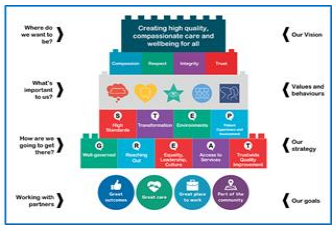

NHS
Leicestershire Partnership
NHS Trust

Clinical System Access and Confidentiality Audit Policy

This policy sets out the expectations relating to the access to clinical systems and the confidentiality audit and monitoring undertaken to support assurance that controls are in place to ensure appropriate access and compliance with confidentiality requirements.

Key words: Clinical Systems, access confidentiality, audit, monitoring

Version: 2

Approved by: Data Privacy Group

Ratified By: Finance & Performance Committee

Date this version was ratified: 20th August 2024

Date issued for publication: 22nd August 2024

Review date: January 2027

Expiry date: 20th August 2027

Type of Policy: Clinical and Non-Clinical

Contents

Policy On A Page

SUMMARY & AIM

What is this policy for?

TARGET AUDIENCE:

Who is involved with this policy?

TRAINING

What training is there for this policy?

KEY REQUIREMENTS

What do I need to follow?

1.0 Quick look summary

Please note that this is designed to act as a quick reference guide only and is not intended to replace the need to read the full policy.

1.1 Version control and summary of changes

Version number	Date	Comments (description change and amendments)
2	03/06/2024	Updated policy in new format

For Further Information Contact:

1.2 Key individuals involved in developing and consulting on the document.

- Chris Biddle, LHIS Cyber Security Manager
- Simon Jones, LHIS IM&T Business Manager – CHS
- Samantha Rogers, LHIS IM&T Business Manager – DMH
- Gurpal Singh, LHIS IM&T Business Manager - FYPC
- Afroz Kidy, LHIS Security, RA & Assurance Manager
- Claire Mott, Records Exploitation Manager
- Pat Upsall, CHS Clinical Safety Officer
- Tom Gregory, DMH IM&T Clinical Lead, Clinical Safety Officer
- Ruth North, FYPC&LDA Clinical Safety Officer

1.3 Governance

Level 2 or 3 approving delivery group – Data Privacy Group

Level 1 Committee to ratify policy – Finance & Performance Committee

1.4 Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender),

gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

If you would like a copy of this document in any other format, please contact lpt.corporateaffairs@nhs.net

1.5 Due Regard

LPT will ensure that due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- Strategies, policies and procedures and services are free from discrimination.
- LPT complies with current equality legislation.
- Due regard is given to equality in decision making and subsequent processes.
- Opportunities for promoting equality are identified.

Please refer to due regard assessment (Appendix 4) of this policy

1.6 Definitions that apply to this policy.

Due Regard: Having due regard for advancing equality involves:

- Removing or minimising disadvantages suffered by people due to their protected characteristics.
- Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Alerts: Notification of an action taken that requires reviewing

Clinical Systems: An information system designed for use in a healthcare environment to record interactions with individuals being provided with care, treatment, or support.

Confidential Audit: Focus on control within electronic records systems to ensure rules around access are adhered to.

Confidential personal data/information: Information relating to natural persons who can be identified or are identifiable directly from information or who can be indirectly identified from that information in combination with other information, and where it includes information of a sensitive nature (special category data) such as health data, genetic data, biometric data and ethnicity etc.

Controls: Tools used to manage, organise, and run in electronic systems.

Information Asset Owner: The individual responsible for ensuring specific information assets are handled and managed appropriately.

Information Asset Administrator: Responsible for the day-to-day management of data.

Legitimate Relationship: The relationship that exists between a patient and a healthcare professional providing the therapeutic support.

Privacy Officer: The healthcare administrator responsible for safeguarding patient confidentiality.

Proactive: Creating or controlling a situation rather than just responding to it.

Reactive: Acting in response to a situation rather than creating or controlling it.

Sub Privacy Officer: Responsible for safeguarding patient confidentiality working under the Privacy Officer.

Third Party: Someone who is not one of the main people involved in an activity but who is involved in a minor way.

2.0 Purpose of the Policy

This Policy addresses the access to clinical systems and the appropriate confidentiality audit procedure to monitor access to confidential personal data.

