Liverpool Women's NHS Foundation Trust

Ref: PL002

Confidentiality Policy

Version	3.2
Designation of Policy Author(s)	Head of Information Governance and Records
Policy Development Contributor(s)	None
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date issued	01/04/2023
Review date	31/03/2024
Coverage	Trust Wide

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.

CONTENTS Page

1 Executive Summary

1.1 Applicability and Scope

i. This Policy covers all aspects of personal 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 confidential information

4 Duties and Responsibilities

4.1 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~~ advises 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
- Supports the implementation of Information Governance overall objectives as directed by the Senior Information Risk Owner

4.4 Head of Information Governance and 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 Subject Access and Freedom of Information requests.
- Implements the Information Governance related directives and objectives of the Senior Information Risk Owner

4.5 Local Information Governance Leads

- Act as the primary departmental point of contact for Information Governance and Information Security related matters.
- Attend the Trust Information Governance Committee meetings.
- Co-ordinate departmental compliance to Information Governance and Information Security training and deal with any areas of non-compliance.
- Undertake local Information Governance and Information security assessments where necessary.
- Ensure the Information Governance Committee decisions are implemented within the area represented.

4.6 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

4.7 Information Assurance 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

5 Main Provisions

5.1 General Provisions

i. All staff are responsible for ensuring that access to any area that contains confidential information is only granted to individuals who have an operational need to be there at that time and are authorised to enter that area

ii. All staff are responsible for ensuring that confidential information is not left unattended and/or unsecured, which applies to, but is not limited to, physical information, such as filing cabinets and electronic information such as information stored on computer systems

iii. Staff may only access confidential information as part of their duties within the Trust and must not access confidential information for their own interests, including their own clinical records

iv. All Staff must ensure that no document containing confidential information is left anywhere where it can be viewed by anyone who does not have the authority or need to do so

v. Staff must ensure that conversations involving the sharing of confidential information are not held where they can be overheard by anyone who does not need to know the information that is the subject of the discussion

vi. Staff are required to ensure that any printed materials are removed from printers or fax machines immediately after they have been printed and to ensure documents are managed electronically wherever possible.

vii. Where staff contact service users and need to leave a telephone message for them, staff should ensure that the wording of the message that is left for them is in line with the Caldicott Principles and only the minimum information is contained within the message to achieve the intended purpose. Unless there is a specific need to do so and there is certainty that only the recipient will receive the message, staff should state only their name and number and that they are calling from the Liverpool Women's Hospital, then ask the person, who they left the message for to call them back. When the person calls back, staff must verify the identity of the caller before discussing any matter with them.

viii. Staff must ensure that they access information systems only for purposes relating to their role and discharging their responsibilities in that role

ix. Staff are responsible for ensuring that items that are used to control access to confidential information, such as keys or physical access swipe cards, are not left unattended at any time

x. Any member of staff in a position to sign a contract, Service Level Agreement or other formal document, which involves the processing of confidential information, shall ensure that:

- There is a clause describing how the information will be stored, handled and processed
- It is an equivalent standard to what is expected if the information was handled internally by the Trust
- There is a clause stating that the Trust has the authority to inspect the conditions under which the agreement partner is processing such information
- There is sufficient indemnity for the trust in relation to inappropriate actions of the agreement partner or their staff
- There are explicit statements specifying that all data processors and sub-contractors shall act only in accordance with instructions issues to them by the Trust

There is a general duty on all signatories to undertake “due diligence” during any formal agreement consideration process, which means that reasonable efforts should be taken to ensure the agreement partner is compliant with all data protection obligations such as the General Data Protection Regulations and the Data Protection Act 2018.

xi. Managers will ensure that staff within their department or area are given sufficient opportunity to undertake appropriate annual Information Governance training

xii. Managers are responsible for the systems and processes in operation within their department, which support Information Governance standards and will ensure the acceptable standards are maintained

xiii. The Trust will take appropriate action against any individual who has been found to have deliberately, or by deliberate omission of action, failed to maintain the minimum standards of conduct expected of them

xiv. The Trust will allow access to confidential information that is processed by the Trust to only those individuals who have expressly agreed, or are contractually obliged, to comply with this Confidentiality Policy.

xv. Where it is deemed appropriate, the Trust may report any individual, who has breached confidentiality, to the Information Commissioner. Where such action is considered necessary, it shall be approved by the Director of Workforce and Marketing

xvi. The Chief Information Officer shall preside over all disciplinary cases where a breach of confidentiality is the primary matter that is being considered

5.2 External Employees including Contractors

i. Individuals who are not directly employed by the Liverpool Women's Hospital shall not be granted access to any Liverpool Women's Hospital information system unless such access has been approved via the completion of Form FM001 and FM002

ii. No individual who is not directly employed by the Trust shall be granted access to Trust data or systems for any period not covered by a valid FM001 and FM002 form

iii. At all times, external employees including contractors, will act under the instructions of the Trust

5.3 Staff who Access their own Personal Clinical Records

~~i.~~ Where a member of staff uses any of the Trust systems to access their own personal clinical records, the Head of Information Governance will report the matter to the member of staff's department manager.

ii. Where a member of staff accesses their own personal clinical records and, in doing so, accesses personal information about another individual then the matter shall be considered a breach of confidentiality

iii. Where any member of staff, having already been subject of a notice specified in para 5.3.i, accesses their own clinical record for a second time, the matter will be reported to the Head of Service for the department within which the member of staff is employed. The individual may, therefore, be subject to disciplinary action

