorate of Clinical and Quality Assurance & Trust Secretary

DATA PROTECTION AND PERSONAL INFORMATION FAIR PROCESSING POLICY

Reference:	CQP013
Version:	1.1
This version issued:	07/03/13
Result of last review:	Minor changes
Date approved by owner (if applicable):	01/03/13
Date approved:	17/03/11
Approving body:	Trust Governance Committee
Date for review:	March, 2016
Owner:	Director of Clinical and Quality Assurance & Trust Secretary
Document type:	Policy
Number of pages:	16 (including front sheet)
Author / Contact:	Jill Mill, Head of Risk Management

Northern Lincolnshire and Goole Hospitals NHS Foundation Trust actively seeks to promote equality of opportunity. The Trust seeks to ensure that no employee, service user, or member of the public is unlawfully discriminated against for any reason, including the "protected characteristics" as defined in the Equality Act 2010. These principles will be expected to be upheld by all who act on behalf of the Trust, with respect to all aspects of Equality.

Contents

1.0 Introduction

Under the Data Protection Act 1998 the Trust is a registered controller of **all** types of Personal/Health data/records and must, by law, comply with the annual registration requirements of the 1998 Act. The Trust is also obligated to ensure patients are informed of the kind of purposes for which information about them is collected and the categories of people or organisations to which information may need to be passed.

2.0 Purpose

The purpose of this policy is to provide the employees of Northern Lincolnshire and Goole NHS Foundation trust, with a framework through which all personal identifiable data is acquired, stored, processed and transferred in accordance with the Data Protection Act 1998, the Caldicott Principles and the Confidentiality NHS Code of Practice. The Trust has a duty to ensure that patients are informed about the management and control of their personal data.

3.0 Area

This policy is applicable to all Trust staff, including non-executives, students on placement, volunteers and temporary staff.

4.0 Duties

4.1 The Chief Executive

The Chief Executive is accountable for the confidentiality of personal information within the Trust and ensuring that appropriate management arrangements are in place.

4.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is responsible for risk at board level and has responsibility for the Information Governance Agenda in the Trust. The SIRO ensures risk is properly identified, managed and that appropriate assurance mechanisms exist.

4.3 Trust Caldicott Guardian

The Director of Clinical and Quality Assurance & Trust Secretary is the designated Caldicott Guardian with responsibility for providing the organisation with advice on agreeing and policies governing the confidential management and movement of identifiable information and images within and beyond the Trust. The Caldicott Guardian is the Trust lead for the Confidentiality and Data Protection Assurance and signs off the agenda annually.

4.4 Directorate/Department Managers

All managers have a responsibility to understand the policy and the legislations it supports; to establish appropriate procedures to control and manage information accordingly, and ensure that these procedures are followed.

4.5 All Staff

All staff are responsible for compliance with this policy and have a duty maintain their knowledge.

5.0 Actions

5.1 Notification Requirement of the Data Protection Act 1998

5.1.1 The Trust is required to provide the following details to the Information Commissioner's Office on an annual basis:

- Name and address of the Trust
- Name of nominated representative
- A description of Personal data being processed, and the categories of data subject to which they relate
- A description of the purposes for which the data are being/are to be processed
- The source(s) from which the Trust intended to obtain the information
- The names of countries outside the Economic European Area (EEA) to which the Trust intends or may wish to transfer personal data

5.1.2 It is a criminal offence for any Trust employee to knowingly or recklessly operate outside the descriptions contained in the Trusts notification entry.

5.1.3 The Trust registration documents will be held by the Head of Governance on behalf of the Trust.

5.2 Employee & Third party Compliance to the Data Protection Act

5.2.1 The Data Protection Act 1998 has eight principles. The principles apply to **all** personal data (manual/electronic) processed by the Trust.

