Liverpool Women's
NHS Foundation Trust

Ref: PL013

Audit Compliance Measurement and Maintenance of Standards

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	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.

Content 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, 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 mechanisms the Trust will use to measure the performance of Information Governance and Information Security Policies

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 and standards for Information Governance and Information Security for the Trust

4.2 Caldicott Guardian

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

4.3 Chief Information Officer

- Has overall responsibility for the standards and compliance of systems and processes within Digital Services for the Trust
- Ensures the overall approach taken to managing compliance and standards is appropriate

4.4 Head of Information Governance and Patient Records

- Maintains and develops the Trust Information Governance and Information Security Policy and Framework.
- Oversees standards and compliance across Digital Services in relation to confidentiality, data protection and information security.

5 Main Provisions

5.1 General Provisions

i. The Information Governance Department is responsible for setting the general standards for all Digital Services departments, where the issue to be considered relates to Confidentiality, Data Protection, or Information Governance

ii. The Information Governance Department is responsible for monitoring compliance of all Digital Services departments to the defined standards.

iii. The Information Governance Manager is responsible for monitoring compliance to the defined standards and monitor resultant action plans that have been created.

iv. The Trust will implement a range of measures that will provide effective definition of standards for all departments, will provide for effective monitoring of compliance compared to expected standards and effective monitoring of resultant remedial actions.

5.2 Data Security and Protection Toolkit

i. The Trust recognises the NHS Data Security and Protection Toolkit as the definitive standard to which it will work to with the overall objective being to achieve at least “Standards Met” across all 10 standards.

ii. The Head of Information Governance and Patient Records has overall responsibility for the effective management of the Data Security and Protection Toolkit. The Information Governance Manager is responsible for the day-to-day management of the Data Security and Protection Toolkit.

iii. All individuals who have responsibility to manage the system as a whole, or any of the individual requirements, have a responsibility to ensure they comply with both the standards of the Data Security and Protection Toolkit and the associated deadlines for submission.

iv. The Information ~~Assurance~~ Governance Manager will ensure that all individual requirements are delegated appropriately for the most effective management.

5.3 Cyber Essentials Plus

i. The Trust will aim to maintain accreditation of Cyber Essentials Plus

ii. The Head of Technology will be responsible for overseeing the Trust Cyber Essential Plus accreditation.

5.4 International Standards Organisation (ISO)

i. The Trust will maintain accreditation with ISO 27001

ii. The Information Governance Manager will be responsible for day-to-day management of the ISO process.

5.5 Information Governance Spot-check Programme

i. The Information Governance Department will undertake regular inspections and spot-checks, which will be managed by the Information Governance Manager. The regime will seek to assess different Trust department’s compliance to Information Governance standards, Trust Policies, and reasonable expectations.

ii. The Information Governance Manager will provide periodic updates to the Information Governance committee.

iii. Managers in areas that have been subject to inspection, and where issues of non-compliance have been identified, are expected to remedy any issues that have been identified by the Information Governance Manager without undue delay.

iv. The Information Governance Department have authority to assess any area of compliance under the Spot-check programme where there is a need to assess compliance against any policy that sits within the Information Governance and Information Security Policy and Framework

5.6 Audit

i. The Information Governance Committee may, at its discretion, instigate any audit that it deems reasonable to conduct and where assurance on any aspects of compliance to any policy covered by the Information Governance and Information Security Policy and Framework is necessary.

ii. The Information Governance Manager will be responsible for co-ordinating audits where necessary.

5.7 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.

5.8 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 1988
ii. The UK 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. Information Governance Toolkit
viii. The Computer Misuse Act

7 Associated Documents

i. Information Governance and Information Security Policy and Framework

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	C Farmer		
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: 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			

9.2 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. Minimal updates to wording and KPIs
31/03/2020	2.0	Russell Cowell,	Major review and revision of wording considering

		Head of Information Governance	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	Minimal wording changes
31/03/2022	3.1	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
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. No major 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:	