Public – To be published on the Trust external website

Title: Monitoring and Auditing Service User Confidentiality

Ref: CORP-0063-v2.1

Status: Approved
Document type: Procedure

Document lead responsibilities (to be deleted on completion of this document)

No.	Who	What	New documents	Amended documents
1	Document Lead	Identify the need to develop a new document/change an existing document	✓	✓
2	Document Lead	Start the Equality Analysis process. Read the equality analysis policy and the equality analysis guidance which can be located on the policies page on the intranet. Ensure language is consistent with OJTC values and follow Policies and procedures – guidance for writers.	✓	✓
3	Document Lead	Please contact the Equality, Diversity and Human Rights Team by email tewv.eandd@nhs.net to make your appointment to discuss your document's Equality Impact Assessment	✓	✓
4	Document Lead	Draw up a list of stakeholders/people/bodies you may need to consult for questions on legal matters, process, terminology etc.	✓	✓
5	Document Lead	Identify who has final approval of the document	✓	✓
6	Document Lead	Develop document using the template	✓	✓
7	Document Lead	Complete the Equality Analysis (EA) screen form (Appendix 1)	✓	✓
8	Document Lead	Submit the completed procedure to the Policy Manager for QA check and EA review	✓	✓
9	Document Lead	Submit the procedure to the relevant sub-group for approval (see Governance of Policies)	✓	✓
10	Policy Manager	Publishes via intranet and, when authorised, external website	✓	✓
11	Document Lead	Disseminate and request implementation of policy/procedure	✓	✓

Contents

1 Introduction

Paris is the Trust's electronic patient record system. Access to Paris is given to staff that have a legitimate need to view and/or record clinical information for their role. Staff access to the system is approved by their line manager.

This procedure provides guidance to be followed by every person who is authorised by the Trust to use the electronic patient recording (EPR) systems such as Paris (and other associated systems) and the national Summary Care Record (SCR).

Strategic goal 1: To co-create a great experience for patients, carers and families

The Data Protection Act 2018 and Freedom of Information Act 2000, which underpin all aspects of information governance, give transparency to all aspects of the way that information is processed within the Trust.

Implementing this procedure provides assurance to patients that when records are accessed there is a legitimate business need for this access.

Importantly, patients may request a report on which staff have accessed their records. This leads to transparency and openness in the way that staff are accessing patient information.

2 Purpose

Following this procedure will help the Trust to:-

- Comply with the requirement of lawfulness of processing personal data under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018).
- Demonstrate that effective control mechanisms are in place to safeguard confidentiality;
- Demonstrate the principles laid down within the National Care Record Guarantee which operates within a privacy framework that makes twelve commitments. In particular within commitment number 2 it states *"everyone looking at your record, whether on paper or computer, must keep the information confidential. We will aim to share only as much information as people need to know to play their part in your healthcare".*
- Comply with assertion 6.1.3 of NHS Digital's Data Security and Protection Toolkit.

Following this procedure will help Trust staff/ system users to:-

- Comply with the Data Protection Act 2018 (GDPR) and UK GDPR;
- Comply with the common law duty of confidentiality;
- Comply with the Computer Misuse Act 1990
- Comply with the relevant Trust policies;
- Comply with the Health & Social Care Information Centre code of practice on confidential information.
- Adopt an open and transparent culture relating to accessing records.
- Provide assurance to patients that staff access to records is monitored.
- Enhance patient confidentiality and trust.

3 Who this procedure applies to

- This procedure is actioned by the Privacy Officer.
- All staff access to Paris is monitored by the Privacy Team.
- The existence of this procedure makes staff responsible for their access to patient information.
- Staff must respect patient information by only accessing records with a legitimate business need.

4 Related documents

This procedure describes what you need to do to implement section 6.3.5 of the Information Governance Policy – Privacy Officer Standard Operating Processes.

The Information Governance Policy defines confidentiality which you must read, understand and be trained in before carrying out the procedures described in this document.