5.2.2 All employees must, without exception, comply with the eight principles as defined within the Data Protection Act 1998:

- Personal data shall be obtained and processed fairly and lawfully. Personal data shall not be processed unless:
  - At least one of the conditions in schedule 2 is met and
  - In the case of sensitive personal data, at least one of the conditions in schedule 3 is also met
- Personal data shall only be obtained for **specified** and **lawful** purposes. Any further processing of data will only be in accordance with the Trust's registration with the Information Commissioner's Office in a compatible manner

- Where personal data is held it will be adequate, relevant and not excessive in relation to the purpose for which it is held
- Personal data will be accurate and , where necessary , kept up to date
- Personal data will be held no longer than is necessary for the purposes for which it is kept
- Personal data will only be processed in accordance with the rights of the data subjects
- Personal data will be surrounded by proper security
- Personal data will be only transferred outside the European Economic Area if there is adequate protection

5.2.3 Where third party employees have legitimate and contractually agreed access the Trust's information systems compliance is, without exception, the same as that is demanded of Trust employees.

5.2.4 In the event of confidence being breached by a Third Party contractor, the penalty will be termination of contract, and this will be specified.

5.3 Legitimacy of Processing Conditions (Schedule 2 & 3) & Employee Access

5.3.1 The Trust will only process Personal data where at least one of the following conditions (as defined in schedule 2) has been met:

- The processing has the consent of the data subjects
- The processing is necessary for the performance of a contact to which the data subject is a party
- The processing is necessary to ensure compliance with any legal obligation to which the Trust is subject, other that an obligation imposed by contract
- The processing is necessary to protect the vital interest of the data subject. Reliance on this condition may only be claimed when processing is necessary for matters of life and death
- The processing is necessary to carry out public functions:
  - Administration of justice
  - Exercise of functions contravened by or under any enactment
  - Exercise of functions of the Crown
- The processing is necessary to pursue legitimate interests of the controller unless prejudicial to the interest of the data subject
- The delivery of personal care or treatment
- Clinical Governance and the improvement of quality health

- The monitoring and protection of Public Health
- The co-ordination of the NHS with other agencies
- The effective administration of healthcare
- Teaching
- Statistical analysis and research

5.3.2 Where the disclosure of information is to support the business needs identified above, the inclusion of person identifiable information will only be permitted where it can be justified and is considered absolutely essential.

5.3.3 Wherever the use of person identifiable information is justified, the minimum necessary will be permitted on a need to know basis.

5.3.4 In order to process |personal data lawfully, the Trust will regard compliance with condition 6 above as having been routinely met.

5.3.5 In the case of **sensitive** personal data (as defined in schedule 3), the Trust will only undertake processing where at least one of the conditions in have been met and further compliance with at least one of the following criteria is also met:

- Explicit consent has to be given by the data subject
- To ensure compliance with the Trust's legal duty in connection with employment
- To protect the vital interest (matters of life and death) of the data subject or another person in cases where:
  - Consent cannot be given by or on behalf of the data subject
  - The Trust cannot reasonably be expected to obtain consent
  - The vital interest of another person requiring protection and consent by or on behalf of the data subject is being reasonably withheld
- The processing conforms with special rules relating to social, political and religious organisations or trade unions:
  - Processing is not conducted for profit
  - Ensures appropriate safeguards for the rights and freedoms of the data subjects
  - Relates only to individuals who are members of the body or association of having regular contact
  - Does not involve disclosure to the third party without consent of the data subject
- The information has been made public by the data subject

- The processing is **necessary** to support legal proceedings:
  - Obtaining legal advice
  - Defending legal rights
  - Administration of justice
  - Exercise of functions contravened by or under any enactment
  - Exercise of functions of the Crown
- 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 health care services), and is undertaken by a health professional or someone under a similar duty of confidentiality (i.e. equivalent to that which would arise if that person was a health professional)
- The processing is required to identify and review equal opportunity and equal access to treatment monitoring and is carried out with appropriate safeguards for the rights and freedom of the data subjects
- The processing is specified by order of the Secretary of State

5.3.6 Sensitive personal data is defined as:

- Racial
- Ethnic
- Political
- Religious
- Trade Union
- Health
- Sexual
- Offence

5.3.7 In order to process sensitive data lawfully, the Trust will regard compliance with condition 7 as having been routinely met.

5.3.8 To comply with additional statutory restrictions, the following sensitive information will not be passed on in an identifiable format:

- HIV/AIDS
- Other sexual transmitted disease
- Assisted conception
- Termination of pregnancy

5.3.9 In the event of a patient wishing their information to be with held from someone who might otherwise have received it in connection with his or her care, the patient will be advised of the implications but the request will be respected unless there are over-riding considerations to the contrary.