This includes:

- Ensure users understand their obligations in relation to accessing the clinical systems.
- How access to confidential personal data will be monitored.
- Who will carry out the monitoring/auditing of access.
- Reporting and escalation processes
- Disciplinary processes

The procedure also ensures that overall responsibility for monitoring and auditing access has been assigned to appropriate senior staff members e.g. Senior Information Risk Owner (SIRO), Caldicott Guardian, Head of Data Privacy (Information Governance Lead for the Trust) and Information Asset Owners (IAO's).

Confidentiality audits will focus primarily on controls within the electronic patient record system (clinical system) but should not exclude paper

record systems, the purpose being to discover instances of inappropriate access and whether confidentiality has been breached or put at risk through deliberate misuse of access or because of weak, or non-existent or poorly applied controls.

This document defines the procedure for providing access to systems and carrying out audits relating to access to personal confidential data in the Trust to ensure staff only access the records for individuals with whom they have a legitimate relationship, where there is a legitimate business need, in line with the NHS Care Record Guarantee, Data Security and Protection Toolkit and compliance with Data Protection Legislation.

With advances in the electronic management of information within the NHS, the requirement to monitor access to personal confidential data has become increasingly important. Furthermore, with the increased movement of information via electronic communications, there exists an increasing threat of information being accessed by individuals who do not have a legitimate right to access it.

The procedure applies to all staff who work for or on behalf of LPT (including those working temporarily, on secondment, as students or as part of an integrated team arrangement) and who have access to LPT clinical systems. It also applies to relevant people who support and use these systems such as Application Support Staff in the Leicestershire Health Informatics Services (LHIS).

3.0 Introduction

The Data Protection Act 2018 and the Retained General Data Protection Regulation 2016/679 (UK GDPR) require the Trust to implement technical and organisational measures to protect all personal data and information held within its systems. These control measures should support the Trust to manage and safeguard confidentiality, including mechanisms to highlight problems such as incidents, complaints and alerts. Documented procedures should be implemented to ensure these controls are monitored and audited. This forms part of the key assurance requirement and underpins the Confidentiality aspect of the CIA Triad (Confidentiality, Integrity and Availability).

Service users of the Trust expect that information in their clinical record will be treated as confidential. The Trust expects all employees to recognise and act upon their responsibility to maintain patient confidentiality. The

duty of confidentiality is confirmed in professional guidelines and contracts of employment.

Trust standards and expectations relating to information security and confidentiality are detailed in the Trusts' Data Protection and Information Sharing, and Information Security and Risk Policies. Any breach of confidentiality with regard to the disclosure of, or inappropriate access to, patient's personal information held by the Trust is a disciplinary offence, and may result in dismissal and/or prosecution.

Leicestershire Partnership NHS Trust (LPT) is required to have processes to highlight actual and potential confidentiality breaches in its systems, particularly where sensitive/personal confidential data is held. The Trust should also have procedures in place to evaluate the effectiveness of controls within these systems. All systems which process personal/sensitive confidential data should have audit trails that can report details of who has viewed and accessed specific records.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purpose may result in a breach of confidentiality, thereby contravening the requirements of Data Protection legislation, the Human Rights Act 1998 and the Common Law Duty of Confidentiality

Types of Confidentiality Alerts:

- Follow ups or failed log-in reports provided for information systems
- Monitoring of incident reports regarding stolen/lost computers/laptops, disclosure of confidential information
- Internal audits of reviews of IT security
- Complaints from members of the public/patients or staff
- Informal alerts made by staff
- Reported near misses
- Privacy Officer alerts generated within the clinical system

'Legitimate access' to a patients' record is defined as 'A clinical reason to access the record'. It is not acceptable to simply search the clinical systems. Should a staff member know a person open to services personally they should declare this to their line manager.

4.0 Policy Requirements

This policy applies to all of the Trust's staff and staff employed by partner organisations including non-healthcare providers who, during the course of their duties, will require access to the information held on the clinical system. Please note that should the need to share information with volunteers arise this must be done with the service user's consent.

The Policy sets out the processes required to provide access to clinical systems (mainly the electronic patient record) as well as the monitoring and auditing processes that are in place to safeguard personal and personal confidential information held within the clinical systems.

- New User Access requires that staff complete and sign the Registration Authority terms and conditions which outlines their responsibilities when accessing clinical systems. There are additional steps for access required for research purposes as well as those requiring temporary access as a temporary worker who arrive without a smartcard or with a smartcard and no access to unit. (both bank and agency) – See Appendix 7 for flowchart.?

