Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

CONFIDENTIALITY AUDIT POLICY

POLICY

Reference	IG/003		
Approving Body	Information Governance Committee		
Date Approved	30th January 2023		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	February 2023		
Version	5.0		
Summary of Changes from Previous Version	Fact-find procedure		
Supersedes	4.0		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group		
Date of Completion of Equality Impact Assessment	12th January 2023		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	UK General Data Protection Regulation Data Protection Act 2018 Human Rights Act 1998 Common law duty of confidentiality Regulation of Investigatory Powers Act 2000 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 The Network and Information Systems Regulations 2018 Computer Misuse Act 1990		
Target Audience	All staff		
Review Date	30/01/2025		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Jacquie Widdowson, Information Governance Manager and Data Protection Officer		
Lead Division/ Directorate	Corporate		

Lead Specialty/ Service/ Department	Information Governance
Position of Person able to provide Further Guidance/Information	Information Governance Manager and Data Protection Officer

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Information Security Policy	December 2022
Template control	June 2020

CONTENTS

APPENDICIES

1.0 INTRODUCTION

The National Health Service (NHS) Care Record Guarantee[1] and Confidentiality NHS Code of Practice[2] requires that all NHS organisations put in place mechanisms to ensure that confidential patient information is protected. This requires access to confidential information to be monitored and audited locally and, in particular, requires that there are agreed procedures for investigating confidentiality alerts.

It is also a requirement of the NHS Digital's Data Security and Protection Toolkit (DSPT)[3] that the Trust establishes appropriate confidentiality audit procedures to monitor access to confidential patient information. Therefore, the Trust has a proactive programme of system audits, acting as both a deterrent and a means of identifying potential violations to patient/staff confidentiality through inappropriate use of systems.

The Human Rights Act 1998, Article 8 relates to the right of Privacy. If information is inappropriately disclosed the individual can take legal action for breach against the public body concerned. Not only must patient information be held confidentially, but it must also be held securely. Failure to do so will also breach the right to respect for private life

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 Data Protection legislation, the Human Rights Act 1998 and the common law duty of confidentiality.

2.0 POLICY STATEMENT

Systems used by the Trust represent a considerable investment. Much of the information is of a confidential and sensitive nature, and it is necessary for all information systems to have appropriate protection against any events whether accidental or malicious, which may put at risk the activities of the Trust or the investment in information.

The Trust has a responsibility to maintain the confidentiality, integrity and availability of information held both manually and electronically.

- Confidentiality - Data is available to those with specific authority who require access; Data is not disclosed to people who do not require it.
- Integrity - is about information being accurate and up-to-date. Systems must be designed so that the input and management of information is not prone to human error and that the flow of

[1] https://www.happyhealthylives.uk/download/clientfiles/files/Care-Record-Guarantee.pdf
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
[3] https://www.dsptoolkit.nhs.uk/

information does not result in loss or alteration. Data should be complete and accurate and not tampered with during or after submission. Ensuring that during the process of transmission data integrity is maintained.

- Availability – is about information being there when it is needed to support care. System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing healthcare. Data is available and delivered to the right person, at the time when it is needed and that there is accessibility to systems at all times. Having safeguards in place for power outages, natural disasters, hardware failures and systems upgrades.

This document sets out the appropriate confidentiality audit procedure to monitor access to confidential patient/employee information. This includes:

- How access to confidential information 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 Officer (SIRO) and Caldicott Guardian, Information Governance (IG) Manager or Information Asset Owner (IAO).

Confidentiality audits will focus primarily on controls within electronic systems but should not exclude paper records 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 carrying out audits relating to inappropriate access to confidential patient/employee information within the Trust. The Trust must ensure that confidential patient/employee information is only accessible to staff who need it for their current role and that access is removed as soon as it is no longer required. The Trust must operate on a least privilege principle so that staff do not have access to data they have no business need to see. For the avoidance of doubt this includes inappropriately accessing records of individuals with whom staff do not have a legitimate relationship ie patient, clinician. ,

With advances in the electronic management of information within the NHS, the requirement to monitor access to personal confidential information 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 relationship and a legal right to access it.

3.0 DEFINITIONS/ ABBREVIATIONS

CQC	Care Quality Commission
DoH	Department of Health & Social Care
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
DSPT	Data Security and Protection Toolkit
NCRS	NHS Care Record Guarantee
SIRO	Senior Information Risk Owner

4.0 ROLES AND RESPONSIBILITIES

Caldicott Guardian

It is a requirement for all NHS organisations to appoint a Caldicott Guardian, who must be a senior person within the organisation. The Medical Director is the Trust's appointed Caldicott Guardian and has overall responsibility for protecting the confidentiality of people's health and care information and making sure that it is used appropriately. The SIRO and Caldicott Guardian will be informed where serious breaches occur, they will also be updated with the findings of any confidentiality audits and ensure that appropriate action is taken.

The Caldicott Guardian will also be responsible for ensuring that access to personal confidential information remains relevant and is regularly audited within the Trust.

Information Governance Department

The role of the Information Governance Manager/Data Protection Officer is to help ensure the Trust's handling and sharing of personal data is undertaken in a confidential and secure manner, to appropriate ethical, professional and legal standards.

They will provide advice or participate in the investigations of breaches of confidentiality as required.

People Directorate

Will be informed where serious breaches occur, requesting confidentiality audits where applicable supporting leaders to manage staff where breaches occur via Human Resources Policies and Procedures.

Information Asset Owners / System administrators

Information Asset Owners (IAOs) are responsible for ensuring that access to confidential patient/employee information is secure and strictly controlled within their Divisions/Departments.

Monitoring of clinical systems should be carried out by the responsible administrator/manager, such that instances of alleged inappropriate access or misuse of confidential information can be identified and reported to the IG department for action to be taken. Support on how and when to conduct a confidentiality audit will be provided by the IG department.
Access to confidential patient/employee information 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 additional access being given.

Requests to audit a user will only be provided to IT Services (Nottinghamshire Health Informatics Service – NHIS) and System Administrators once the request has been authorised and sanctioned by both the information governance department and the Operational People Directorate Team.

All Staff
Staff may also report concerns relating to potential breaches of confidentiality, which may result in an audit of user access and activity on the relevant Trust system(s).

All investigations and outcomes will be recorded by the IG department and passed on to the relevant Division /Specialty and/or operational People Directorate for further action, which may include an initial fact-finding meeting, and potentially disciplinary investigation and action against the member(s) of staff involved, the implementation of additional controls, or other remedial action as necessary.

Actual or potential breaches of confidentiality should be reported to the IG department immediately and an incident report completed on the Trusts incident reporting system (Datix).

All staff, whether permanent, temporary or contracted, should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality.

5.0 APPROVAL

The Confidentiality Audit Policy will be approved at the Trust's IG Committee.

6.0 MONITORING AND AUDITING ACCESS TO CONFIDENTIAL INFORMATION

All work areas within the Trust which processes confidential information will be subject to a confidentiality audit.

In order to provide assurance that access to confidential 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. This will be achieved by putting in place arrangements for both proactive and reactive auditing of access to confidential information and communicated to all staff.

Proactive Monitoring

This will generally be achieved for systems where an automated function exists for the alerting of user access to records for subsequent review by someone with Caldicott Guardian, SIRO, IAO or Information Governance roles within the system.

Examples of proactive monitoring on systems accessed by Trust staff include;

- Summary Care Record (SCR)
- SystmOne
- Orion.

Automatic system alerts are generated when staff override any of the privacy controls that are in place.

These alerts will prompt the receiving staff member to establish if the access was justified or potentially inappropriate, which will warrant further investigation. A proportionate sample size of alerts will need to be reviewed on a monthly basis.in

Privacy monitoring tools will also be used for proactive monitoring of staff access to (records and systems. the monitoring tool will review staff access to identify suspicious and potentially inappropriate patterns of access for further investigation by the Information Governance department. The outcome of these reviews will be escalated to People Directorate for further investigation as appropriate.

Reactive Monitoring

Reactive confidentiality audits will generally fall into 2 scenarios:

1. Misuse of system access is alleged in relation to data breaches ie inappropriate access, confidentiality.
2. Evidence is required to support line manager concerns/investigations about staff conduct, e.g. excessive use of the Internet, email activity or conduct (where the primary concern is not about a breach of privacy/confidentiality however the audit information may have privacy implications). Line manager concerns/ investigations will also be covered under the relevant policies (i.e. Information Security Policy and Email and Internet Policy.

7.0 CONFIDENTIALITY AUDIT AND ESCALATION PROCESS

The response to an IG breach will be considered on an individual basis.

Where an audit of user activity or access to records is required as part of a fact-find, the request should be initiated by the line manager or an appropriate senior manager. The People Directorate may also request audits. Audit requests must include a brief outline of the report/allegation and information required, giving justification of the relevance of the audit information to the investigation.

The form located in Appendix A must be completed for all audit requests and forwarded to the IG team sfh-tr.information.governance@nhs.net or directly to the IG Manager/ Data Protection Officer for review and authorisation. The IG team will ensure that a legitimate and lawful reason for access to the information is provided. Consent will be obtained if appropriate. Caldicott Principles must be adhered to at all times, with only the relevant and minimum information being shared regarding the need for the audit.

Approved requests will be sent to appropriate system administrators in the Trust for processing.

Upon completion of the audit, system administrators will provide the audit report to the IG team to review and remove any irrelevant information and feed back to the line manager. It is important that audit reports are only seen by as few staff as possible; likewise, the audit report must be kept secure.

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/passwords and smartcards
- Inappropriate communications with patients
- 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.

Investigating Confidentiality Events and Alerts

The Information Governance team, where required, will be responsible for liaising with the People Directorate to co-ordinate investigations into confidentiality breaches.

Investigation and management of confidentiality events and alerts will be in line with the Trust's Disciplinary Policy and Data Protection, Confidentiality and Disclosure Policy.

Inappropriate Access to Systems

Staff who have inappropriately accessed a record will receive a 'soft' or 'hard' letter, depending on the individual situation, reinforcing the requirement to adhere to Information Governance policies and procedures at all times. The letter advises that a further repeat of this could result in a Fact Finding exercise or formal Disciplinary action.

Staff who have inappropriately accessed a record and receives a 'hard' letter will be issued with an invite to meet to undertake a fact-finding exercise to ascertain the reasons behind accessing the record. On completion of the fact find, the information will be reviewed and a decision will be made regarding the next steps. One outcome of the fact find could be that it proceeds to a formal investigation under the Trust's Disciplinary policy.

Providing Audit Information To Patients/Service Users

Both the National Information Board in 'Personalised Health and Care 2020' and Dame Fiona Caldicott in the 'Report of the Caldicott2 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 health records can be made available in a suitable form to service users on request. All requests of this nature need to be directed to the IG team

8.0 MANAGEMENT OF DATA BREACHES (IG INCIDENTS)

The IG team proactively monitor data breach incidents logged in the Trusts incident reporting system, Datix. The IG team will review, provide guidance and follow up all data breach incidents to ensure a satisfactory outcome in liaison with investigators. More serious data breach incidents are recorded on NHS Digital's Data Security and Protection Toolkit.
All data breaches are reported to the IG Committee, which will escalate any unsatisfactory outcomes to Audit and Risk Committee and communicate pertinent IG issues/messages to staff using, for example, Trust Briefing and intranet notice board bulletins/icare2. Trends in incidents will be monitored in order to learn lessons and provide continual service improvement.