5.3.10 Any decision made for not passing on information will be formally recorded in the patients' records.

5.3.11 The Trust will not process any personal data for the purposes of direct marketing or fund raising.

5.3.12 Decision making by the Trust and/or its employees which significantly affects an individual/data subject will not be based solely on the automatic processing of personal data.

5.4 Reasons for Collecting Patient Identifiable Information

5.4.1 The main reasons for which the Trust collects information about a patient are:

- Providing healthcare and treatment
- To assess the needs of the general population
- Managing and planning services:
  - Making sure that our services meet patients needs in the future
  - Auditing accounts
  - Preparing statistics on NHS performance activity
  - Investigating complaints or legal claims
- Helping staff to review the care they provide to make sure it is of the highest standard
- Training and educating staff
- Conducting health research and development

5.5 The Type of Information Held

5.5.1 Patient identifiable information may be held in manual or electronic format. The information may include:

- Basic demographic details
- Contacts such as clinic visit and admissions
- Notes and reports about health and treatment/care provided
- Results of investigations, such as X-rays and laboratory tests
- Any other relevant information from healthcare professionals

5.6 Disclosure of Patient Identifiable Information

5.6.1 Patients will be advised that the Trust will only disclose information that can be justified in line with Caldicott principles.

5.6.2 Disclosure will always contain the minimum level of identifiable information needed to meet the purpose. The process of transfer will conform to information sharing protocols as agreed by the Caldicott Guardian.

5.6.3 Patient identifiable information will never be transmitted across the internet without adequate security.

5.6.4 The decision to pass on information will usually be taken by the healthcare professional responsible for the patients care.

5.6.5 Disclosure of information will normally be:

- With the patients consent
- On a need to know basis
- In line with statute or a court order
- Actioned if justified for public protection purposes

5.6.6 In the event of a patient wishing to withhold information from someone who might have received it in connection with his/her care the patient will be advised of the implications, but the request will be respected unless there are overriding considerations to the contrary.

5.6.7 The reasons for not passing on information will be recorded in the patient's records.

5.7 Disclosure of Information Outside of the European Economic Area (EEA)

5.7.1 Personal data, even if it would otherwise constitute as fair processing, must not, unless certain exemptions apply or protective measures take, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

5.7.2 In the event that any member of staff wishes to process personal information outside of the United Kingdom, the Caldicott Guardian must be consulted prior to any agreement to transfer or process information.

5.8 Subject Access

5.8.1 The Trust will endeavour to ensure that where personal data is being processed by, or on behalf of the Trust individuals will be given:

- A description of the data
- Purposes the data is being used for
- The recipients to whom the data will be disclosed

5.8.2 Subject access will be managed in line with the rights given to each individual by the Data Protection Act 1998. The Trust will ensure:

- All requests for subject access will be accepted in writing (which includes transmission by electronic means) only
- All requests will be responded to within 40 days from receipt of a valid request or, if later, within 40 days of receipt of:
  - Information confirming identity/legitimacy of individual making the request/assisting in the location of relevant data;
  - The fee
- All requests for subject access will incur a fixed fee up to the maximum permitted within the Act.
- A request will not be met in the absence of:
  - Written request
  - The fee;
  - Information confirming identity of the individual/assisting the location of data (where necessary)
- All requests for subject access will receive a reply even when no data is held about the individual concerned
- Where personal data has been requested, and its release is not covered by exemptions under the Act a copy of the data held will be supplied to the requester
- In the event of information in the copy being unintelligible a reasonable explanation will be given to the requester by an appropriate Trust employee
- The information given in response to a subject access request will be all that which is contained in the Personal data at the time the request was received

- Where a subject access request has been met previously, additional requests for similar or identical access by the same person will only be met following a reasonable time elapse. In deciding a reasonable time lapse the following factors will be considered:
  - The nature of the data
  - The purpose for which the data are processed
  - Frequency with which the data are altered
- Where a subject access request would result in the disclosure of information relating to an individual other than the data subject the Trust will only comply with the request there:
  - The other individual has consented to disclosure of the information
  - It is reasonable in all the circumstances to comply with the request without the consent of the other individual. In deciding reasonableness the Trust will give regard to:
    - Any duty of confidentiality owed to the other individual
    - Steps taken to seek consent of the other individual
    - Capability of the other individual to give consent
    - Refusal of consent by the other individual
- When requests are made by or on behalf of children, the Trust will at all times work within the law relating to the legal capacity of children (i.e. the request must be in the interests of the child and not just the parents)

5.9 Non-Disclosure and Subject Access Exemptions

5.9.1 Within the Act there is recognition that the public interest requires disclosure of personal data that would otherwise be in breach of the Act.

