Safe Haven Policy

Controlled document
This document is uncontrolled when downloaded or printed.

Reference number	WHHT: G031
Document type	Policy
Version	9
Author's name & job title	Nicola Bateman
Department/Speciality	Information Governance
Division	Information and Performance
Reviewed by	Informatics Group
Review date	18 November 2022
Approved by PGRG	12/12/22
Ratified by QSG	02/01/23
Next review date	Oct 2025
Target audience	All Staff
Search terms	Confidentiality, Data Protection, Privacy
Previous document name (if different)	

Contents

CONTRIBUTION LIST

Key individuals involved in developing this version of the document

Name	Designation
Nicola Bateman	Information Governance Manager
Approved by Committee	Informatics Group
Ratified by Committee	

CHANGE HISTORY

Version	Date	Author	Reason	Ratification Required
V2.0	Oct 08	Nicola Bateman	Updated to comply with NHS requirements	Yes
V3.0	Nov 09	Nicola Bateman	Updated section on Email. Added sections	Yes
V3.1	Jan 10	Nicola Bateman	Inserted section on – Transporting Paper records –	Yes
V4	Sep 11	Nicola Bateman	Inserted link on SMS text messaging	Yes
V4.1	May 12	Nicola Bateman	Inserted guidance on Answer Phones	Yes
V5.0	Jul 14	Nicola Bateman	Included Caldicott Principle 7	Yes
V6.0	Jul 15	Nicola Bateman	Added guidance on whiteboards, incoming & outgoing telephone calls. Many sections updated.	Yes
V7.0	Jun 17	Nicola Bateman	Amendments to Fax Guidance	Yes
V8.0	Sep 20	Nicola Bateman	Updates made to all sections to incorporate DPA18 and changes to NHS Mail and the decommissioning of fax machines	Yes
V9.0	Oct 22	Nicola Bateman	Minor changes	Yes

1. Introduction

The concept of 'safe havens' was introduced into the NHS in 1992 to protect the confidentiality of patient information transferred between organisations to support the payment of invoices for treatment.

In this context, a safe haven was a designated address or fax number where sending organisations could be assured that the information would be attended to promptly, that it would be disclosed only as necessary to process validation and payment, would be securely stored and in due course shredded or incinerated as confidential waste.

Since then, the recommendations of the Caldicott Report and more recently the Government's response to the Caldicott2 review, the concept has now been extended to cover all internal and external routine flows of patient-identifiable data.

This policy sets out the trust's approach and commitment to the adoption of appropriate safe haven principles and procedures and applies to all personal confidential data received and sent from the trust to ensure all sharing methods (i.e., email, post and courier) and formats (i.e. digital and hardcopy) are identified and are secure at all stages of the transfer.

2. Purpose

The purpose of this policy is to set out practical guidelines for all staff who handle confidential information as part of their legitimate working duties to ensure they are vigilant when transferring such information using Safe Haven procedures, and that information is always stored safely within a "Safe Haven" location.

3. Scope

This policy provides:

- The legislation and guidance that dictates the need for a safe haven.
- A definition of the term 'safe haven';
- Outlines when a safe haven is required
- The necessary procedures and requirements that are needed to implement a safe haven.
- Rules for different kinds of safe haven.
- Sets out access disclosure rules

This policy applies to all employees (permanent, seconded, interims, contractors, management and clinical trainees, apprentices, temporary staff, and volunteers) of the Trust. This includes the sharing of personal confidential data to organisations and companies outside of the trust which will also be governed by appropriate information sharing agreements where required.

4. Objectives

The objectives of this policy are to:

- Ensure the transfer and sharing of personal confidential data is managed and handled securely.
- Ensure all staff and third parties understand their responsibilities in managing patient confidentiality.

5. Legislation and Guidance

Several Acts: guidance and principles dictate the need for safe haven arrangements to be set in place, they include:

A key principle of the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation (GDPR)) is that organisations process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

NHS Digital Code of practice on confidential information – Annex 1 - 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 secure as they can be.