- There are circumstances where third party workers i.e. healthcare workers employed by organisations outside of the Trust but working in partnership, require access to the Trusts clinical systems. In these circumstances a Third-Party Access Agreement is required to be completed prior to any access being applied.

- Privacy Officer and Sub Privacy Officer roles are important in the proactive monitoring of confidentiality audit and systems have been put in place to enable monitoring and reporting to the Data Privacy Group.

- Reactive auditing takes place where there are complaints, concerns or data protection incidents. This process is managed by the Trusts' Data Protection Officer and Deputy Data Protection Officer, with escalation to the Caldicott Guardian and SIRO

5.0 Duties within the Organisation

5.1 The Trust Board has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

5.2 Trust Board Sub-committees have the responsibility for ratifying policies and protocols.

5.3 Senior Information Risk Owner (SIRO) acts as an advocate for information risk on the Board and will be updated with the findings of the audits and receive copies of reports.

5.4 Head of Data Privacy/Data Protection Officer – the GDPR introduced the legal duty to appoint a Data Protection Officer (DPO) for all public authorities and on organisations that carry out certain types of processing activities.

The DPO will be responsible for ensuring that access to confidential information is audited within the Trust. Ensuring that reports produced from the clinical systems and other local computer systems by LHIS App Support are reviewed and followed up.

5.5 The Data Privacy Team provides support to the Data Protection Officer and fulfils the role of the Caldicott Guardian within the Trust's clinical system, which enables the monitoring of access when a clinician self-claims a legitimate relationship to a service user within the system and overrides consent.

5.6 Caldicott Guardian has overall responsibility for monitoring incidents and complaints relating to confidentiality breaches within the Trust and for ensuring that access to confidential information is regularly audited. They will work closely with the Head of Data Privacy to ensure that recommendations and concerns arising from confidentiality audits are actioned in a reasonable timeframe.

5.7 Data Privacy Group – will be responsible for ensuring that Confidentiality Audit Procedures are implemented throughout the Trust in line with DSPT requirements.

5.8 Information Asset Owners (IAOs) are the Clinical Service Directors or their nominated deputies who are responsible for ensuring that staff for whom they are responsible are aware of their responsibilities with regard to the confidentiality of information, including ensuring that all staff have undertaken mandatory Data Security Awareness (IG) Training.

They will be responsible for ensuring their staff are fully aware of the mechanisms for reporting actual or potential personal data breaches

within the Trust.

5.9 Information Asset Administrators (IAA's) are responsible for ensuring that access to personal confidential data is secure and strictly controlled. Monitoring should be carried out by the responsible administrator/manager, such that instances of alleged inappropriate access or misuse of confidential personal data can be identified and reported.
Access to personal confidential data must be allocated on a strict need to know basis, by those who require such access to perform their duties. Appropriate documented authorisation must be obtained to demonstrate the need to know prior to any additional access being given.

5.10 Clinical Systems Change Team (LHIS) are responsible for the management, configuration, administration, and operational support of the clinical systems on behalf of LPT. They are responsible for system development, upgrades, testing and ensuring that the system meets with local and national requirements. They are required to adhere to LPT Standard Operating Procedures and to provide assurance on activities undertaken on behalf of the Trust.

5.11 Human Resources are responsible for any investigations in accordance with the Trusts' Disciplinary Policy in conjunction with Trust managers as deemed appropriate based on the severity of the incident.

5.12 Managers and Team leaders are responsible for ensuring that staff for whom they are responsible for are aware of their responsibilities with regard to confidentiality of information and ensure all their staff have completed their data security awareness (information governance) annual training.

They are also responsible for ensuring that their staff are fully aware of the mechanisms for reporting actual or potential confidentiality breaches; complying with confidentiality audits and ensuring subsequent recommendations are complied with within specified time frames.

Access to electronic and/or manual confidential information must be strictly controlled within each manager's area of responsibility. They will be responsible for ensuring appropriate authorisation is gained prior to allowing access to clinical systems and personal confidential data in order that only those with a legitimate right are given access.

5.13 LHIS Registration Authority Team are responsible for ensuring authorisation is documented and retained for monitoring purposes, this should include information as to who has gained access, the department, the reason the access was required, the date access was given etc.

5.14 Service leads are required to monitor failed access attempts (password lockout tasks) where a request for access has been denied or prevented. Regular monitoring should be undertaken in order to highlight potential areas of concern.

5.15 All Staff have a duty to read and work within current policies. They should ensure that personal confidential data is not accessed without prior authorisation and completion of appropriate documentation. Personal confidential information should also not be disclosed to unauthorised recipients.

Any breach or refusal to comply with this policy is a disciplinary offence, which may lead to disciplinary action in accordance with the Trust Disciplinary Policy, up to and including, inappropriate circumstances, dismissal without notice.

All staff should be made aware of confidentiality audits may take place at any time.

6.0 System Access

6.1 User Access Request

New system users, including those requiring 'read only' access, will be required to complete an electronic system access form through the LHIS Self Service portal, which will need to be authorised (have an Approver selected). Users must indicate that they have read and understood this policy and the Registration Authority terms and conditions. Amendments to existing accounts will need to be requested via the same method.

Each request for access will be considered on an individual basis to ensure that the request is clinically appropriate and that the relevant access rights are granted.

6.1.1 Researcher Access Request

Where the applicant for an account is a Researcher, the request for a 'read only' account is made by the Research and Development Team, with the relevant R&D signatory. This is to ensure that the researcher is working on a research project where access to medical records with service user/patient consent has been approved by an Ethics Committee, or where appropriate, approval under Section 251 (access to medical records with patient consent) has been given by the Health Research Authority (HRA).

6.1.2 Non-substantive Worker Access

Access to patient's electronic records is required by all health professionals to facilitate continuation and clarity regarding patients care requirements and documentation of care delivered or issues encountered between all health professionals. It is therefore important that all staff providing care on behalf of the Trust are provided with the appropriate access.

Staff are required to follow the Non-Substantive Staff Access SOP for further information. See appendix 7 Non-substantive Staff Access Flow chart.

6.2 Access for Staff employed by Third Parties

There may be occasions when, in order to support seamless pathways of care, external agencies or partner organisations request that their staff are granted access to the clinical system.
An external agency might include (but not limited to):

- Another NHS Trust
- Local Authority
- Voluntary Sector Provider
- Private Sector Provider

A Third-Party Access Agreement and where necessary, a Data Protection Impact Assessment will need to be completed and agreed both by the requester and the Trust and approved before any system access is granted.

All third-party personnel requiring access to clinical systems will need to complete required system training and checking with their relevant organisation that they have completed information governance training. Those third-party personnel that require read and write access will need to undertake the relevant training for their role.

All requests for access to clinical systems by external agencies will be reviewed by the Data Privacy Team. A log will be retained of the access granted and the reasons for granting.

6.3 Additional Access Requests

The Trust may need to provide access to clinical information to a number of groups including but not limited to: Legal Advisors, Auditors,

Commissioners, Police Officers, Independent Medical Staff, Independent Mental Health Advocates and Mental Health Act Commissioners.

Dependent on the request, access may be granted via the subject access request process or via the supervised system access process.

Supervised access to the clinical system will be supported by a nominated member of staff to be able to access the relevant information in a timely manner.

The Data Privacy Team must be notified of each occurrence of supervised access in advance (where notice is provided) via the supervised system access request proforma. A register of all supervised access will be maintained, and this will be reported in the Caldicott Report.

6.4 Notification of De-Activation of accounts

Line managers are responsible for requesting the de-activation of clinical system accounts when members of their team leave the Trust or move service within the Trust. Access to SystmOne units needs to be managed carefully and all accounts must be removed when no longer required for a staff members current role.

The manager will ultimately be responsible for all transactions that take place on accounts that should be closed and are still active as a result of non-notification on behalf of their manager. Requests for de-activation of accounts must be made via the LHIS Self Service Portal.

6.5 Review of User Accounts

The Registration Authority Team will conduct bi-monthly reviews of the use of active clinical system user accounts. Accounts that have not had a successful log in during the previous 90-days will be suspended. A request for re-activation of the account must via lpt.lhis.cis@nhs.net and approved by an Authorised Signatory/Sponsor.

7.0 Monitoring and Audit Access

In order to provide assurance that access to personal confidential data is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis. This will be achieved by putting in place arrangements for both proactive and reactive auditing of access and communicated to all staff.

Monitoring may be carried out through the Data Privacy Team or with the Caldicott Guardians express written permission, the IAO in order that irregularities regarding access can be identified. If irregularities are detected these should be reported to the Data Privacy Team through to the Caldicott Guardian and action taken by the IAO to rectify the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

Actual or potential breaches of confidentiality should be reported immediately to the Data Privacy Team and by logging this as an incident on Ulysses (incident reporting system – eIRF), in order that the incident can be assessed and action taken to prevent further breaches.

