Ref: PL007

Liverpool Women's NHS Foundation Trust

Access to Clinical Systems

Version	3.3
Designation of Policy Author(s)	Head of Information Governance and Patient Records
Policy Development Contributor(s)	Head of Information and Performance
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	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 information within the organisation, including (but not limited to) patient/client/service user information, personnel information, 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 organisation and any individual directly employed or any individual undertaking activity under the control or direction of the organisation.

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 using accessing Trust clinical systems

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 Security for the Trust

4.3 Chief Information Officer

- Takes overall responsibility for IT Services for the Trust
- Ensures that the organisation complies with all mandatory requirements in respect of Information Technology, Information Security and Cyber Security
- Has overall responsibility for Information Security for the Trust
- Ensures the overall approach taken to managing Information Security, Information Systems and Information technology is appropriate

4.4 Head of Technology

- Is responsible for the management of Information Security across the Trust.
- Monitors local responses to Information Security incidents and provide support in developing proportionate and effective responses to manage risk.
- To be responsible, as operational Lead, for IT services and the associated security risks.
- Manages the Trust Information Technology infrastructure on a day to day basis as directed by the Chief Information Officer

5 Main Provisions

5.1 General Provisions

i. Only individuals who have been provided with a username and password are authorised to access any clinical system.

ii. Individuals may only access a clinical system if they are sufficiently trained are competent and can comply with all obligations.

iii. Access to a clinical system will be provided to individuals who have fully completed the necessary application forms.

iv. No individual may have access to any of the Trust clinical systems if there is no formal contractual association between the individual and the Trust.

v. The Trust reserve the right to undertake any reasonable investigations to enforce the provisions of this policy.

vi. The Trust reserves the right to suspend or terminate the access rights of any individual where there is reasonable belief that the user is not complying with any or all of the Trust policies or the user account has been compromised. Where such action is deemed to be necessary, it shall be approved by an Approving Officer

5.2 Responsibilities

i. All individuals granted access to any clinical systems have a personal responsibility to ensure that their login credentials are appropriately protected. Failure to apply appropriate protection for login credentials could be considered a disciplinary offence.

ii. Staff may only access a clinical system for activities related to their role with the Trust and any other purpose that is explicitly required and approved by the Trust.

iii. Staff are responsible for informing the Trust at the earliest opportunity where they have a reasonable belief that their access credentials have been compromised.

iv. Staff must ensure that they access information systems only for purposes relating to their role and discharging their responsibilities in that role and are responsible for all activities undertaken on their accounts.

v. Members of staff who deliberately use another person's login credentials may be subject to disciplinary actions.

5.3 Ensuring Access is relevant and Up To Date.

i. Information Asset Owners should ensure that an individual's access rights to any systems aligns with what they need to access within the system.

ii. Information Asset Owners should ensure procedures are in place to ensure that individuals access rights continue to align to their current role.

5.4 External Employees and Contractors

i. Access to clinical systems by individuals that are not directly employed by the Trust must be approved by an Approving Officer. Except as allowed under any other specific provisions elsewhere within this policy, access will only be provided for the period to undertake the necessary work.

ii. An external employee may not be granted access to a clinical system unless and until the individual has completed the Trust Confidentiality Forms as specified in the Confidentiality Policy and the individual has been registered on the Leavers System. External employees must declare an expected end date for when access is expected to end. Where a date is not declared then, notwithstanding other information that would indicate ~~if~~ that the individual has left before their scheduled end date, the individual's access will be deactivated after 6 months.

iii. The Information Governance Department will maintain, through the Leavers System, a register of all users that are not directly employed by the trust and have been granted access to the Trust network.

iv. An application by an employee for access to a clinical system must be sponsored by an appropriate manager, who is an employee of the Liverpool Women's Hospital. External employees cannot be given access for a continuous uninterrupted period exceeding 2 years. If the period of access reaches 2 years, then the individual shall re-apply for access. The Trust will accept no responsibility for users that have been deactivated as a result of a failure to submit a renewed application.

v. Allocation of User Accounts

The following rules will apply to the creation of user accounts and Office 365 accounts.

a. Where an individual is commissioned by the Liverpool Women's Hospital to provide a service then they shall be provided with the appropriate accounts, facilities and privileges that are needed for them to discharge their responsibilities that they have been commissioned to perform for the Trust.

b. Where an individual, or the organisation they work for, has requested access to clinical systems then, if approved, the level or access or extent of privileges shall be determined exclusively by the Trust. The Trust reserve the right to pass on any cost to the Trust in providing those facilities or privileges.

5.5 Password Management

i. Sharing of usernames and passwords or otherwise allowing an individual uncontrolled access to a clinical system is not allowed.

5.6 Intervention and Monitoring

i. The Trust may access any user account, or any software associated with that account, where it is considered necessary or there is a belief that a user account may be compromised. Where it is considered necessary to access an individual's user account then the instance of access shall be approved by an Approving Officer

ii. The Trust will monitor clinical systems access through the use of dedicated monitoring systems as part of its normal activity to ensure users are acting in accordance with their obligations.

5.7 Scheduled Termination or suspension of Access

~~i.~~ The Information Governance Department shall be informed of the leaving date of all leavers, which will be before the actual leaving date, and will provide the Information to IT Services~~.~~ The user account will be deactivated or suspended on the first working day after the date the individual leaves.

6.8 Unscheduled Termination or Suspension of Access

i. Where the need arises to deactivate or suspend the user accounts of individuals who require immediate account deactivation or suspension, it is the responsibility of the relevant manager to inform the Information Governance Department as soon as the need to immediately deactivate or suspend the user account is identified.

ii. It is the responsibility of the Information Governance Department to register the individual on the Leavers System and to inform system owners of the need to de-activate or suspend the user. Requests for immediate deactivation or suspension of user accounts shall be considered a priority and will be acted upon by system owners without undue delay and, in any case, within 30 minutes of being notified by the Information Governance Department

5.8 Authority to Act

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

5.9 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 General Data Protection Regulations
iii. The Information Security 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

7 Associated Documents

i. 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	14/02/2023	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: February 2023		End Date: February 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
03/09/2018	1.1	Russell Cowell, Head of Information Governance	Periodic review with minimal wording and KPI updates
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 related provisions and provisions following independent external review by Data Protection Officer
04/12/2020	3.0	Russell Cowell, Head of Information Governance	General review and minor update on policy wording to make provisions clearer based on experience.
31/03/2022	3.1	Russell Cowell, Head of	Review only and re-approval. No changes

		Information Governance	
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 review and re-approval by Information Governance Committee. Minimal 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:	