NHS Digital's Data Security and Protection Toolkit- require organisations to have a documented plan to ensure that transfers of person identifiable and sensitive information are adequately secure.

6. Definitions

6.1. Personal Data

The Data Protection Act 2018 defines 'personal data' as:

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person',

6.2. Special Category Data

This is information that contains sensitive personal detail and is a subset of Personal Data. Sensitive personal information is personal data consisting of information as to a data subject's:

(a) racial or ethnic origin.
(b) political opinions.
(c) religious beliefs or other beliefs of a similar nature.
(d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) physical or mental health or condition.
(f) sexual life.
(g) the commission or alleged commission of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

6.3. Confidential Personal Information

Confidential Patient Information is a legal term in use across the health and care system. It is defined in section 251(11) of the National Health Service Act 2006. Section 251 has been updated to ensure that the definitions used expressly include local authority social care, that is care provided for, or arranged by, a local authority. Broadly it is information about either a living or deceased person that meets the following 3 requirements:

- identifiable or likely identifiable e.g., from other data likely to be in the possession of the data recipient; and
- given in circumstances where the individual is owed an obligation of confidence; and
- conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

6.4. Business Sensitive information

This is information that if disclosed could harm or damage the reputation or image of an organisation.

6.5. Safe Haven

The term Safe Haven is recognised throughout the NHS to describe administrative arrangements in place to safeguard the confidential transfer of personal confidential data and business sensitive data between individuals and third parties.

7. Responsibilities

7.1. Chief Executive

The Chief Executive holds overall responsibility for the confidentiality and security of personal identifiable information.

7.2. Caldicott Guardian

The Caldicott Guardian is responsible for ensuring procedures governing access to, and the use of patient information and where appropriate, the transfer of that information across organisational boundaries. Some of these responsibilities including the development of Safe Havens have been delegated to the Information Governance Manager.

7.3. Senior Information Risk Owner (SIRO)

The SIRO is responsible for ensuring that all risks to information are identified and managed effectively in line with relevant legislation.

7.4. Information Governance Manager

The Information Governance Manager is responsible for managing the annual review of all inbound and outbound flows of personal confidential information and ensuring each data flow is compliant with the policy document.

7.5. Senior Managers

Managers at all levels are responsible for ensuring that they (and their staff) are aware of and adhere to this Policy and undertake information governance training ensuring this policy is built into local processes and that there is on-going compliance and improvement.

7.6. All Staff

All staff are required to comply with Information Governance requirements including the Safe Haven Policy, e.g., staff who work with person identifiable and/or sensitive information which is received or transmitted as securely and confidentially as possible.

8. What is a Safe Haven Location

The following arrangements need to be in place for an area to be considered a ‘Safe Haven’ location:

- it should be a room that is locked, or accessible via a coded keypad known 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 member of staff who work in the same building or office, or any visitors.

- if sited on the ground floor, any windows should have locks on them.
- the room should conform to health and safety requirements in terms of fire, safety from flood, theft, or environmental damage.
- manual paper records containing personal confidential data should be stored in locked cabinets.
- computers should not be left on view or accessible to unauthorised staff, they should have a secure screen saver function or switched off when not in use;
- Safe Haven procedures should be in place in any location where a large amount of personal information is being held, received or communicated, especially where the personal information is of a sensitive nature, e.g. patient confidential data.

9. Procedures for Transferring & Receiving Information

9.1. Fax (facsimile) machines

In April 2020 the NHS banned organisations from using fax machines for normal communications, and to use modern and more secure communication methods, such as secure email, to improve patient safety and cyber security.