The Data Privacy Team will be responsible for informing the Caldicott Guardian and SIRO of any concerns highlighted as a result of monitoring activity.

Should unauthorised access to personal confidential data be gained by any individual or if information is disclosed to unauthorised recipients, this will be dealt with in accordance with the requirements of the Disciplinary Policy.

7.1 Proactive Monitoring

This will generally achieved for systems where an automated function exists for alerting of user access to records for subsequent review by someone with Privacy Officer/Caldicott Guardian roles within the system.

Examples of proactive monitoring systems accessed by LPT staff include:

- Summary Care Record
- SystmOne

These generate alerts when users access or override one of the information governance controls.

The alerts will prompt receiving staff to establish if the access was justified or potentially inappropriate, which will warrant further investigation. A reasonable sample size of alerts will generally be reviewed on a monthly basis.

The outcome of these reviews will be escalated for further investigation

as appropriate, and issues/themes will be discussed at the Trust Privacy Officer Group in order to identify any lessons/review controls.

The role of the Privacy Officer and Sub-Privacy Officer is outlined in the Privacy Officer Standard Operating Procedure.

7.2 Reactive Monitoring

Reactive confidentiality audits will generally fall into two scenarios:

1. Where misuse of a system is alleged in relation to privacy/confidentiality breaches.

2. Where evidence is required to support management's concerns/investigations about staff conduct, e.g. excessive use of the internet, email activity or conduct (where the primary concern is not about privacy/confidentiality however the audit may have privacy implications).

This procedure addresses audit requests where privacy/confidentiality breaches are reported or suspected; and procedures for conducting audits in relation to staff conduct, management concerns/investigations will also be covered under relevant policies (i.e. Information Security and Risk Policy; Data Protection and Information Sharing Policy).

8.0 Confidentiality Audit and Escalation Process

8.1 Reactive Audit Process

Where an audit of user activity or access to records is required as part of an investigation, the request should initiated by the commissioning manager or an appropriate senior manager and audit requests should generally include a brief outline of the report/allegation and the information required, giving justification of the relevance of the audit information to the investigation.

An audit request form (Appendix 6) should be completed for audit requests and forwarded to the Data Privacy Team mailbox for the Data Protection Officer/Deputy Data Protection Officer to authorise and who has the responsibility to ensure that where necessary, a legitimate reason for access to the information is determined and

where appropriate consent is obtained and the privacy of staff is not unnecessarily breached.

Approved requests will be sent to the LHIS Cyber Security Manager for logging as a service request.

Caldicott principles should be adhered to at all times, with only the relevant information being shared regarding the need for the audit.

Upon completion of the audit, the LHIS Cyber Security Manager will provide the audit report to the Data Privacy Team to review and remove any irrelevant information and feedback to the commissioning manager. It is important that audit reports are only seen by as few staff as possible; and the audit report kept securely.

Reactive/Investigation audits may identify evidence of:

- Unauthorised viewing/access to confidential/patient/staff records;
- Failed attempts to access confidential information;
- Repeated attempts to access confidential information;
- Successful access of confidential information by unauthorised staff;
- Evidence of shared login sessions and smartcards;
- Inappropriate communications with patients/service users;
- Inappropriate recording and/or use of sensitive/patient information;
- Inappropriate allocation of access rights to systems or other data;
- Inappropriate staff access to secure/restricted physical areas

The Data Privacy Team, where required, will be responsible for liaising with HR colleagues to co-ordinate investigations into confidentiality breaches.

Investigation and management of confidentiality events and alerts will be conducted in conjunction with the relevant Privacy Officer and in line with the Trust's Disciplinary Policy and the Incident reporting Policy.

8.2 Proactive Audit Process

The Data Privacy Team will work with the Trusts Clinical Safety Officers and Privacy Officers to undertake sample audits of staff access within their relevant SystmOne Units during the financial year. A timetable will be developed and shared with the Data Privacy Group through the Data Privacy Highlight Report submitted to the Group in Q4 in order that there is a clear audit and reporting schedule.

8.3 Providing Audit information to Patient/Service Users

Both the National Information Board in 'Personalised Health and Care 2020' and Dame Fiona Caldicott in the 'Report of the Caldicott Review' have reaffirmed the commitment made in the NHS Care Record Guarantee to ensure that a record of who has accessed a service user's/patient's record can be made available in a suitable form to service users/patients on request. All requests of this nature need to be directed to the Data Privacy Information Request Team.