5.9.2 Where an exemption from the non-disclosure provision **properly** applies, such disclosure would not be in breach of the Act.

5.9.3 Non-disclosure and subject access exemptions will apply in the following circumstances:

- Where failure to disclose Personal data would be likely to prejudice:
  - National Security
  - The prevention or detection of crime
  - The apprehension or prosecution of offenders;
  - The assessment or collection of any tax or duty;

  - The maintenance of professional standards by professional bodies or the ability of the Health Service commissioned to discharge their function

- Where giving subject access would be likely to cause serious harm to the physical or mental health of the data subject

- Where the Trust has reasonably decided that giving subject access would be likely to lead the data subject to identify another person who has not consented to the disclosure of his or her identity

- Where data is held for the purpose of replacing other data in the event of loss, destruction of impairment

- Where personal data is held **only** for preparing statistics, carrying out research or historical purposes, results will not be made available in a form that identifies data subjects

- Where the disclosure if personal data is required under enactment, law or Court Order

- Where the disclosure of Personal data is necessary for:

  - Legal proceedings

  - Obtaining legal advice

  - Establishing, exercising or defending legal rights

5.9.4 Decisions invoking exemption clauses, or permitting access to patient identifiable information on an exceptional basis where it is usually denied, will only be made by the Trust Caldicott Guardian or nominated individual.

5.9.5 The Trust will maintain a log listing the circumstances where exemption clauses or exceptional approval have been invoked / permitted.

6.0 Complaints, Compensation and Enforcement

6.1 Wherever practical the Trust will take steps to share Personal data held with individual data subjects to maintain a high level of data accuracy.

6.2 In the event of an individual successfully applying for a court order to rectify, block, erase or destroy data that are inaccurate, the Trust will action the change immediately.

6.3 In the event of an individual suffering damage and/or distress because of any contravention of the Act by the Trust, the entitlement to compensation as determined by the Courts is recognised.

6.4 Where it is clear an individual employee has failed to comply with the principles detailed in section 11.0 or operated outside the descriptions contained in the Trust's notification entry. Disciplinary action including the possibility of dismissal from the Trust's employment will be evoked.

6.5 Where data processing is undertaken by a data processor, the Trust will have in place a written contract containing specific instructions and agreed security measures. All reasonable steps to ensure compliance will be taken.

6.6 In the event of non-compliance compliant or request for assessment being lodged against the Trust, the Trust will work with the Information Commissioner to reach a satisfactory resolution.

6.7 In the event of the Information Commissioner serving one the following notices:

- An enforcement notice
- A de-registration notice
- A transfer prohibition notice

6.7.1 The Trust will, if appropriate, lodge an appeal to the independent Data Protection tribunal.

7.0 Partner Organisations

7.1 The principal partner organisations with whom patient identifiable information may be shared:

- NHS Trusts
- Primary Care (PCT's and GP's)
- Ambulance Service
- Booking Management Service
- Private Sector Providers
- Strategic Health Authorities

7.2 Information may also be shared / stored subject to a Information Sharing Agreement with:

- Social Services
- Education Services
- Law enforcement agencies
- Voluntary sector providers
- Information system suppliers

8.0 Monitoring Compliance and Effectiveness

8.1 The Information Governance Steering Group has the responsibility for overseeing the implementation and compliance monitoring of this policy.

8.2 The group will receive quarterly incident analysis reports and escalate any concerns appropriately through the management structure and implement any necessary actions to ensure compliance.

8.3 The group will receive quarterly reports on the implementation of the Trust Confidentiality & Data Protection agenda. Monitoring progress of the Confidentiality agenda in year with the Information Governance Toolkit and any other confidentiality or data protection initiatives undertaken within the organisation.