9.0 RELEVANT POLICIES AND PROCEDURES

- Corporate Records Policy
- Data Protection, Confidentiality and Disclosures Policy
- Data Quality Policy
- Disciplinary Policy
- Internet and Email and Internet Policy
- Freedom of Information Act Policy and Procedure
- Health Records Management Policy
- Information Governance Policy
- Information Security Policy

- Retention and Destruction Policy.

10.0 EQUALITY AND DIVERSITY STATEMENT

All patients, employees and members of the public should be treated fairly and with respect, regardless of age, disability, gender, marital status, membership or non-membership of a trade union, race, religion, domestic circumstances, sexual orientation, ethnic or national origin, social & employment status, HIV status or gender re-assignment.
All trust policies and trust wide procedures must comply with the relevant legislation (non-exhaustive list):

- Code of Practice on Age Diversity in Employment (1999)
- Disability Discrimination Act (1995)
- Employment Equality (Age) Regulations 2006
- Employment Equality (Religion or Belief) Regulations 2003
- Employment Equality (Sexual Orientation) Regulations 2003
- Employment Relations Act (1999)
- Equal Pay Act (1970 and amended 1983)
- Equality Act (Sexual Orientation) Regulations 2007
- Fixed Term Employees - Prevention of Less Favourable Treatment Regulations (2001)
- Health & Safety at Work Act 1974
- Human Rights Act (1998)
- Part Time Workers - Prevention of Less Favourable Treatment Regulations (2000)
- Race Relations (Amendment) Act 2000
- Rehabilitation of Offenders Act (1974)
- Sex Discrimination Act (1975 amended 1986)
- Trade Union and Labour Relations (Consolidation) Act 1999.

11.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Staff access to systems	Information Governance Manager & Data Protection Officer	Staff monitoring of systems and audits	Ad-hoc	Information Governance Committee

12.0 TRAINING AND IMPLEMENTATION

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[4] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation
A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[5]

13.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document has not been subject to an Environmental Impact Assessment.

14.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:
- Computer Misuse Act 1990
- Confidentiality: NHS Code of Practice 2003
- Data Protection Act 2018
- Human Rights Act 1998
- NHS Care Record Guarantee
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- UK General Data Protection Regulation

[4] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[5] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/

Related SFHFT Documents:

- Corporate Records Policy
- Data Protection, Confidentiality Policy and Procedure
- Freedom of Information Act Policy
- Health Record Keeping Policy
- Health Records Management Policy
- Information Security Policy
- Retention and Destruction Policy and Procedure

15.0 KEYWORDS

Personal confidential data, data, information, availability, integrity, confidentiality.

16.0 APPENDICES

- List of appendices are provided in the contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: CONFIDENTIALITY AUDIT POLICY			
New or existing service/policy/procedure: EXISTING			
Date of Assessment: 12th January 2023			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None

Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None

What data or information did you use in support of this EqIA?

- Trust guidance for completion of equality impact assessments

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

- No

Level of impact
Low Level of Impact

Name of Responsible Person undertaking this assessment:
Gina Robinson

Signature:

Date: 12th January 2023

APPENDIX 2: APPROVAL FOR STAFF MONITORING – AUDIT DATA

Name & Job Title of Requester	
Date of Request	
Name & Job Title of the employee	
Detail the information that is required (eg require all websites accessed between May and June this year) Access to what systems	
What is the justification for requesting audit data? E.g. required as part of an investigation by People Directorate.	
Are you the lead investigator?	
Is this part of a People Directorate investigation, fact-find?	
Is this a breach of Health & Safety that could jeopardise other workers	
Why do you require the information and how will the information be used and for what purpose	
Is this in relation to Criminal Activity at work or gross misconduct (please indicate severity)	
What is the timescale for the data to be provided?	
Has the member of staff been informed where the audit data may have privacy implications for the individual concerned (e.g. if emails are to be searched in the absence of the employee)? If no, then explain why.	

Signature of service lead/ Deputy Director of People Directorate :
IG Authorise or Decline:
Reason for decision:
Date:

Please Note: The information produced as part of this investigation monitoring may be required to be retained on the workers file.