East London
NHS Foundation Trust

Data Protection and Confidentiality Policy

Version number :	1.1
Consultation Groups	Quality Committee
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	September 2019
Name of originator/author:	Data Protection Officer
Executive Director lead :	Executive Director of Planning and Performance
Implementation Date :	September 2018
Last Review Date	July 2019
Next Review date:	July 2022

Services	Applicable
Trustwide	√

Version Control Summary

Version	Date	Author	Status	Comment
1.0	03.12.18	Information Rights Manager	Final	New policy providing guidance on data protection and confidentiality.
1.1	18.07.2019	DPO	Final	Updated to include committee structure, Information Asset Owner responsibilities, DPO requirement

Contents

Executive Summary

Data is essential to East London NHS Foundation Trust; it enables effective treatment, supports research and allows the Trust to better plan its resources. Personal data belonging to current, past and prospective service users, current, past and prospective employees, suppliers, contractors, business partners is one of our most valuable assets in providing services.

The Data Protection Act (2018) and the General Data Protection Regulation sets the legal framework by which the Trust can process personal information. It applies to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A).

This policy provides a guide to the key elements of the legal framework governing information handling, outlines the responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling.

Data Protection and Confidentiality Policy - Data Protection Principles

The Data Protection Act (2018) defines six Data Protection Principles; which all processors of personal information must abide by. The six principles are:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed 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 or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

1 Introduction, Scope and Purpose of this Policy

1.1 Introduction

1.1.1 The NHS cannot operate effectively if the patients we need to treat do not trust us to provide confidential and effective care. Part of this trust is being able to provide confidential information to clinicians and other staff and be confident that if will remain confidential and only be shared when necessary.

1.1.2 This document provides guidance for everyone on processing information in accordance with the principles and legal obligations outlined in the Data Protection Act (2018), General Data Protection Regulation and common law duty of confidentiality. It explains how we can comply with best practice for information handling within the NHS as described in the NHS Code of Confidentiality, Data Security and Protection Toolkit and the Caldicott Reports.
.

1.2 Scope

1.2.1 This policy provides guidance to ensure that information processed by Trust staff is handled in a safe and secure manner which complies with current legislation and best practice relating to data protection and confidentiality.

1.2.2 It will apply to all areas of the Trust and all staff who handle information. It will be of particular relevance to staff members who handle personal and sensitive information relating to both patients and staff.

1.2.3 Data Protection and Confidentiality is a component of Information Governance and as such this policy and associated procedures form part of the Trust's overall Information Governance Framework.

1.3 Purpose

1.3.1 The objectives of this policy are:

- To demonstrate the ways in which we ensure that patient and staff data is handled effectively and securely
- To promote best practice and innovative use of personal information, especially to inform care and research
- To ensure that we understand our responsibilities and obligations.

1.4 Definitions

Term	Definition
Personal data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
Data controller:	The person (or company) who determines the purposes for which, and the manner in which any personal data are, or are to be, recorded. In our case, the Data Controller is the Trust
Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person who processes data on behalf of the data controller.
Direct care	The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider. Examples include assessment, performing procedures and implementation of a care plan.
Duty of confidence	A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.
Explicit consent	A form of consent normally given orally or in writing and is where a patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.
Information governance	Information governance is a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.

Legitimate relationship	A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.
Processing	This term covers the collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to alteration, retrieval, disclosure and destruction or disposal of the data.
Non care or secondary purpose	Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

2 Related Trust Policies

- Health Records Policy
- Non Health Records Policy
- Disciplinary Policy
- Clinical Data Quality Policy
- Audio Visual Recording Policy
- Clinical Coding Policy
- Freedom of Information Policy
- Incident Policy
- Access to Health Records Policy
- Third Party Access Policy
- Registration Authority Policy
- Network, Internet and Email Usage Policy
- Information Governance & IMT Security Policy

3 Roles and Responsibilities

3.1 Management Responsibilities

3.1.1 The **Chief Executive is the Trust's Accountable Officer** and responsible for overall leadership and management of the Trust with the ultimate responsibility for ensuring compliance with the Data Protection Act (2018), the General Data Protection Regulation, Human Rights Act (1998) and the Common Law Duty of Confidentiality. The Chief Executive delegates aspects of her responsibility to relevant executive directors according to their organisation portfolios.