8.4 In the event of a potential or actual breach of patient confidentiality, the reporting and escalation processes are in line with the Risk Management Strategy, Incident Reporting Policy/Procedure, and the Policy for Dealing with Serious Untoward Incidents.

9.0 Associated Documents

9.1 Confidentiality Policy.

9.2 Information Security Policy.

9.3 Risk Management Strategy.

9.4 Incident Reporting Policy/Procedure.

9.5 Policy for Dealing with Serious Untoward Incidents (Clinical & Non Clinical).

9.6 Subject Access to Health Records Policy.

9.7 Safe Haven Policy.

10.0 References

10.1 The Confidentiality NHS Code of Practice.

10.2 The Caldicott Report 1997.

10.3 Information Governance Toolkit.

11.0 Definitions

11.1 The definition of a health record means any record which:

- Consists of information relating to the physical or mental health or condition of an individual and
- Has been made by or on behalf of a health professional in connection with the care of that individual

11.2 The Act gives the right to individuals in respect of personal data held about them by others. The rights are:

- Right of Subject Access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Right in relation to automated decision making
- Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

11.3 The Trust must have in place an active fair processing framework through which patients are informed about the kind of purposes for which information, including images about them is collected, and the categories of people or organisations to which such personal information may be passed.

11.4 Such a framework will indicate whether disclosures of data are mandatory or optional and will attempt to distinguish data, which is 'essential' in order to treat patients within the health service.

11.5 Such a framework will ensure that the individual's consent is informed.

12.0 Dissemination

12.1 This policy will be available on the intranet.

13.0 Training

13.1 Information Governance training will be included in the Corporate Induction and is a part of the Trust's mandatory training programme.

The electronic master copy of this document is held by Document Control, Directorate of Clinical and Quality Assurance & Trust Secretary, NL&G NHS Foundation Trust.

Appendix A

Information Governance Roles and Responsibilities

Caldicott Guardian	**Director of Clinical and Quality Assurance and Trust Secretary**	The **Caldicott Guardian** is responsible for providing the organisation with advice on policies governing the confidential management and movement of identifiable information and images within and beyond the Trust.
Senior Information Risk Officer (SIRO)	**Director of Finance, Planning and Performance**	The **SIRO** is responsible for risk at board level and has responsibility for the Information Governance Agenda in the Trust. The SIRO ensures risk is properly identified, managed and that appropriate assurance mechanisms exist.
Information Governance Lead	**Director of Clinical and Quality Assurance and Trust Secretary**	The **IG Lead** is responsible for ensuring that data security is managed effectively in compliance with the appropriate regulatory framework.
Information Lifecycle Management Lead	**Director of Clinical and Quality Assurance and Trust secretary**	The **Information Lifecycle Management Lead** ensures the guidelines that apply to information on paper or other forms including electronic, microfilm, audio and video are adhered to.
Information Security Officer	**Deputy Director of Information and Information Technology**	The role of **Information Security Officer** is to ensure IT security complies with the standards set out in the Information Governance Framework
Data Protection Officer	**Deputy Director of Clinical and Quality Assurance and Ass Trust secretary**	The **Data Protection Officer** is responsible for ensuring all data is processed in accordance with the Data Protection Act 1998 providing advice on how the information, whether the information is disclosed and the ways in which we protect users' privacy.
Chair – IG Steering Group	**Director of Clinical and Quality Assurance and Trust Secretary**	**The IG Steering Group** will oversee implementation of the Information Governance Strategy, the application of the Information Governance (IG) Policy and the implementation of the action plan.
Freedom of Information (FOI) Lead	**Director of Clinical and Quality Assurance and Trust Secretary**	The **FOI Lead** ensures arrangements are in place to respond to requests received under FOI Act, within agreed timescales. Provides advice and guidance on the application of FOI principles
Information Governance (Operational Lead)	**Head of Risk Management**	The **IG Operational lead** ensures effective implementation of the IG strategy and Policy on a day to day basis and provides advice and guidance on implementation
Data Protection (Operational Lead)	**Head of Risk Management**	The **Data Protection Operational Lead** ensures effective implementation of the IG strategy and Policy on a day to day basis and provides advice and guidance on implementation