The trust has dedicated devices located on all sites which retain fax machine functionality for use only by authorised exception in the event of a major incident response declared by the trust's incident response management

9.2. Post

If it is necessary to send personal confidential information from Trust sites via the Royal Mail, the following steps should be taken:

- Confirm the name and address of the intended recipient.
- Ensure the contents of the letter cannot be seen through the envelope
- Ensure the envelope is properly sealed
- The Trust's 'return address details' to be printed on the outside
- Mark the envelope 'Private and confidential – to be opened by addressee only'
- Where possible patient confidential data should be sent via Recorded Delivery
- For sensitive information courier or special delivery should be used and signed confirmation of receipt obtained
- Request confirmation of receipt from the recipient.
- Electronic media must be encrypted with password provided to the intended recipient via telephone or email.

9.3. Use of Couriers and Taxis to transport confidential information

Only companies that hold an existing service level agreement with the organisation with an appropriate confidentiality clause can be used to transport Trust patients, staff, equipment, or documentation – advice should be sought from the Information Governance Team if the name and contact details of the company are not known.

- Authority to use courier service is obtained from appropriate level of management.
- Any items for transport in this way should be signed in and out appropriately and copy evidence of sending/receipt retained
- All electronic transfers of personal confidential data copied to DVD/CD ROM DVD & CD-ROM/tapes/floppy disks/memory sticks must be encrypted before they are despatched.

- Packaging must be checked to ensure it is sufficient to protect the contents from any physical damage likely to arise during transit such as exposure to heat, moisture, or electromagnetic fields.
- The identification of courier is checked before handover of media
- The courier collects the encrypted disk and both parties sign the signature sheet.
- A telephone call to notify despatch is made from the despatching organisation to a named individual in the receiving organisation. The data disks are couriered directly to the destination.
- Nominated staff at the destination receives disks and sign the signature sheet
- The recipient then telephones for the passphrase to decrypt data.
- The disks are then given back to the couriers with appropriate signatures and returned to the despatching organisation for destruction.

9.4. Telephone Calls

Incoming - When speaking with individuals in person over the telephone it is important to confirm their identity before any confidential or sensitive information is disclosed.

Patients

Staff should ensure they gain assurance of the patient's identity by obtaining confirmation of (for example) certain personal details:

- Date of birth
- Address and Post Code
- Appointment Dates
- Treatment / Clinic Details
- Hospital or NHS Number

Relatives and Friends

Information should only be disclosed to a next of kin, relatives, or friends when the consent of the patient has been obtained. It is important to note that next of kin do not have any automatic right to confidential patient data.

Parents or those with parental responsibility have a right to information about their children unless the child has sought treatment independently of their parents. The Confidentiality: NHS Code of Practice provides detailed guidance relating to this.

Personal information relating to outpatients should only be disclosed to the patient. For inpatients, all calls are directed to the ward / department where the patient is located. Wards should obtain information from patients when they arrive on the ward who will call to enquire about them.

Where the patient is conscious and competent their consent should always be sought before information about them is disclosed. If this is not possible then decisions on whether to disclosure should be made on a case-by-case basis considering what are the best interests of the patient involved. It is advised that decisions involving disclosures should always be documented.

Other individuals

Where other individuals (e.g., NHS organisations, health and social care providers, the Police) request information about a patient, the individual must verify their identity and

provide evidence that they are authorised to receive the information (such as the patient's consent, legal authorisation etc.).

A caller's identity can be confirmed by calling them back on an independently verified contact number (e.g., a number available on their website).

Outgoing - Calls from trust landline phones show as from a 'Private Number' which can hinder the ability to talk to patients when calling them.

The patient's right to privacy means that when making outgoing calls we need to speak to the patient directly, unless it is justifiable to speak to someone else – e.g., the patient has provided their consent for us to do so, or it is in their best interests.
Wherever possible, if you think you may need to contact a patient by phone, ask them in advance if they have any preferences:

- Would they prefer to be called at work?
- Would they prefer to be called at home?
- Can we call a mobile phone number instead of a landline?
- Would they like information to be left with a family member if they know they cannot be contacted directly?
- Are they happy for messages to be left on their answer phones?

These consent preferences should be regularly checked with the patient.

If someone other than the patient answers the phone avoid using alarmist language such as "it is confidential".

If you know that the patient is unable to speak to you or if the recipient acts on the patient's behalf, you can pass limited information on to the recipient, but avoid disclosing clinical information.

9.5. Leaving Answer Phone Messages

There are privacy risks associated with leaving answer phone messages unless the patient has provided their consent to do so. Leaving a message on a patient's own mobile phone number is more secure than a landline number.

If you do not have consent then any answer phone message left should be limited to your name, the hospital name, and your telephone number.

There is a balance to be struck between respecting the privacy of the patient, not unduly worrying them with an obscure message, and ensuring that the recipient understands that it is a genuine message (e.g., not a scam that is looking to get them to call back a premium rate number).

Staff should take responsibility for considering whether any particular privacy issues exist that could affect whether it is appropriate to leave an answer phone message. Consider the following:

- If you leave an answer phone message, the patient may not be the first to hear it
- Who else might hear the message?
- Are you sure you have dialled the correct number?

- Will the patient fully understand the content of the message?
- How can you be certain the message has ever been received?
- You may inadvertently breach patient confidentiality because the patient's friends or relatives may not know the patient is receiving health care.

9.6. **Short Message Service (SMS**)
Short Message Service (SMS) is an easy to use, standardised, mobile communications service for the exchange of short alphanumeric text messages usually between mobile telephone devices.

SMS Text messaging is currently in use within the Trust prominently for reminding patients of their outpatient appointment for the purpose of reducing Did Not Attend (DNA). Patient identifiable information must never be included within a text message and must not contain sensitive information.

The following is a link to national guidance relating to the appropriate use of text message communication.

https://transform.england.nhs.uk/information-governance/guidance/email-and-text-message-communications/

9.7. Transporting Information

9.7.1 Paper Records
The following principles apply to paper-based records containing personal confidential data or Trust sensitive information.

- Paper-based Health Records must be transported between sites by authorised daily 'courier' transport providers, not employees.

- Paper business records must only be taken off-site where a line manager has identified an authorised business need. It must be recorded what has been taken, why, where to and by whom.

- Records must be transported in sealed containers e.g., secured envelope, locked briefcase or transit bag. Not carried 'loosely'.

- If staff are required for business purposes to transport records in their vehicle, they must be kept out of sight in a locked boot at all times during a journey, and not left in the vehicle overnight.

- The person handling the records holds the responsibility for their safety and ensuring they are always kept secure.

- Remember you are bound by the same rules of confidentiality even if your 'place of work' is 'home-working' or 'mobile' in the community. You are responsible for ensuring documents are always held 'secure and confidential' in your possession.

- While at home you have personal responsibility to ensure the records are kept secure and confidential. This means locked away or out of sight from other members of your family including your friends and colleagues

9.7.2 Removable Media

If there is a requirement for personal confidential data or business sensitive information to be transferred on any forms of removable media, then this must be achieved in accordance with the Information Security Policy. When information sharing is to organisations and companies outside of the trust where an appropriate information sharing agreement must also be established, this must also document the type of removable media and the security measures to be applied.

9.8. E-mail

NHS Mail is currently the only NHS approved method for exchanging person identifiable or sensitive data, but only if both the sender and recipient use an NHS Mail email account or they are on another approved government secure domain. The following link provides information of email addresses that are known to be secure NHS Guidance for sending secure email

NHS Mail is a communication method, not a 'filing system', and all information received should be stored appropriately on receipt. For example, transferred into a patient's electronic patient record (EPR), saved to folders with restricted access (available only to authorised members of staff) or details should be transferred into the relevant database. Attachments should never be retained in emails but stored on department or personal file shares

9.8.1 Email encryption

The NHS Mail encryption feature means that users can also securely exchange sensitive information with users of non-accredited or other email systems used by the public , for example those ending in nhs.uk, Hotmail, Gmail and Yahoo. The NHS Mail encryption feature means that health and social care staff now benefit from a secure service which allows them to communicate across organisation boundaries and industry sectors. NHS Mail can be used securely across the entire health and social care community – in fact with anyone using any email account. With the NHS mail encryption feature:

- Users can easily communicate securely with ANY email service without having to manually 'password protect' or encrypt sensitive information
- Users can send attachments which will also be automatically encrypted and remain secure
- Organisations save money by replacing existing post, fax and phone-based processes with secure email
- Users of non-accredited or non-secure email services can communicate securely with NHSMail users saving time and money, speeding up communications and improving patient care
- Communication is faster, easier and more reliable.

9.8.2 Sending to non-NHS mail users:

To send emails to non-accredited or non-secure email services with whom you need to exchange sensitive information, you MUST enter the word SECURE within square brackets [] as the first word on the subject line. This then encrypts the whole document and attachments.

The recipient will receive an automatic email message from NHS Mail requesting them to log into an encryption website to retrieve their email and its contents.

Recipients can reply to the email sender, using the same encryption website at the time or later by logging into the website first

Step-by-step instructions can be found in the guidance for recipients, which should be sent as a un-secured email to them first.

9.8.3 Sending using the encryption service must note the following:

- Before you send an encrypted email, talk to the person you're sending it to – make sure that they're expecting the information and know how to retrieve this from the encryption system and are ready to deal with it appropriately.
- It's your responsibility to safeguard any sensitive data you send – if you are sending the information on behalf of an organisation, you should do so in line with local data protection and information governance policies.
- If you are sending information to a patient, gain consent from them before you communicate with them via email and do so in line with your local information governance policies.
- Email delivery to Internet email addresses (e.g., Hotmail.com) can be unreliable. Sometimes messages are silently lost or sometimes a delivery notification is returned even if the message has not been received by the recipient. Where delivery assurance is required, please ask the sender to reply to you confirming receipt

9.9. Safe Haven Printers

Trust printers operate a 'secure print' function, and these must be used to print confidential documents. These are multi-functional devices that require a personal pin entered into the printer before documents will securely print. Pin codes are obtainable following the instructions available on the trust's Intranet Page and are linked to an employee's NHS Mail email address.

Local printers MUST only be used where staff are permanently based in the location of the device for their complete employment duration. Documents MUST be collected from the device when immediately printed.

9.10. Use of Computers

- Access to any computer must be password protected in line with current IT access rules; this password must not be shared.
- Computer screens must not be left on view so members of the public or staff who do not have a justified need to view the information can see person identifiable data. Always lock your computer when away from your desk. Computers or laptops not in use should be switched off or have a secure screen saver device in use.
- Information should be held on the organisation's network servers, and not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.
- Information should not be saved or copied into any PC or media that is "outside the NHS infrastructure".
- Personal information via email MUST be sent using NHS Mail with appropriate safeguards:
    - Clinical information is clearly marked as confidential.
    - Email addresses checked before 'Send' to ensure the correct recipient.

- Use ‘Cc’ or ‘Bcc’ when required to hide recipiant’s email addresses in ‘bulk’ communications.
- Browsers set up so passwords are not saved, and temporary internet files are deleted on exit.
- The receiver is ready to handle the information in the right way.
- Information sent by email removed from emails and safely stored and archived as well as being incorporated into patient records.
- There is an audit trail to show who did what and when.
- There is Disaster Recovery & Business Continuity procedures and fail-safe arrangements.

9.11. File sharing externally

When using an external system to share documents with external organisations the data location must be within the UK, have a secure transmission method and built-in ‘encryption-at-rest’ for document management to NHS Cyber Security Standards. Where possible these should be used by staff to communicate meeting agendas, minutes, data quality reports etc. with other organisations and trust staff at the same time rather than sent via email so that all users have the same information in real time.

Safe Haven areas can be created which allows the secure sharing of information by granting authorised staff access to the information via a password log in to a separate area. This removes the need to ‘send’ information via other means e.g., email/post.