3.1.2 The **Chief Finance Officer** is the **Senior Information Risk Officer (SIRO).**

3.1.3 **The Associate Director of Information Governance** is the **Data Protection Officer** and responsible for managing data protection issues throughout the Trust. A Data Protection Officer is a legal requirement under Article 37 of the General Data Protection Regulation. The Data Protection Officer monitors internal compliance with data protection matters, provides advice and information on data protection obligations, acts as a contact point for data subjects and the Information Commissioner's Office. The Data Protection Officer is independent and has direct communication with the Board.

3.1.4 **The Director of Corporate Affairs** has executive responsibility for information governance including chairing the **Information Governance Steering Group,**

where data protection issues are discussed and escalated to relevant groups and committees when necessary.

3.1.5 Day to day responsibility for data protection and confidentiality management is the responsibility of the **Information Governance Manager**.

3.1.6 The **Chief Medical Officer** is the **Caldicott Guardian** with specific responsibility for the confidentiality agenda and the collection, use and sharing of patient information.

3.1.7 **Service Directors / Associate Directors** are Information Asset Owners, supported by **Team Managers** who are Information Asset Administrators.

3.1.7 All **Managers** are responsible for the local implementation of this policy in their areas of responsibility.

3.2 Individual Responsibilities

3.2.1 Everyone working for the NHS has a legal duty to keep information about service users and other individuals such as staff or volunteers confidential. Staff are required to adhere to confidentiality agreements, e.g., common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

3.2.2 The terms and conditions within Trust employment contracts include specific conditions relating to confidentiality which must be adhered to.

3.2.3 All members of staff are responsible for ensuring they keep up to date with Information Governance/Data Security training in accordance with the Trust Statutory and Mandatory training needs analysis as this training covers relevant data security requirements.

3.2.4 This requirement also applies to agency staff, contractors and volunteers working at the Trust who may have access to personal information. Most agencies working with the NHS provide their staff with this training. Where this is not the case, local arrangements should be made to ensure the employee is adequately trained before working at the Trust.

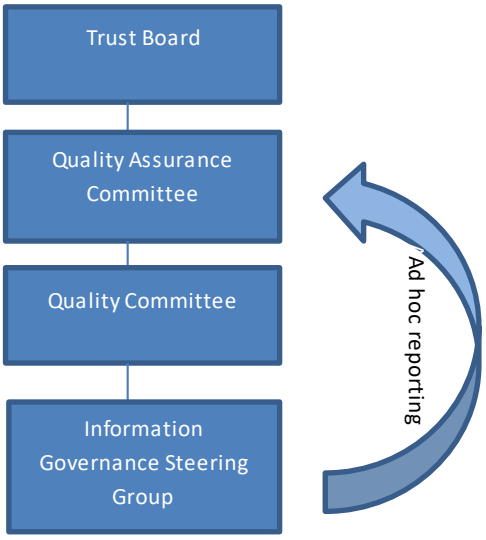
4. Reporting structures

4.1 The Information Governance Steering Group oversees the information governance agenda and is responsible for holding the information governance function to account.

4.2 The Information Governance Steering Group is a sub committee of Quality Committee. Quality Committee receives bi annual update reports on information governance matters plus any exception reporting. It ratifies policies approved at Information Governance Steering Group.

4.3 The Quality Assurance Committee is a Board sub committee. Quality Committee reports to the Quality Assurance Committee. The two bi annual reports tabled at Quality Committee are then tabled at Quality Assurance Committee. Ad hoc information governance reports including the annual SIRO report are regularly tabled at Quality Assurance Committee.

4.4 The Board receives a summary of information governance reports tabled at Quality Assurance Committee.



5 Principles and Procedures

5.1 Data Protection Act 2018 and GDPR

5.1.1 The Data Protection Act (2018) (DPA) and the General Data Protection Regulation (GDPR) sets out the legal requirements and duties placed on data controllers (i.e. the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about).

5.1.2 The Trust is required to register annually with the Information Commissioner as a Data Controller. The Trust's unique registration number is **Z5601596.**

5.1.3 The DPA sets out six data protection principles which describe legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the six data protection principles is unlawful.

5.1.4 The Data Protection Act (2018) does not apply to deceased persons. The Access to Health Records Act 1990 governs the access to health records of deceased patients. The NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought from the Information Governance Team: elft.information.governance@nhs.net

5.1.5 Under GDPR each controller of personal information must decide under what basis it is processing personal information. If there is no relevant basis, then the processing is likely to be illegal.

- Under Article 6, the Trust's basis for processing personal information is: "the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law".