5.4 Use of Cameras and Other Visual Recording Devices by Staff and Patients

i. The Trust recognises that modern devices, such as mobile phones, have the capability to be used as either visual or audio recording devices. It shall be down to local department managers to consider the extent to which devices, that can record, may be used within their Departments

ii. The Trust recognises that the use of audio or video recording devices by patients and visitors will give rise to a risk of breaching the confidentiality of patient's, visitor's or staff member's confidentiality. The Trust expects staff to be vigilant when such devices are being used by patients and it is up to staff to remind them, whenever necessary, to respect the confidentiality of others whilst on the Trust premises and to ask them to comply with those local rules. Where staff have satisfied this obligation but patients or visitors do not comply, staff are expected to escalate the matter to an appropriate manager

iii. Members of staff are allowed to use mobile phones, or other equivalent devices, except in circumstances where they would breach any Trust policy, professional obligation, professional code of conduct, or reasonable expectation

5.5 Use of Visual Communication Technology for Trust Business

i. The Trust regards “Microsoft Teams” and “Attend Anywhere” as secure, meaning that they can be used for normal day to day operational use as a communication tool and will provide technical support to support their use.

ii. In recognising “Microsoft Teams” and “Attend Anywhere” as operationally beneficial, the Trust will allow personal confidential information to be used within those environments but only to the extent that those platforms are used for communication purposes.

iii. The Trust regards “Zoom” as a platform that staff may use for normal day to day operational use as a communication tool, however, the Trust does not provide technical support to support its use.

iv. All platforms referred to in Paragraph 5.5 are platforms that are to be used for communication purposes only. Personal confidential information cannot be processed within those platforms for any reason other than for the purposes of communication.

v. All platforms referred to in Paragraph 5.5 may not be used as a data repository for any personal confidential information.

vi. The use of other technology platforms that are to be used for Trust operational activities shall be considered on a case by case basis and approved for use in accordance with provisions of Paragraph 5.8

5.6 Call recoding and Monitoring

i. Where it is considered necessary, the Trust will implement call recording and monitoring on its telephone network. Where call recoding is operating on any telephone extension then the Trust will ensure, so far is reasonably practicable, that that patients, staff, visitors and others that may communicate on behalf of, or with, the Trust, are made aware that their calls are being recorded

5.7 Home and Remote Working

i. Where a member of staff is working from home or from any other remote location:
    a. The member of staff will ensure that only Trust approved hardware and software are used
    b. The member of staff shall make all necessary arrangements to ensure that any internet connected devices that have the capability to “listen”, such as smart speakers, are not able to “listen” to any Trust related conversations that take place in the member of staff’s home or remote location

ii. Where a member of staff is to work from home or from any other remote location and there is an expectation that such arrangements will become a normal part of a member of staff’s working pattern:
    a. A risk assessment must be carried out prior to the commencement of those working arrangements to ensure that any identified risks are identified and mitigated.

b. The arrangements shall be such that there is no increased risk created by the arrangements than that which would exist if the member of staff was working on Trust premises

5.8 Authority to Act

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

5.9 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. All associated documents are available via the Trust Intranet at:
http://imt012/Policies_Procedures_and_Guidelines/default.aspx

ii. Procedures:
PR001 – Fairwarning Standard Operating Procedure

iii. Forms:
FM001 – General Confidentiality 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	19/03/2018	None
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: January 2018		End Date: January 2018
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.
12/02/2019	1.2	Russell Cowell, Head of Information Governance	Wording modified for paragraphs 5.3.i and 5.3.ii Emphasis shifted from clinical records to both clinical and non-clinical records
31/03/2020	2.0	Russell Cowell, Head of	Major review and revision of wording

		Information Governance	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 update of wording to ensure policy is kept up to date with changes to practice and legislation. Additional paragraphs added to accommodate rules on home and remote working.
30/03/2022	3.1	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
30/03/2023	3.2	Russell Cowell, Head of Information Governance and Records	Policy brought up to date with changes to job title of Head of Information Governance to add “and Records”. Reallocation of sponsorship to Chief Information Officer. Addition of paragraph to define the policy position for staff when leaving phone messages for patients

10 Initial Equality Impact Assessment Screening Tool

Name of policy/ business or strategic plans/CIP programme: **Confidentiality Policy**	**Details of policy/service/business or strategic plan/CIP programme, etc:**	
Does the policy/service/CIP/strategic plan etc affect (please tick) **Both** X		
Does the proposal, service or document affect one group more or less favourable than another on the basis of:	**Yes/No**	**Justification/evidence and data source**
Age	No	All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity
Disability: including learning disability, physical, sensory or mental impairment.	No	
Gender reassignment	No	
Marriage or civil partnership	No	
Pregnancy or maternity	No	
Race	No	
Religion or belief	No	
Sex	No	
Sexual orientation	No	
Human Rights – are there any issues which might affect a person's human rights?		**Justification/evidence and data source**
Right to life	No	Obligations laid out within the policy are primarily defined by the Data Protection Act. All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity. There would be no impact on the Human Rights as the Policy is a direct reflection of legislation, which itself would have considered the impact on Human Rights
Right to freedom from degrading or humiliating treatment	No	
Right to privacy or family life	No	
Any other of the human rights?	No	
EIA carried out by: Quality assured by: PGP Meeting	01/04/2022	Russell Cowell, Head of Information Governance