Liverpool Women's NHS Foundation Trust

REF: PL003

Data Protection, Access to Information and Information Sharing Policy

Version	3.3
Designation of Policy Author(s)	Head of Information Governance and Patient Records
Policy Development Contributor(s)	None
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date issued	01/04/2024
Review date	31/03/2025
Coverage	Trustwide
Grade of Change	Minor Change
Summary of Changes	General wording update to ensure policy is aligned with policy decisions taken and legislation. No significant changes.

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at www.nrls.npsa.nhs.uk/beingopen and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

Content Page

1 Executive Summary

1.1 Applicability and Scope

i. This policy covers all aspects of information within the organisation, including (but not limited to) patient/client/service user information, staff personnel information and organisational information.

ii. This Policy covers all aspects of handing information within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information.

iii. This Policy covers all Information systems purchased, developed, and managed by/on behalf of the Trust and any individual directly employed or any individual undertaking activity under the control or direction of the Trust.

2 Introduction

i. The Trust regards all person identifiable information that it holds or processes as confidential and will implement and maintain policies to ensure compliance with all necessary mandatory obligations.

ii. The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Effective information governance plays a key part in supporting clinical governance, service planning and performance management.

iii. Effective Information Governance gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently, and effectively in order to deliver the best possible care.

iv. The Trust will ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

3 Policy objectives

i. To define the standards and Trust rules for all individuals for the management of Data Protection and the release or sharing of information

4 Duties and Responsibilities

4.1 The Senior Information Risk Owner

- Is accountable for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control.
- Reviews and approve actions in respect of identified information risks

- Ensures that the organisation's approach to information risk is effective in terms of resource, commitment and execution
- Sets the overall objectives for Information Governance for the Trust

4.2 Caldicott Guardian

- Is agreed as the patient 'conscience' of the organisation and to advise the Trust Board on matters relating to patient confidentiality.
- Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
- Approves the release of patient information where consent from the data subject is not considered necessary or appropriate

4.3 Chief Information Officer

- Has overall responsibility for the operation of Information Governance for the Trust
- Ensures the overall approach taken to managing Information Governance is appropriate

4.4 Head of Information Governance and Patient Records

- Maintains and develops the Trust Information Governance and Information Security Policy and Framework.
- Manages Confidentiality and Data Protection across the Trust as the Subject Matter Expert.
- Is responsible for the Trust Information Governance submission.
- Implements the Information Governance related directives and objectives of the Senior Information Risk Owner

4.5 Data Protection Officer

- Informs and advises the Trust about obligations to comply with the UK General Data Protection Regulations (UKGDPR) and other data protection laws.
- Monitors compliance with UKGDPR and other data protection laws and with relevant policies.
- Advises on, and ~~to~~ monitors, Data Protection Impact Assessments
- Acts as a point of contact for the Information Commissioner

4.6 Information Governance Manager

- Manages the Trust Data Security and Protection Toolkit process and submission.
- Provides advice and guidance on compliance to mandatory standards and monitors adherence to those standards.
- Monitors action plans related to the maintenance of, compliance with or adherence to mandatory compliance standards.
- Is responsible for Subject Access and Freedom of Information requests.

5 Main Provisions

5.1 General Provisions

i. The Trust will ensure that:

- Personal data is processed fairly and lawfully and shall not be processed unless specific GDPR conditions are met
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018 and UK General Data Protection Regulations
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

ii. The trust will maintain its annual registration with the Information Commissioner

5.2 Individuals Rights

i The Trust recognises that individuals about whom the Trust processes information have specific rights that are derived from UKGDPR and will ensure those rights are enacted appropriately

ii. The Trust will ensure an individual's "Right to be Informed" is enacted through the publication of Privacy Notices, which will be published on the Trust website

iii. The Trust will provide a "Right of Access" about whom the Trust processes information through the Subject Access process, the details of which can be found in Paragraph 5.3

iv. Where an individual believes that information the Liverpool Women's Hospital holds about them is incorrect then the Trust will enact the "Right to Rectification", which means that if information is found to be factually incorrect then it will, without undue delay, be rectified.