- As the Trust processes special category information – which includes health data then it must have a second basis (under Article 9), which are:
    - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of

health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5.2 NHS Caldicott Report

5.2.1 The Caldicott Report was published in 1997 (updated in 2013 and 2016) and focused on the protection and processing of patient identifiable information within the NHS. The reports provided the NHS with a series of principals to adhere to:

- Justify the purpose for collecting or holding patient-identifiable information
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

5.2.2 The Caldicott Guardian advises the Trust Board on matters of patient confidentiality and promotes the safe and secure handling of patient data. The Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures, where there are ethical considerations.

5.3 Data Processing

5.3.1 Data processing covers the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintaining confidence between the Trust and its patients, staff and others with whom we deal.

5.3.2 The DPA requires that processing of any personal information held by the Trust must be both fair and lawful. This requires that the processing meets fair processing criteria and satisfies one or more 'conditions for processing' set out in the DPA.

5.3.3 To ensure 'fair processing' we must be lawful, fair and transparent about the way we will use the personal data we hold. We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- help people to understand their rights

5.3.4 To meet this requirement the Trust publishes a fair processing notice to inform individuals about the way we handle and use their personal data. This is published on the Trust public website.

5.3.5 Routine data processing for the purposes of patient care will normally be conducted for a purpose that satisfies one of the processing conditions in the DPA. When sharing takes place for non-care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

5.3.6 A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information.

5.4 Access to IT Systems

5.4.1 It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

5.4.2 The Information Governance & IMT Security Policy provides detailed guidance on the security of Trust IT systems including minimum standards of access controls.

5.4.3 Individuals should not attempt to access or use electronic record systems they have not been trained to use or authorised to access. Existing system users should not allow others to access systems using their login credentials. Action may be taken against individuals who share passwords and Smartcards.

5.5 Access to Records

5.5.1 The Trust holds individual service user records in a variety of formats. In addition it holds personal records for present and former members of staff and others it does business with. While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

5.5.2 Many of our digital clinical systems will allow a user to access any individual record held in that system. Users should only access records for those data subjects (patients, staff etc) that they have authorisation to access for specific purposes or in the case of health records where they have a 'legitimate relationship' with the service user.

5.5.3 Staff have no right to access personal information held in records about their relatives or friends unless the circumstances in paragraph 4.5.2 apply.

5.5.4 While some Trust staff are in a position to potentially access personal data held about them in Trust records (e.g. their personal medical records) this is not a facility available to members of the public. NHS policy is that NHS staff should follow the same procedure as members of the public to access their data. Therefore **Trust staff should not access their own data held in any Trust records without specific authorisation**, they should make a subject access request.

5.5.5 Procedures for obtaining access to or copies of health records held by the Trust about individuals are explained in the Access to Health Records Policy.

5.5.6 The Trust carries out audits of access to personal data and any individual who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' record data may face action.

5.6 Communicating Personal Information

5.6.1 To provide effective care services there is a need to transfer information between organisations and individuals. To comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

.

5.6.2 Any electronic data containing identifiable information transferred outside the Trust for processing must be securely encrypted during transit. Any transfer outside the European Economic Area must only be carried out if appropriate security controls are in place.

5.6.3 A guide on the transfer or communication of personal data by post, fax, by hand and e-mail and the use of portable media is available on the intranet**.**

5.7 Disclosure and Sharing of Personal Information

Sharing Personal Information for Care Purposes

5.7.1 To provide safe and effective care, personal information about service users will need to be shared with all those caring for an individual. In addition to the clinical team providing care, the direct care team may include laboratory staff, social care staff, specialist care teams and administrative staff supporting the care process.

5.7.2 In accordance with both DPA 2018, GDPR and Caldicott principles information shared for care purposes should be relevant, necessary and proportionate.
In applying this principle care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

5.7.3 Caldicott principle 7 (Duty to share) emphasizes the need to share information in certain circumstances where the duty to share information clearly outweighs the normal duty of confidentiality owed. This would be the case when there is a threat to the safety of others and the sharing of personal information about individuals (e.g. vulnerable adults or children) with the police or other agencies may prevent that threat materialising.

Sharing Personal Information for Non Care Purposes

5.7.4 Non care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using anonymised or de-identified data. This removes the need to consider consent issues.

5.7.5 In certain circumstances the law requires that confidential information should be disclosed when consent may not be provided. Examples of this include a direction within a court order to disclose confidential information or the requirement to notify Public Health officials when a patient is suspected of suffering from a notifiable disease.

5.7.6 Where a legal obligation to disclose does not exist there are some limited circumstances where the sharing of personal information without consent may be justified in the 'Public Interest'. Disclosures made without consent to support the detection, investigation and punishment of serious crime and to prevent abuse or serious harm to others are examples of such circumstances. Such disclosures are considered on a case by case basis and can be complex. The public good that would be met by sharing the information has to be weighed against the obligation of confidentiality owed to an individual and the public good in maintaining trust in a confidential service.

5.7.7 Further guidance on specific aspects of information sharing and disclosure is given in **Appendix A**. This guidance covers disclosures to the police, disclosure to relatives and carers, and access to information about service users for the purposes of clinical audit, service improvement and research purposes.

5.8 Disposal of Personal Information

5.8.1 It is a principle of the DPA that data should 'not be kept for longer than necessary'. To assist staff in meeting this requirement the Trust adopts the retention schedule contained in the NHS Records Management Code of Practice.

5.8.2 All printouts, reports and printed copies of records containing personal data should be kept secure at all times. This particularly applies to handover reports and documents used by staff working in ward areas.

5.8.3 Any documents containing personal data should be disposed of securely and not discarded in domestic waste and recycling bins. The Trust operates a confidential waste disposal service and provide regular collections of confidential waste from all Trust areas.

5.8.4 The disposal of items of electronic equipment which may hold personal data (PCs, laptops and any other devices with information storage capabilities) should be carried out through the ICT department to ensure all data is effectively removed before disposal.

5.8.5 The disposal of medical devices and equipment should follow the guidance on Decommissioning and Disposal provided in the Medical Devices Policy.

5.9 Breach of Policy and Procedure

5.9.1 Any breach of data protection and confidentiality can have severe implications for the Trust, our service users and staff and, where significant numbers of service users are involved, can impact on the reputation of the NHS as a whole.

5.9.2 Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 may constitute a serious disciplinary offence or gross misconduct under the Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

5.9.3 The Information Commissioner's Office (ICO) regulates data protection and is charged with upholding individual's information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of a financial penalty of up to 20,000,000 Euros.

5.9.4 Staff who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Trust Incident Reporting Policy.

6 Implementation

6.1 This policy will be published on the Trust's intranet and the publication of this version will be highlighted in the information governance pages on the intranet. Annual IG training must be completed by all staff in accordance with the Trust training needs analysis for all staff groups and reference to the existence of this policy is made during face to face IG training sessions.

6.2 The Trust information leaflet for service users (Your Records and You) contains key

information published in this policy.

7 Monitoring Compliance and Effectiveness

7.1 The purpose of monitoring is to provide assurance that the agreed approach is being followed – this ensures we get things right for patients, use resources well and protect our reputation. Our monitoring will therefore be proportionate, achievable and deal with specifics that can be assessed or measured.

What aspects of compliance with the document will be monitored	What will be reviewed to evidence this	How and how often will this be done	Detail sample size	Who will co-ordinate and report findings	Which group or report will receive findings
Breaches of procedure	Reported incidents	Quarterly review and summary report on all IG incidents	N/A	Trust Information Governance Manager	Information Governance Steering Group
Legitimate access to personal Information	Requests from users to access patient records	Quarterly as part of audit of record tracking	50 records per quarter	IG coordinator	Information Governance Steering Group
Legitimate access to personal Information	Review of privacy Notifications on NHS Portal	Monthly	N/A	IG coordinator	Identified Breaches escalated as appropriate
Overall compliance with NHS best practice and legal requirements	Compliance with standards set in the Data Security and Protection Toolkit	Annual assessment made by IGSG	N/A	Chair of IGSG	IGSG approves assessment before submission to NHS Digital

7.2 Where monitoring identifies deficiencies actions plans will be developed to address them.

8 Arrangements for Review of the Policy

8.1 This policy will be reviewed in three years unless a substantial change in policy or legislation takes place when an earlier review will be undertaken.

9 References

Information Commissioner Website
https://ico.org.uk/for-organisations/guide-to-data-protection/

Health and Social Care Information Centre Confidentiality Policy Section:
http://systems.hscic.gov.uk/infogov/confidentiality

10 Appendix A: Guide to the Disclosure and Sharing of Personal Information

Staff Guidance on the Disclosure and Sharing of Personal Data

Introduction

This appendix considers some common disclosure situations encountered by ELFT staff and is provided to support staff to make decisions about disclosure in such situations.

Information governance policies and procedures are designed to support best practice in information handling and should not be a barrier to the sharing of personal information when necessary and appropriate. However, it is recognised that some circumstances produce complex situations which require careful consideration and if unsure about a specific issue, staff should seek guidance from line management and/or the Information Governance Team.

A flowchart to follow when considering how to respond to a request to share /disclose information about a patient is attached at annex 1. It will cover many but not all situations staff will.

Disclosing Information to Relatives and Carers

Staff will deal with numerous inquiries from relatives and friends of patients seeking information about progress and treatment. Many inquiries will be made over the telephone by people who are not registered as the patient's next of kin or carer and in these circumstances it is sometimes difficult to decide if any information should be passed on.

While in most circumstances a patient will not object to updates about their condition being given in response to an inquiry, circumstances do arise when this will not be appropriate. It is therefore good practice to establish and record if the patient wishes to place any restrictions on the information provided about them to others. This will make it easier to respond appropriately to any telephone inquiries received. Where restrictions are placed on information to be provided about patients it is important all staff likely to handle inquiries are made aware of the details to avoid a breach of confidentiality.

On receipt of an inquiry from a person not known to staff, where practical, the consent of the patient to disclose information should be sought. Where this is not possible a disclosure decision has to be made based on the information provided by the caller justifying their 'need to know'. Sensitive and detailed information should normally only be disclosed or discussed with nominated or recognised next of kin, close relatives or carers.

If suspicious about the motives of a person making an inquiry about a patient do not pass on any details but take a contact number and discuss with a senior colleague and seek advice before making contact again.

Disclosing Information to the Police

Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 provides a lawful basis for the Trust to disclose personal data about a person in the absence of their consent where this will support certain aspects of law enforcement and in particular:

- the detection, punishment and prevention of crime
- the identification, apprehension and prosecution of offenders

Most inquiries made by the police for information using this provision will be handled first by the Information Governance Team. Occasionally inquiries will be made direct to wards and departments and where time permits these should be discussed with the Information

Governance Team.

Occasionally urgent requests will be made asking for specific information to be provided in a short period of time. Often this is due to strict timelines imposed on the police to make decisions to charge suspects or to support urgent lines of investigation. In these circumstances decisions may have to be made quickly but staff should not be pressured into disclosing information when they feel it is not in the patient's best interest.

While the law permits disclosure in the circumstances outlined above it does not compel the Trust to comply with such information requests. Each case should be considered on the individual merits of the request. Where consent to disclose information to the police is not provided or refused the Trust has to consider the duty of confidentiality owed to the data subject and the public interest in maintaining a confidential service and balance this with the wider public interest in making the requested disclosure to support law and order purposes. Striking the appropriate balance in some situations can be challenging and in these scenarios, where possible, staff should seek specialist advice from the Information Governance Team.

In addition to the police it should be noted that other agencies such as the Home office, HMRC and NHS Counter Fraud Services may request information about patients using exemptions.

Access to Information for Audit, Service Improvement and Research Purposes

Clinical Audit

Clinical audit is recognised as a necessary tool to check the care provided by the Trust meets acceptable standards and is safe and effective. Access to patient personal information (e.g. detailed medical records) without consent for the purpose of clinical audit is normally permissible. The audit should be internal to the Trust and not part of a multi-site/organisation audit and the audit would normally be registered with the Trust clinical audit service. Where these criteria are not met and access to patient information is requested advice should be sought before sharing information or allowing access to patient records.

Service Improvement

Dependent on the circumstances access to patient personal information without consent for the purpose of conducting a Service Improvement project may also be permissible. The term 'service improvement' is widely used to cover a range of improvement activities and caution should be exercised to ensure the boundaries between service improvement and research activities are not blurred.

Research

The Trust undertakes medical research and clinical trials. Most research activity requires formal ethical approval and patient consent is normally required before access to any patient personal information is provided or made. The need to obtain patient consent can be waived in some circumstances following formal application to the NHS Research Authority (NHSRA).

Sharing Information for Safeguarding Purposes

Caldicott principle 7 makes clear that in certain situations the duty to share information is as important as considerations of confidentiality. This is particularly the case in matters of safeguarding where in the past public authorities have failed individuals by not sharing information they have held which if passed on may have prevented someone harming them.

Where an individual is thought to be at risk, relevant information should be shared between

agencies involved with the individual if the provision of that information might reduce or eliminate the identified risk. If it is possible to obtain consent from the subject to share their data this should be done, but the absence of or a refusal to provide consent should not deter staff from sharing information where it is felt to be appropriate and justified to support a safeguarding purpose.

Annex 1 to Appendix A