Essex Partnership University
NHS Foundation Trust

CONFIDENTIALITY AUDIT PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG59c
VERSION NUMBER:	2 (old numbering v4)
KEY CHANGES FROM PREVIOUS VERSION	Three year review
AUTHOR:	Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Committee; Caldicott Network; Clinical / Operational Leads
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	May 2021
LAST REVIEW DATE:	May 2021
NEXT REVIEW DATE:	May 2024
APPROVAL BY IGSSC	April 2021
RATIFICATION BY QUALITY COMMITTEE:	May 2024
COPYRIGHT	

PROCEDURE SUMMARY

These procedural guidelines will ensure that all staff are aware of the monitoring of access to Trust systems in regard of patient, staff, general wider public information / data that occurs and which ensures that processes are in place to highlight actual or potential confidentiality breaches in systems.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

Auditing and Datix reporting to monitor the compliance with confidentiality across the Trust.

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is The Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONFIDENTIALITY AUDIT PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONFIDENTIALITY AUDIT PROCEDURE

Assurance Statement

These procedural guidelines will ensure that all staff are aware of the monitoring of access to Trust systems in regard of patient, staff, general wider public information / data that occurs and which ensures that processes are in place to highlight actual or potential confidentiality breaches in systems.

Please read in conjunction with the Data Protection Act 2018 and Confidentiality Policy and associated procedures.

1.0 INTRODUCTION

1.1 Advances in electronic management of health and employment records / information within the NHS has resulted in the requirement to monitor access to such confidential systems and therefore the information governance agenda requires that all organisations that handle person identifiable information have arrangements in place to manage and safeguard confidentiality.

1.2 As large numbers of staff use these systems it is imperative that access is monitored and controlled and the Trust should, therefore, as best practice, have processes to highlight actual or potential confidentiality breaches in their systems, particularly where person identifiable information is held.

2.0 SCOPE

2.1 These procedures must be adhered to by all staff (including permanent/contract/agency/locum/trainees etc.) using Trust information systems / processes where person identifiable information / data is held.

2.2 This procedure covers all forms of information / data, including paper, electronic, digital, etc.

3.0 RESPONSIBILITIES

3.1 Caldicott Guardian / Deputy Caldicott Guardian

3.1.1 The Caldicott Guardian will be informed of any serious breaches of confidentiality in regard of patient identifiable information and act accordingly.

3.2 Senior Information Risk Officer / Deputy Senior Information Risk Officer

3.2.1 The Senior Information Risk Officer will be informed of any breaches of confidentiality in regard of person identifiable information and act accordingly.

3.3 Information Governance Manager

3.3.1 The Information Governance Manager will, in conjunction with the appropriate managers / leads for the individual systems set up processes for undertaking the monitoring audits on a regular basis (i.e. annually/bi-annually/quarterly/bi-monthly/monthly).

3.3.2 The key leads will provide reports to the Information Governance Manager on the outcomes of these audits and advise of any anomalies which may be considered breaches for investigation, and where processes may need to be changed or improved.

3.3.3 The Information Governance Manager will ensure that the Caldicott Guardian and / or Senior Information Risk Officer are apprised on breaches, investigations and outcomes, as appropriate, providing advice and guidance where necessary.

3.3.4 The Information Governance Team is responsible for the definition, implementation and monitoring of the Information Asset Register (IAR).

3.4 Privacy Officer

3.4.1 The Information Governance Manager is the designated Privacy Officer for the Trust.

3.4.2 The Privacy Officer will receive automatic alerts concerning access to the systems / processes where a legitimate relationship does not exist.

3.5 Data Protection Officer

3.5.1 The Data Protection Officer is responsible for:

- Ensuring that appropriate data protection Act notifications are maintained for applicable Trust's systems and information.
- Dealing with enquiries, from any source, in relation to the Data Protection Act and facilitating advice and support relating to formal subject access requests.
- Advising users of information systems, applications and networks on their responsibilities under the Data Protection Act, including subject access requests.

3.6 Information Security Officers

3.6.1 The Associate Director of IT Strategy & Technical Projects is the Trust's designated Information Security Manager.
They will work closely to ensure the implementation of information governance / security practices across the organisation.
Attending the Information security Forum on a regular basis and through the Forum maintaining the Trust's Security risk register.

4.0 MONITORING ACCESS TO CONFIDENTIAL INFORMATION

4.1 In order to provide assurance that access to person identifiable information 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.

4.2 The Information Governance Team and the Caldicott Guardian / Senior Information Risk Officer will decide on any actions to be taken to address anomalies identified, through the implementation of, for example:

- Additional controls
- Restriction of access
- Investigation
- Presentation of investigation outcomes with recommendations for further action such team working processes, recommended disciplinary action, additional training needs etc.

Outcomes of these discussions and actions to be taken will be fed back to the key leads by the Information Governance Team.

4.3 Any anomalies (evidence of improper use of systems / libraries; change of role requiring adjustment to access, etc.) – will be reported via Datix and investigation through the normal channels of information incidents investigation (see also Reporting Information Incidents procedure).

4.4 Monitoring will include, but not be limited to, review / audit of:

- Failed attempts to access person identifiable information by an unauthorised person/s
- Repeated attempts to access person identifiable information by an unauthorised person/s
- Successful access of person identifiable information by unauthorised person/s
- Evidence of shared login sessions / passwords
- Access to potential family and friends / neighbours and colleagues information
- Creating / deleting / altering records for the purposes of inappropriate use and without approval
- Overriding consent

4.5 Monitoring will take place across a range of systems / access routes to person identifiable information, for example:

- PARIS
- Intranet Client Information
- Smart Card access

- ESR (Electronic Staff Records)
- Paper Records (from records tracer)
- SystmOne
- Mobius
- Networks
- Closed account emails / open account (leavers)

This list is not-exhaustive.

4.6 Monitoring will consist of random checks within the systems (as above 4.5).

4.7 Breaches of confidentiality, reported via Datix, will be investigated and the Trust systems may be interrogated as part of that investigation to identify whether unauthorised access has occurred.

4.8 In addition the Information Governance Team will regularly carry out spot-check audits of services, teams to review compliance to Trust policy, local and national guidance around the protection of information / data / systems.

4.9 Results of all audits are fed back to the team managers, where anomalies, breach of confidentiality or non-adherence to policy is identified for further action and investigation. The outcome of the investigations will be reported back to the Information Governance Team.

4.10 All suspected breaches / unauthorised access to confidential information systems will be investigated. This may result in further investigation under the Trust's disciplinary or conduct & capability procedures.

5.0 MONITORING AND REVIEW

5.1 These procedural guidelines will be monitored and reviewed in line with Trust policy, every three years and / or in line with changes to national / local guidance.

5.2 Compliance to this procedure will be undertaken in line with Trust policy and timetables for compliance audits.

5.3 The Caldicott Network and Information Governance Steering Committee will have overall responsibility for overseeing the implementation of these procedural guidelines.

6.0 REFERENCE OTHER DOCUMENTATION

- Trust Information Governance & Security Policy and associated procedures
- Trust Records Management Policy and associated procedures
- NHS Information Governance Toolkit
- NHS Confidentiality Code of Conduct

- Registration Authority Governance Arrangements for NHS Organisations
- Caldicott Principles
- Data Protection Directive
- Data Protection Act 2018
- Computer Misuse Act 1990
- Health & Social Care Act 2012
- Human Rights Act 1998
- NHS Constitution
- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulation

This list is not exhaustive.

END