9.0 Management of IG Incidents

The Data Privacy Team monitors IG related incidents logged via the Trusts Incident Reporting system and will follow up all IG incidents via the Incident Review Meetings to achieve a satisfactory outcome in liaison with investigating managers. More serious incidents are managed using the Incident Reporting Tool on the Data Security and Protection Toolkit and are reported to the Data Privacy Group, which will escalate any unsatisfactory outcomes to the Executive Management Board and communicate pertinent IG messages/issues to staff using the Staff Newsletter, targeted communications etc.

Trends in incidents will be monitored in order to learn lessons and provide continual service improvement.

10.0 Training Needs

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as role based development training.

11.0 Monitoring Compliance and Effectiveness

Page/Section	Minimum Requirements to monitor	Method for Monitoring	Responsible Individual /Group	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group). Frequency of monitoring
P.10/S3 P17/S.7.1	Sample size of Privacy Alerts reviewed	Privacy Officer Reports	Privacy Officer Group	Monthly
P.8/S2 P.9/S3 P.11/S.4 P.21/S.12	Review of access in response to concern investigation	Data Privacy Highlight Report	Data Privacy Group	Bi-monthly
P.13/S.5.10 P.19/S.8.1	Liaison with HR to co-ordinate investigations	Data Privacy Highlight Report	Data Privacy Group	Bi-monthly
P.19/S.8.2	Timetable of sample audits of staff access within SystmOne Units.	Data Privacy Highlight Report	Data Privacy Group	Annually
P.20/S.9.0	Monitoring IG incidents of unauthorised/disclosure	Data Privacy Highlight Report	Data Privacy Group	Bi-monthly

12.0 Standard/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
Data Security and Protection Toolkit.	The organisation knows who has access to what systems – list held of access granted
Data Security and Protection Toolkit.	An audit of user lists and profiles provided

13.0 References and Bibliography

Data Protection Act 2018
Retained Regulation (EU) 2016/679 (UK GDPR)

Non-substantive Staff Access Standard Operating Procedure
Data Protection and Information Sharing Policy
Information Security and Risk Policy
LHIS Registration Authority Procedure

14.0 Fraud, Bribery and Corruption consideration

The Trust has a zero-tolerance approach to fraud, bribery and corruption in all areas of our work and it is important that this is reflected through all policies and procedures to mitigate these risks.

Fraud relates to a dishonest representation, failure to disclose information or abuse of position in order to make a gain or cause a loss. Bribery involves the giving or receiving of gifts or money in return for improper performance. Corruption relates to dishonest or fraudulent conduct by those in power.

Any procedure incurring costs or fees or involving the procurement or provision of goods or service, may be susceptible to fraud, bribery, or corruption so provision should be made within the policy to safeguard against these.

If there is a potential that the policy being written, amended or updated controls a procedure for which there is a potential of fraud, bribery, or corruption to occur you should contact the Trusts Local Counter Fraud Specialist (LCFS) for assistance.

Appendix 1 Training Needs Analysis

Training topic:	Privacy Officer	
Type of training: (see study leave policy)	☐Mandatory (must be on mandatory training register) ☒Role specific ☐Personal development	
Division(s) to which the training is applicable:	☒Adult Mental Health & Learning Disability Services ☒Community Health Services ☒Enabling Services ☒Families Young People Children ☐Hosted Services	
Staff groups who require the training:	*Those individuals designated through their Clinical Safety Officer as a Privacy Officer within the EPR SystmOne*	
Regularity of Update requirement:	Once	
Who is responsible for delivery of this training?	CSO	
Have resources been identified?	Yes	
Has a training plan been agreed?	Yes	
Where will completion of this training be recorded?	☒ULearn ☐Other (please specify)	
How is this training going to be monitored?	Report from Learning Management System	
Signed by Learning and Development Approval name and date		Date:

Appendix 2 The NHS Constitution

- The NHS will provide a universal service for all based on clinical need, not ability to pay.
- The NHS will provide a comprehensive range of services.

Shape its services around the needs and preferences of individual patients, their families and their carers	☐
Respond to different needs of different sectors of the population	☐
Work continuously to improve quality services and to minimise errors	☒
Support and value its staff	☐
Work together with others to ensure a seamless service for patients	☐
Help keep people healthy and work to reduce health inequalities	☐
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	☒

Appendix 3 Stakeholders and Consultation

Key individuals involved in developing the document.