v. Where an individual about whom the Liverpool Women's Hospital processes information has provided consent to process their personal information then, so long as there is no other overwhelming reason to continue processing, such as where there is a legal obligation, the Trust will:

a. Enact the "Right to Erasure" and erase information it holds on the individual.
b. Enact the "Right to Restrict Processing" and restrict the processing of the information whilst requests are being considered.

c. Enact the “Right to Data Portability” and provide the information to the individual, where technically possible, in a format that is portable and can be read by other IT systems.

vi. Under certain circumstances, individuals will have a Right to Object to the Trust processing their personal information and, where an objection is received, it will generally be honoured so long as there is no other legal or reasonable justification to continue to process the information.

vii. Individuals have a Right to be informed where the Trust is undertaking automated decision making. Information in relation to such processing will be made available within the Trust Privacy Notices which are published on the Trust website.

5.3 Access to Information (Subject Access)

i. The Trust will provide services that allow individuals, about whom it processes information, to access the data in accordance with the Subject Access Provisions of the Data Protection Act 2018 and UK General Data Protection Regulations

ii. The Information Governance Department will, with the exception of requests that are managed in accordance with Paragraph 5.3.iii (below) and Paragraph 5.3.iv (below), manage all Subject Access Requests in accordance with the provisions of the Data Protection Act 2018 and UK General Data Protection Regulations, which incorporates the following requirements:

- The Trust will not charge for the release of information under the Subject Access Provisions but reserves the right to charge for copies of requests that have already been processed and released
- Subject Access Requests shall be released, as soon as reasonably practical and in any case, within 28 days of the date the request was received
- A Subject Access Request shall only be considered a valid request if the data subject has the authority to make the request
- Simultaneous requests made by two or more individuals for information the Trust holds about them shall be processed as separate requests
- Where there is information about other individuals in a data subject’s records, the records shall be ordinarily redacted unless it is reasonable not to do so in all circumstances or authority has been given by the other individual not to withhold the information about the other individual(s)

iii. The Safeguarding Department will manage all requests for the release of information:

a. That are received from the Police, regardless of their nature.
b. Where the purpose of the release is pertinent to child protection, regardless of the source of the request.
c. Where the purpose of the release is pertinent to any other safeguarding issue, such as family domestic violence, regardless of the source of the request.

iv. The Imaging (Radiology) Department will manage all requests for the release of information where such information is of a type that is normally held or controlled by the Imaging (Radiology) Department

v. Staff will ensure that the rights of individuals to access information, which the Trust holds about them, are appropriately respected and support is provided to individuals who wish to make such requests by referring them to the relevant department.

vi. Although the Data Protection Act 2018 and the General Data Protection Regulations apply only to living individuals, in line with the Common Law Duty of Confidentiality, the Trust will manage and protect the information of deceased individuals in the same way as living individuals.

vii. Any individual, about whom the Trust holds information, has a legal right to have the information the Trust holds about them as being accurate. Where an individual believes the information, that the Trust holds about them, is inaccurate then the Information Governance Department shall be the central point for reporting the inaccuracies. The Information Governance Department will then liaise with the relevant Department to progress the matter and, where it is found to be inaccurate, co-ordinate the necessary changes.

5.4 Pseudonymisation

i. There may be circumstances where it is reasonable to share information and, at the same time, ensure the information is linked to identifying information, but is, at the same time, not appropriate or lawful to allow identifying information to remain within the data. Under these circumstances it may be appropriate to pseudonymise the information. Where this is the case then the information will be pseudonymised in accordance with the Standard Operating Procedure for Pseudonymisation.