This procedure also refers to:-

- Information Governance Policy
- Confidentiality and Sharing of Information Policy
- Information Security and Risk Policy
- Access to Information System Policy

5 Procedure

5.1 The Law That Regulates This Procedure

Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). [Data Protection Act (DPA) 2018 (UK GDPR) Article 5 1(f)]

The Trust regards all personal identifiable information relating to patients as 'special' (Article 9 GDPR) and confidential, with disclosure on a strict 'need to know' basis within and outside of the Trust. [Data Protection Act (DPA) 2018 (UK GDPR) Article 12].

All staff who use patient records are made aware of their responsibility for facilitating and maintaining confidentiality of those records. Systems and processes ensure that employees only have access to those records necessary to carry out their role. Access to records is logged and periodically audited to ensure staff are complying with the common law duty of confidentiality.

Staff are made aware of the Trust's security measures put in place to protect all health records. The Trust has policies and procedures in place to ensure compliance together with disciplinary measures for failure to comply.

The Trust will establish and maintain procedures to monitor and investigate all reported instances of actual or potential data loss or confidentiality breach incidents, details will be included in annual reports. Some incidents will be reported to the Information Commissioner's Office through NHS Digital's Data Security and Protection Toolkit.

5.2 Trust Commitment to NHS Standards

The Trust adopts the principles laid down within the National Care Record Guarantee. This operates within a privacy framework that makes twelve commitments. In particular within commitment number 2 it states *'everyone looking at your record, whether on paper or computer, must keep the information confidential. We will aim to share only as much information as people need to know to play their part in your healthcare'.*

Where information is shared without permission we will make sure that we adhere to the Data Protection Act 2018 (UK GDPR), the HSCIC code of practice on confidential information and other national guidelines on best practice.

5.3 Additional Relevant Legislation and Policies

Often, when a servicer user's confidentiality is breached, other policies, codes and acts of law have also been contravened in addition to the Data Protection Act 2018 (UK GDPR), such as:

- Computer Misuse Act 1990 (as amended 2006)
- Confidentiality and sharing information policy
- Information Governance Policy
- Professional Code of Confidentiality
- Access to Information Systems Policy
- Information Security and Risk Policy

5.4 DPA Requirements for Monitoring and Auditing

This procedure focuses primarily on controls within electronic patient recording systems. Controls on paper records are stipulated in the Records Management Policy and Records Management Procedures.

5.5 Break Glass Security

The Trust uses an open system, Paris, on which to store clinical records. To protect service users' data and to comply with legal requirements, the Break Glass function was introduced.

Break Glass security controls the access to all service users' electronic records on Paris based on legitimate relationships and team access. If a member of staff or a system user tries to open a record that is not in their team's caseload, they will be challenged and asked to give a reason before the record is accessed.

A member of staff or a system user who has been set up on a team that is currently delivering care to a service user will not be challenged to go through the 'Break Glass' security as their legitimate access is already confirmed. If a member of staff or a system user is **not** in a team currently delivering care for the service user, a Break Glass window will be presented. In order to continue to access the record, the system user needs to select a reason code from the dropdown list and make an entry in the details box to describe what information they need to access and why such information is needed.

Since the control is based on the legitimate relationship of the member of staff or system user, the legitimate relationship with the service user ends once the referral/s for the team/s they belong to have been closed. Over the course of time, it will not be uncommon to be challenged on accessing a record for a patient when the team is resuming care.

The member of staff or the system users are advised that as long as they have a legitimate reason for accessing a record then the system will not prevent them from doing this. It is acceptable to break glass and the member of staff or system users are encouraged to break glass so that they can deliver care or support the delivery of care to our service users.

Each completed record access attempt that is made via 'Break Glass' is recorded in the system. It is therefore important that the member of staff or the system users give the correct reason and provide accurate comments in the details box. This should prevent unnecessary investigations where there is a legitimate reason for viewing the record.

The term 'break glass' is also commonly used by other NHS trusts. Accessing a service user's Summary Care Record (SCR) on the NHS Spine Portal is also subject to a security process and this is also known as break glass. Refer to this leaflet for more information on access to the SCR.