Name	Designation
Chris Biddle	LHIS Cyber Security Manager
Simon Jones Samantha Rogers Gurpal Singh	LHIS IM&T Business Manager – CHS LHIS IM&T Business Manager – DMH LHIS IM&T Business Manager - FYPC
Afroz Kidy	LHIS Security, RA & Assurance Manager
Claire Mott	Records Exploitation Manager
Pat Upsall	CHS Clinical Safety Officer
Tom Gregory	Clinical Safety Officer/DMH IM&T Clinical Lead
Ruth North	FYPC&LDA Clinical Safety Officer

Circulated to the following individuals for comment.

Name	Designation
Data Privacy Group	Various

Appendix 4 Due Regard Screening Template

Section 1	
Name of activity/proposal	Clinical Systems Access and Confidentiality Audit Policy
Date Screening commenced	04/07/2024
Directorate / Service carrying out the assessment	Enabling/Data Privacy
Name and role of person undertaking this Due Regard (Equality Analysis)	Sarah Ratcliffe, Head of Data Privacy
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: To provide clear instruction around the processes for assigning access to systems and monitoring the activity against those systems in line with Data Protection Requirements	
OBJECTIVES: Provide clear instruction on the process for providing access to systems. Provide clear instruction on the processes and escalation of monitoring and audit of systems	
Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact, please give brief details**
Age	No impact
Disability	No impact
Gender reassignment	No impact
Marriage & Civil Partnership	No impact
Pregnancy & Maternity	No impact
Race	No impact
Religion and Belief	No impact
Sex	No impact
Sexual Orientation	No impact
Other equality groups?	
Section 3	
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.	
Yes	No
High risk: Complete a full EIA starting click here to proceed to Part B	Low risk: Go to Section 4.☒
Section 4	

If this proposal is low risk please give evidence or justification for how you reached this decision:			
The Policy is designed to ensure that the security and confidentiality of patient information held in the Trusts' electronic patient record is maintained and access monitored to ensure compliance with staff responsibilities for maintaining confidentiality.			
Signed by reviewer/assessor	SRatcliffe	Date	04/07/2024
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed		Date	

Appendix 5 Data Privacy Impact Assessment Screening

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy. The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.		
Name of Document:	Clinical Systems Access and Confidentiality Audit Policy	
Completed by:	Sarah Ratcliffe	
Job title	Head of Data Privacy	**Date 04/07/2024**
Screening Questions	**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	No	
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	Yes	Where a disciplinary issue is identified
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No	
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	No	
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	Yes	Where a disciplinary issue is identified
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise	No	

privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.		
8. Will the process require you to contact individuals in ways which they may find intrusive?	No	
If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.		
Data Privacy approval name:	Sarah Ratcliffe, Head of Data Privacy	
Date of approval	04/07/2024	

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust

Appendix 6 Request for Audit form

Please complete all sections

The request must be approved by the Information Asset Owner (Clinical Service Director)

Please complete sections 1-5 and email to lpt.dataprivacy@nhs.net

1. The Person the audit is to be carried out on:

Name:	
Job Title:	
Base:	

2. System to be audited:

Email:	
Internet:	
SystmOne Unit:	

3. Background reasons for the request:

4. Specifics of audit requested: e.g. times, dates, patient IDs

5. Person requesting the audit

Name:	
Job Title:	
Designation to the above person:	
Contact details:	

Information Asset Owner Authorisation:	An authorisation email can be sent from the authorising IAO to lpt.dataprivacy@nhs.net

Please note:

LHIS staff with treat this as a matter of strict confidence. In some cases, they will need to remove the PC or Laptop concerned for investigation. From the time your request is logged, LHIS staff will keep a written notes of action taken, which will form an audit trail.

LHIS staff can provide advice/evidence from a technical perspective only.

If you have any questions about how the evidence should be treated in regard to a disciplinary policy/investigation, please contact HR.

** Following questions to be completed by the Data Privacy Team **

6. Is the request approved

Date request received:	
Audit Request Reference:	
Is audit approved?:	Yes No – Reason?

7. Feedback from Audit findings

Appendix 7 Non-substantive staff access (LPT Bank and Agency Workers) Emergency Only Temporary Access to SystmOne