5.5 General Conditions in relation to Information Sharing and Release

i. All staff who share any patient information are expected to ensure that the sharing is lawful. Where doubt exists, the member of staff responsible for the information is expected to consult with the Head of Information Governance and Patient Records.

ii. It is recognised that certain departments, such as Digital Services or Estates, engage the services of external companies to support the Trust in its day-to-day activities, and in doing so, employees of those companies may need to have access to identifiable information. The manager who signs the contract shall ensure that:
    - There is sufficient indemnity with the contract to protect the Liverpool Women's Hospital from the actions of the contract partner.
    - There are specific and robust provisions in relation to confidentiality within the contract.
    - Due account has been taken of the Caldicott Principles

iii. In all circumstances of information sharing for healthcare purposes, staff will ensure that:
    - Sharing complies with the law, relevant guidance, and best practice

- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it.
- Individuals' rights will be respected, particularly confidentiality and security
- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations

v Where information is shared, the department sharing the information must register the outbound flow on the Data Flow Register, which is maintained by the Information Governance Department

vi The Trust will process and share personal information in line with its Privacy Notices. Where the processing or sharing of information falls outside the Trust Privacy Notices then the Trust will seek consent prior to processing an individual's personal information.

vii The Trust will enact the rights of individuals in accordance with the UK General Data Protection Regulations and any other related UK legislation.

viii The Information Governance Department will be the central point of call for all data subjects who wish to withdraw consent for the processing or sharing of their personal information.

5.6 Information Sharing in Relation to Children

i. The Trust recognises the right of children (anyone under the age of 18) to enact their rights under the provisions of the Data Protection Act 2018 and the UK General Data Protection Regulations. When deciding how to enact a child's data protection rights, the Trust will take due account of:

a. The age of the child, meaning that a child of age 12 or over shall be presumed to be of sufficient age and maturity to enact their own rights.
b. Whether, regardless of age, the child is of sufficient maturity to be able enact their own independent data protection rights.
c. Whether an adult who is acting on the child's behalf is acting in the child's best interests when enacting their data protection rights
d. Whether an adult who is acting on the child's behalf has parental responsibility for that child

5.7 Statutory Instruments and Court Orders

i. Where a mandatory release, such as a Court Order, does not specify the information to be released, those responsible for releasing information are required to demonstrate that they have applied due diligence when considering what to release. Where doubt exists, the matter should be referred to the Head of Information Governance and Patient Records for further consideration. Where necessary, further consideration and approval to release will be sought form the Caldicott Guardian.

5.8 Ensuring Safe and Secure Transfers of Information

i. Staff will ensure all reasonable steps are taken to ensure that any released information is appropriately protected during transmission. It is up to each member of staff to demonstrate they have taken such steps. Where staff have doubts as to the appropriate mechanisms to be applied to appropriately protect identifiable information then they should consult the Head of Information Governance and Patient Records for guidance.

5.9 Information Sharing by Email

i. Staff are expected to ensure that, where it is necessary to transmit personal or sensitive information by Email, then staff will comply with the Caldicott Principles and ensure only the minimum amount is contained within it to achieve the specific purpose.

ii. Where personal or sensitive information is to be E-mailed externally, then an appropriate method of encryption or protection is to be used. In the unlikely event that such methods are not used, the sender will be expected to demonstrate that there was no other reasonable alternative, or the information was transmitted in such a way with the express consent of the data subject.

5.10 Authority to Act

i. Approving Officers are, for the purposes of this Policy:
   - Chief Information Officer
   - Head of Information Governance and Patient Records

ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer

iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest.

iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Governance Committee at the first opportunity.

5.11 Reporting

i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control.

ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

6 Key References

i. The Data Protection Act 2018
ii. The UK General Data Protection Regulations
iii. The Information Security Management NHS Code of Practice

iv. The NHS Confidentiality Code of Practice
v. The Records Management NHS Code of Practice
vi. Freedom of Information Act 2000
vii. Data Security and Protection Toolkit
viii. The Computer Misuse Act 1990

7 Associated Documents

i. Procedures:
PR002 – Management of Subject Access Requests

ii. Forms:
FM010 – Subject Access Application Form

8 Training

i. Training for implementation of this policy is contained within the Trust overall training program and is reference by the Information Governance and Information Security Policy and Framework

9 Policy Administration

9.1 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	14/02/2023	
Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes		
External Stakeholders			
Trust Staff Consultation via Intranet	Start date: 02/2023		End Date: 02/2023
Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)			By Whom will this be Delivered?
The policy is existence already			

Version History

Date	Version	Author Name and Designation	Summary of Main Changes

21/08/2017	1.0	Russell Cowell, Head of Information Governance	Policy has been completely reviewed and re-written. Policy version set to version 1.0 to reflect the substantial changes and the fact that it has been developed as an integrated policy set
08/08/2018	1.1	Russell Cowell, Head of Information Governance	Update to policy to withdraw charging provisions in accordance with the changes required as a result of the implementation of the General Data Protection Regulations
31/03/2020	2.0	Russell Cowell, Head of Information Governance	Major review and revision of wording considering lessons learned, introduction of new governance arrangements, insertion of GDPR definitions and provisions following independent external review by Data Protection Officer
31/03/2021	3.0	Russell Cowell, Head of Information Governance	General wording update to ensure policy is aligned with policy decisions taken and legislation. No significant changes.
31/03/2022	3.1	Russell Cowell, Head of Information Governance	Change to the management of Information Releases
31/03/2023	3.2	Russell Cowell, Head of Information Governance and Records	General wording review and re-approval by Information Governance Committee. Update to job title of Head of Information Governance to add “and Records” to title. Re-allocation of policy sponsorship to the Chief Information Officer
31/03/2024	3.3	Russell Cowell, Head of Information Governance and Patient Records	General wording update to ensure policy is aligned with policy decisions taken and legislation. No significant changes.

10 Equality Impact Assessment

Does The Policy Affect:	Staff		Patients		Both	X

Equality Group	Impact (Positive/Negative/Neutral)
Race (All Ethnic Group)	Neutral
Disability (Inc Physical, long term health conditions & Mental Impairments)	Neutral
Sex	Neutral
Gender Re-Assignment	Neutral
Religion Or Belief	Neutral
Sexual Orientation	Neutral
Age	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Other e.g., caring responsibilities, human rights etc.	Neutral

For each protected characteristic, consider whether the impact is positive. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)
Not Applicable
For each protected characteristic, consider whether the impact is negative. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)
Not Applicable
If your assessment has identified any negative impacts, please detail any actions that have been put in place to mitigate these (upon approval of EIA these actions will be shared with the Equality, Diversity and Inclusion Committee):

Outcome	Actions Required	Time Scale	Responsible Officer

Is there evidence that the s. 149 Public Sector Equality Duties (PSEDs) will be met? Consider whether the proposed policy will…

- Eliminate discrimination, victimisation, harassment, and any unlawful conduct that is prohibited under this act
- Advance Equality of opportunity
- Remove or minimise disadvantages suffered by people who share a relevant protected characteristic that are connected to that characteristic
- Take steps to meet the needs of people who share a relevant protected characteristic that are different from the needs of people who do not share it
- Encourage people who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such people is disproportionately low.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. (Consider whether this is engaged. If engaged, consider how the project tackles prejudice and promotes understanding - between the protected characteristics)

Explain your answers below.

The policy is an administrative policy, which implements established legal obligations neutrally.

Does the EIA have regard to the need to reduce inequalities for patients with access to health services and the outcomes achieved? (this section is a requirement for any services outlined within the NHS England and Improvement Core 20 Plus 5 approach to health inequalities) Explain.

The policy is an administrative policy, which implements established legal obligations neutrally.

Section 2:

To be completed by the EDI Manager authorising the EIA

Anything for noting or any recommendations for consideration by the Board

Guidance Note: Will PSEDs be met? Are Core 20 Plus 5 services considering patient health inequalities?

Review Date:	

Additional Supporting Evidence and Comments: