Public – To be published on the Trust external website

Records management and safe haven

Ref CORP-0026-007-v2

Status: Approved
Document type: Procedure
Overarching policy: Records Management Policy

Contents

1 Introduction

The term “Safe haven” encompasses all secure methods of transmitting or transferring confidential information.   A safe haven is a physical (such as a Post Room) or virtual (such as a server used by the Business Information team) location situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, we have committed to three goals.

The overarching Records Management Policy describes how managing different types of record within the Trust supports all three goals of Our Journey To Change. This procedure further supports these goals by maintaining the privacy and confidentiality of personal information and ensuring the security of data.

2 Purpose

Following this procedure will help the Trust to:-

- Maintain the privacy and confidentiality of personal information;
- Ensure compliance with legal requirements, especially concerning sensitive information (e.g. people’s medical condition);
- Give confidence to Trust staff, other Trusts or other agencies that personal information is being sent to a location which ensures the security of data. It is therefore essential that all departments and services within the Trust put in place adequate safe haven procedures to protect information, specifically:
    - At the point of receipt.
    - Whilst held by the department.
    - When transferring information to others, by whatever means.
    - When archived.
    - At the point of disposal.

3 Who this procedure applies to

This procedure provides:

- The legislative context and guidance which dictates the need for a safe haven
- A definition of the term safe haven
- When a safe haven is required
- The necessary procedures and requirements that are needed to implement a safe haven culture
- Who can have access and who you can disclose to

4 Related documents

- The Records Management Policy defines the legal duty to make sure records are managed and secure throughout their lifecycle.
- You must read and understand the Records Management Policy before carrying out the procedures described in this document.
- All staff are responsible for ensuring the protection of person identifiable information received into a safe haven.

This procedure also refers to:-

- ✓ Information Security and Risk Policy
- ✓ Information Asset Register Procedure
- ✓ Email policy
- ✓ Email procedure

5 Accessibility to safe haven area

If the location of a safe haven makes it impossible for a staff member with a disability to physically access the area, contact the information governance manager who will investigate and resolve the issue on an individual basis.

6 Where should safe haven procedures be in place?

- In any location where large amounts of personal information is being received held or communicated especially where the personal information is of a sensitive nature e.g. patient identifiable information.
- There should be at least one area following safe haven procedures on each of the Trust sites.

7 Legislation and Guidance

7.1 Data Protection Act 2018

66(1) of the Data Protection Act 2018 states:
Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.

7.2 Department of Health NHS Confidentiality Code of Practice

Annex A1 Protect Patient Information - *"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are as secure as they can be".*

8 Location/security arrangements

- It should be a room that is locked or accessible via a coded keypad only to authorised staff OR
- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any members of staff who work in the same building, or any visitors.
- If sited on the ground floor, any windows should have locks on them.
- The room must conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records containing person-identifiable information must be stored in locked cabinets.
- Computers must not be left on view or accessible to unauthorised staff and be either locked (if you plan to return) or switched off when not in use.

- Files and folders should always be saved and closed to allow for back-ups to be taken or in case of unexpected downtime.

9 Communications by telephone

Recorded telephone messages containing person identifiable or sensitive information, e.g. the names and addresses of applicants phoning for a job, or patient details, must be received into a secured, PIN-code protected voicemail box, so that only those entitled to listen to the message may do so.

A deputy should be appointed for times of absence, a group PIN code issued or an administrator password made available. Some areas use a messages book to note messages for absent staff members, this should also be stored securely.

10 Email

Many email systems (not NHSmail) are not secure which all staff are made aware of during induction training and training to use the NHSmail system.

Patient identifiable and other sensitive information must not be sent by email unless it has been encrypted to standards approved by the NHS. See the Email Procedure to identify which email addresses are secure, and for advice on the Trust-approved approach to sending sensitive information to non-secure email addresses.

If a patient expresses a preference to communicate by email, follow the guidance discussed in the Communicating with Service Users Best Practice guidance.

Emails containing confidential information must be stored appropriately on receipt e.g. incorporated within the health record, and deleted from the e-mail system when no longer needed.

11 Sharing information with other organisations (non NHS)

Employees of the Trust authorised to disclose information to other organisations must seek an assurance that these organisations have a secure point for receiving personal information.

The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 2018
- Common Law Duty of Confidence
- Department of Health NHS Confidentiality Code of Practice

Staff sharing personal information with other agencies should be aware that the Trust is a signatory to the *North East Information Sharing Guidelines* guidance which is applicable to all public sector organisations in the North East.

12 Definitions

Term	**Definition**
Safe haven	• "Safe haven" encompasses all secure methods of transmitting or transferring confidential information. • The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.
Personal information	• Information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and private address, name and home telephone number etc.
Sensitive information	Personal information which contains details of that person's: • racial and ethnic origin • offences and alleged offences • criminal proceedings, outcomes and sentences • trade union membership • physical or mental health details • religious or similar beliefs • sexual life • political opinions • genetic and biometric data For this type of information even more stringent measures should be employed to ensure that the data remains secure.

13 How this procedure will be implemented

- ⓘ Breaches of this policy will be investigated and treated as a disciplinary offence under the Trust's disciplinary procedure.

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.

This procedure will be reviewed every three years or more frequently if legislation or guidance from the Department of Health, the NHS Executive and/or the Information Commissioner changes.

13.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	Induction training	1 day	Once
All staff	Data Security and Protection Training for New Starters	2 hours	Once
All staff	Mandatory Data Security and Protection Training	1 hour	Annually

14 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	Routine audit and monitoring of compliance	Managers	Ongoing as part of normal operational management responsibilities
2	Spot checks of compliance and understanding of Data Protection, information confidentiality and security policies and procedures	Continuous programme of audit and spot checks by Information Governance staff	Digital Safety and Information Governance Board
3	Routine audit and monitoring of compliance	Managers	Ongoing as part of normal operational management responsibilities

15 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	02 November 2022
Next review date	02 November 2025
This document replaces	CORP-0026-007-v1 Records Management and Safe Haven
This document was approved by	Digital and Data Management Meeting
This document was approved	25 October 2022
This document was approved by	DPAG
This document was approved	02 November 2022
An equality analysis was completed on this policy on	27 June 2022
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1	June 2018	Renumbered to CORP-0026-007 from 13 June 2018	Published
2	02 Nov 2022	Full revision. Changes include:- • Updated introduction; • Addition of reference to Section 10 Email of – Communicating with service users best practice; • removal of reference to fax machines; • inclusion of virtual safe haven; • refreshed references to training needs analysis; and • revised equality analysis.	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	Digital and Data Services
Title	Records Management and Safe Haven
Type	Procedure/guidance
Geographical area covered	Trust-wide
Aims and objectives	• Maintain the privacy and confidentiality of personal information; • Ensure compliance with legal requirements, especially concerning sensitive information (e.g. people's medical condition); • Give confidence to Trust staff, other Trusts or other agencies that personal information is being sent to a location which ensures the security of data.
Start date of Equality Analysis Screening	17 March 2022
End date of Equality Analysis Screening	27 June 2022

Section 2	**Impacts**
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Patients, family members, carers, staff, third parties
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** • **Veterans** (includes serving armed forces personnel, reservists, veterans and their families **NO**
Describe any negative impacts	The physical location of a safe haven area may present barriers to accessibility for staff members with a disability
Describe any positive impacts	The procedure advises who to contact for support should the physical location of a safe have been a barrier to accessibility

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.)	Data Protection Act 2018 Department of Health NHS Confidentiality Code of Practice NHS Digital Records Management Code of Practice
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	n/a

If you answered No above, describe future plans that you may have to engage and involve people from different groups	NHS Digital Records Management Code of Practice underwent significant national consultation prior to publication. The Trust's Records Management Policy under which this procedure sits is based on the Code of Practice and itself underwent Trust-wide consultation. Trust staff comprise all protected characteristics.

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	n/a
Describe any training needs for patients	n/a
Describe any training needs for contractors or other outside agencies	n/a

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	
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?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
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?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
10.	**Publication**		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	Pubic
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	N/A	