Authorised access groups must be established to ensure only authorised personnel can access specific areas within the product used. Any product to be used which will contain person identifiable information/corporate sensitive information must be located within the United Kingdom and approved by the Information Governance Manager to comply with the UK data protection laws.

10. Clinical Whiteboards

Boards containing personal information should ideally be in areas that are not generally accessed by the public. However, most whiteboards are in public areas of wards to support effective clinical operations. These boards should contain only sufficient information to locate the patient and should not contain confidential information, e.g., diagnosis. The identity of patients must be recorded as initials or first initial and surname only – exemptions must be authorised by Information Governance. The use of codes or symbols on whiteboards may be acceptable where these are known only to staff and where their meaning could not be reasonably inferred.

11. Data Flow Mapping

To support and implement Save Haven principles the trust must ensure that all information transfers are identified by determining where, why, how and with whom it exchanges information.

This is known as Data Flow Mapping. This mapping of information, particularly Personal Confidential Data (PCD) will help identify the higher risk areas of information transfers that require effective management and ensure compliancy with the Data Protection & Security Toolkit Requirement.

12. Monitoring and Assurance

The Information Governance team undertakes annual audit and review of all inbound and outbound data transfers across the trust. Each data flow is documented, and risk assessed to ensure appropriate safeguards have been implemented to protect information.

1	Following local and national policies and guidelines, what key elements require monitoring?	List elements to be monitored	Appropriate methods for the secure flow of personal identifiable information.
2	Who will lead/be accountable for monitoring?	Lead title and/or MDT	Data Protection Officer Senior management in each service and departmental area of the trust.
3	Describe how the key elements will be monitored?	List tools to evidence compliance	Data breaches, Staff surveys, complainants. Data Mapping Flow exercise undertaken yearly.
4	How frequently will each element be monitored?	List frequency of monitoring for each element	Annually
5	Explain the protocols for escalation in the event of problems?	List the processes of escalation	Incident reporting procedure when a data breach occurs.
6	Which Committee/ Panel/ Group will reports go to?	List the Committee/Panel/ Group/Peer Review that the reports will go to	a. Informatics Group
7	Explain how the policy/guideline will be disseminated within the Trust?	List ways identifying how this document will be shared and how it will be recorded that appropriate staff have been made aware of the document and where to find it	a. Trust Induction

There is also an annual programme of internal and external audits in place which provides validation and assurance of the trust's information governance systems.

13. Related Policies

The Policy will be supported by several Information Governance policies that set out both user level and operational level details for implementing effective information security across the Trust. These include.

- ICT Code of Conduct
- Data Protection 2018 Policy
- Health Records Management Policy
- Information Sharing Policy
- Mobile Computing and Remote Working Policy

14. Equality Impact Assessment

Does this policy/guideline affect one group less or more favourably than another on the basis of:				
				Comments
1	Age (younger people & children& older people)	yes	**no**	
2	Gender (men & women)	yes	**no**	
3	Race (include gypsies and travellers)	yes	**no**	
4	Disability (LD, hearing/visual impairment, physical disability, mental illness)	yes	**no**	
5	Religion/Belief	yes	**no**	
6	Sexual Orientation (Gay, Lesbian, Bisexual)	yes	**no**	
7	Gender Re-assignment	yes	**no**	
8	Marriage & Civil Partnership	yes	**no**	
9	Pregnancy & Maternity	yes	**no**	
	Is there any evidence that some groups maybe affected differently?	yes	**no**	
	Could this document have an impact on other groups not covered by a protected characteristic? (e.g.: low wage earners or carers)	yes	***no***	
	If '**NO IMPACT'** is identified for any of the above protected characteristics then no further action is required.			
	If '**YES IMPACT**' is identified a full impact assessment should be carried out in compliance with HR028 Equality & Human Rights Policy and linked to this document			

Any other comments:
None

Assessment completed by:	Nicola Bateman	Date completed:	Oct 2022