Any member of staff given access to the system, whether on Paris or the SCR on the NHS Spine Portal, is bound by the code of confidentiality. Staff must follow all appropriate policies and procedures and adopt good working practices in relation to security and confidentiality of patient information. Failure to comply with these procedures may result in disciplinary action being taken against the member of staff. In the event that the system user is not a Trust staff member, the matter will be taken forward under the relevant authority.

5.6 The Close Monitoring Process

Another control process designed to protect the confidentiality of service users is 'Close Monitoring'. This can be applied when there is particular concern regarding potential unauthorised access to PARIS, for example where:

- a service user has concerns about the Trust holding their care records electronically;
- a member of Trust staff/ system user is accessing Trust services;
- a friend, family member of a service user or someone known to the service user works
- within the Trust;
- they are high profile service users (e.g., a celebrity) who may be of interest to staff

Any member of staff can raise a request for close monitoring but the request must be made through the relevant manager or clinician.

There are two ways to initiate close monitoring; a request or an alert. When close monitoring is initiated through a concern from a service user, this type of close monitoring is classified as a 'request'. In all other circumstances, the close monitoring is classified as an 'alert'.

A member of staff may become aware that someone they know might have been referred to the Trust; they should alert their line manager who may initiate a close monitoring request. This will signify a declaration of interest and will enable both staff and manager to mitigate any risk of unintentional or accidental confidentiality breach.

When close monitoring is requested by a service user, the Privacy Officer will send a confirmation letter to the service user. The Trust's privacy notice will be enclosed with the confirmation letter.

A close monitoring episode can last as long as the potential risk exists. It is always advisable to contact the Privacy Officer before initiating close monitoring so any risks can be fully identified and understood.

The Privacy Officer will audit the record on a regular basis. The frequency of audit will depend on the status of the referral and type of risk.

As long as the risk is considered to exist, the monitoring episode will remain open and will be audited on a regular basis.

The Privacy Officer will assess when a close monitoring episode may no longer be required. When this happens the Privacy Officer will liaise with the relevant clinician or team manager to determine if it is acceptable to close the close monitoring episode.

5.7 Monitoring, auditing and handling privacy breaches

The Trust's Privacy Officer is responsible for monitoring and auditing access to the electronic patient recording (EPR) systems.

Access to the electronic records of patients is on a strict 'need-to-know' basis. Access must be relevant to the staff member/ system user's role in the delivery, support or management of care of the service users or patients; the progress of the Trust's business; or supporting the Trust to comply with its legal requirements. This is known as a direct care function.

In the event that the break glass reason given is unclear or questionable; or the access found to be unjustifiable, the Privacy officer will investigate whether a privacy breach has occurred.

Any suspected privacy breach will be investigated. If the monitoring or auditing identifies any unauthorised access including access by error, the Privacy Officer will liaise with the line manager of the member of staff or the management body of the system user to ensure the incident is investigated and reported on Datix.

If unauthorised access is determined to be a potential privacy breach, the Privacy Officer will liaise with the line manager of the staff to invoke the Trust Disciplinary Policy and

Procedure. At this point, the Privacy Officer will report the incident to the Information Commissioner through the Data Security and Protection Toolkit Incident Reporting system within 72 hours.

When a privacy breach is confirmed, the Privacy Officer will, without undue delay, liaise with the care team manager of the service user/ patient to determine, based on their clinical judgement, whether the service user is well enough to be informed of the breach. The clinical decision shall be recorded in the patient's Paris record.

6 Terms and definitions

Term	Definition
Break Glass	• A security control within a clinical recording system protecting the confidentiality of the patients/service users.
Close monitoring	• A monitoring process applied to the access of records of a particular service user within the patient record system (Paris) on a regular basis to protect and assure confidentiality of the Trust's service users.
Information Commissioner's Office	• The UK's independent authority set up to uphold information rights (data protection and freedom of information) in the public interest, promoting openness by public bodies and data privacy for individuals.

Summary Care Record	• The SCR holds a defined set of key patient data for every patient in England except those who elect not to have one. The data comes from information held on GP clinical systems. The summary record helps to support the continuity of care across a variety of settings. The patient is asked for consent before their SCR is viewed unless it is an emergency situation where the patient is unconscious or cannot communicate. The SCR is in two parts; demographic information and medical information. Trust staff/system users currently access a patient's SCR for information on allergies, current prescriptions and adverse reactions to medicines.

7 How this procedure will be implemented

- This procedure will be published on the Trust's intranet and external website.
- Line managers will disseminate this procedure to all Trust employees through a line management briefing.
- All staff using electronic patient record systems must comply with the Break Glass requirements.
- The Privacy Officer will implement Close Monitoring on electronic patient records.

7.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All Paris Users	Paris	1 day	Once
All Summary Care Record Users	SCR E-learning	30 mins to 1 hour	Once

8 How the implementation of this procedure will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Number of privacy breaches reported on Datix	Quarterly	Digital Performance and Assurance Group (DPAG)
2	Number of privacy breaches reported on the NHS Digital Data Security and Protection toolkit	Quarterly	Digital Performance and Assurance Group (DPAG)
3	Number of privacy breaches under investigation by the Information Commissioner	Quarterly	Digital Performance and Assurance Group (DPAG)

9 References

Data Protection Act 2018
General Data Protection Regulation 2016
The Care Record Guarantee, *Our Guarantee for NHS Care Records in England,* Version 5 January 2011
Health and Social Care Information Centre code of practice on confidential information

10 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	23 March 2023
Next review date	23 March 2024
This document replaces	CORP-0063-v2
This document was approved by	Digital and Data Management Meeting
This document was approved	23 March 2023
This document was approved by	DPAG (virtual approval)
This document was approved	27 April 2023 (virtual approval)
An equality analysis was completed on this policy on	04 January 2023
Document type	Public
FOI Clause (Private documents only)	N/A

Change record

Version	Date	Amendment details	Status
2.1	27 Apr 2023	• Procedure placed on Our Journey to Change procedure template. • Checked links are working. • Checked content is up-to-date.	Approved

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Information Governance
Title	Monitoring and auditing service user confidentiality
Type	Procedure
Geographical area covered	Trust-wide
Aims and objectives	To ensure that staff are aware that access to electronic patient systems is monitored by the Privacy Officer.
Start date of Equality Analysis Screening	04/01/2023
End date of Equality Analysis Screening	04/01/2023

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	The procedure benefits staff and service users. Staff will understand that access is monitored and that they must have a legitimate business reason to access a record. Patients will have assurance that access to their personal information is monitored.
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO**

	• **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO**
Describe any negative impacts	Staff may be dismissed if it is found their access has breached patient confidentiality.
Describe any positive impacts	Patients are assured that their information is protected and any untoward activity will be monitored and acted upon

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	Information from NHSx regarding use of the Summary Care Record.
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	No
If you answered Yes above, describe the engagement and involvement that has taken place	Not applicable

If you answered No above, describe future plans that you may have to engage and involve people from different groups	No future plans.

Section 4	Training needs
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	None
Describe any training needs for patients	None
Describe any training needs for contractors or other outside agencies	None

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes / No / Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	yes	procedure
2.	**Rationale**		
	Are reasons for development of the document stated?	yes	
3.	**Development Process**		
	Are people involved in the development identified?	yes	
	Has relevant expertise has been sought/used?	no	
	Is there evidence of consultation with stakeholders and users?	no	
	Have any related documents or documents that are impacted by this change been identified and updated?	no	
4.	**Content**		
	Is the objective of the document clear?	yes	
	Is the target population clear and unambiguous?	yes	
	Are the intended outcomes described?	yes	
	Are the statements clear and unambiguous?	yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	yes	
	Are key references cited?	yes	
	Are supporting documents referenced?	yes	
6.	**Training**		
	Have training needs been considered?	yes	
	Are training needs included in the document?	yes	

	Title of document being reviewed:	Yes / No / Not applicable	Comments
7.	**Implementation and monitoring**		
	Does the document identify how it will be implemented and monitored?	yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	no	not yet, but it is planned
9.	**Approval**		
	Does the document identify which committee/group will approve it?	no	
10.	**Publication**		
	Has the policy been reviewed for harm?	yes	
	Does the document identify whether it is private or public?	yes	
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	