NHS
Cornwall and
Isles of Scilly

Safe Haven Policy

Date Approved: 11 April 2025

NHS Cornwall and Isles of Scilly Integrated Care Board

Call us on 01726 627 800
Email us at ciosicb.contactus@nhs.net
Visit our website: cios.icb.nhs.uk

Part 2S, Chy Trevail,
Beacon Technology Park,
Dunmere Road,
Bodmin, PL31 2FR
Chair: John Govett
Chief executive officer: Kate Shields

Document control

Title of document: Safe Haven policy
Lead directorate: Corporate Governance
Lead team: Information governance
Document type: Policy
Subject category: Information governance
Author(s) name: Head of information governance
Date ratified: 11 April 2025
Ratified by: People and organisational governance committee
Review frequency: 3 years (standard, unless otherwise indicated)
To be reviewed by date: 11 April 2028
Target audience: All staff
Can this policy be released under FOI? Yes
Give reasons for exemption if no: N/A

Version control

Version No	Revision date	Revision by	Nature of revisions
	March 2016	B Gallagher	Approved version placed on website
1.0	January 2019	J Phelps	Review and update to include GDPR
2.0	February 2019	Trudy Corsellis	Further revisions and EIA added before submission to IGSC
2.1	March 2025	Milton Shoriwa SCW CSU	Review and update ahead of DSP Toolkit

Contents

1. Introduction 5
2. Scope of this policy 5
3. Legislation and guidance 5
4. Definitions 6
5. Where safe haven procedures should be in place 7
6. Responsibilities for implementing the Safe Haven Policy 7
7. Requirements for safe havens 8
8. Fax machines 8
9. Incoming mail 8
10. Outgoing Mail 9
11. Transporting sensitive documents 9
12. Transferring patient or person identifiable information electronically 10
Appendix 1: Regulatory Framework 11
Appendix 2: NHS CIOS ICB related policy documents 12
Appendix 3: Equality Impact Assessment 13

1. Introduction

1.1. All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information held and transferred in and out. The implementation of this policy and supporting procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information (e.g. health information).

2. Scope of this policy

2.1. The aim of this policy is to ensure the use of patient information is subject to strict transfer controls, which already apply elsewhere, where confidential information is handled. There is a very important need to reassure patients, staff and the public that information will be handled securely and safeguards are in place to ensure its security. These safeguards include:

- Fax machines sited in a secure area or cupboard and only used *when absolutely necessary* (all other methods of transfer being unavailable).
- Designated staff are responsible for collecting and delivering the faxed information to the appropriate person.
- A directory of safe haven fax machines in use.
- Security of areas where hard copy patient or personal information is held or stored.
- Security of areas where patient or personal information are received or sent by post.

2.2. This policy provides:

- The legislation 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.
- Rules for different kinds of safe haven.

3. Legislation and guidance

3.1. A number of acts and guidance dictate the need for safe haven arrangements to be set in place:

- The Data Protection Act 2018, within which the third data protection principle is ‘personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.’
- NHS Code of Practice: Confidentiality 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 secure as they can be.’
- A list of the legislation and guidance relating to this policy can be found in appendices 1 and 2.

4. Definitions

4.1. Safehaven - The term ‘safehaven’ describes an agreed set of administrative procedures, or in some cases a piece of equipment, situated on the organisation’s premises, where arrangements and procedures are in place to ensure the safe receipt and secure handling of confidential person identifiable information. It can also be considered to be a location within the organisation where confidential information is stored in a secure manner.

4.2. Person identifiable information - Personal identifiable information is information which can identify a living individual. An individual is ‘identified’ if you can distinguish that individual from other members of a group.

4.2.1. This could be done by various combinations of data, for example:

- Date of birth and postcode
- Gender and postcode
- Name and date of birth
- Name and address
- Name and NHS number

4.2.2. Or it may be a unique identifier for example:

- NHS number
- National insurance number
- Payroll number

4.2.3. Personally identifiable data (PID) could even be a description such as “the tall elderly gentleman with a dachshund who lives at number 15 and drives a Porche Cayenne.”

4.2.4. PID must not be transmitted or transferred without first assessing the risk of doing so.

4.3. Special categories of personal data - Special categories of personal data include where the personal information contains details of that person's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

For this type of information, even more stringent measures should be employed to ensure that the data remains secure.

5. Where safe haven procedures should be in place

5.1. Safe haven procedures should 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.

5.2. There should be at least one area designated as a safe haven at each of the organisation's sites.

6. Responsibilities for implementing the Safe Haven Policy

6.1. Caldicott Guardian - The appointed Caldicott Guardian for the organisation must approve all policies and procedures that relate to the use of patient information.

6.2. Head of Information Governance/Data Protection Officer - The Head of Information Governance is responsible for coordinating improvements in:

- Data protection
- Confidentiality
- Information security

- Data quality

6.3. All staff - All staff who process person identifiable information, and managers who line manage those staff, have a responsibility to ensure the movement of information is carried out in a secure manner in line with all organisational policies and procedures.

7. Requirements for safe havens

7.1. Location/security arrangements:

- It must be a room that is locked or accessible via a coded key pad 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 must 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, must have a secure screen saver function and be switched off when not in use.
- Equipment such as fax machines in safe havens must have a code password and be turned off out of office hours

8. Fax machines

8.1. The NHS has phased out the use of fax machines. As of April 2020, NHS practices are no longer allowed to use fax machines for either NHS or patient communications. This move is part of a broader effort to modernise the health service and improve patient safety and cyber security. Instead, NHS organisations are required to use more secure and efficient communication methods, such as email.

9. Incoming mail

9.1. All incoming mail known to contain patient or personal information, marked ‘safe haven’, ‘confidential’ or ‘private’, must be handled discreetly and passed on to the correct recipient without the mail being opened or read. Where the intended recipient cannot be located, the information must be passed to a senior manager responsible for the area.

9.2. Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified.

9.3. Unsolicited mail may simply be misaddressed and therefore returning it to the sender may be all that is required. However, you should be aware that unsolicited physical mail and electronic mails might be used to gain unauthorised access to organisational information, for example staff must take care not to unintentionally disclose additional sensitive information when returning mail to the original sender.

10. Outgoing Mail

10.1. All outgoing mail to partner organisations containing patient/person identifiable information must be marked 'safe haven' and only be delivered to an appropriate named 'safe haven' address. This means that single letters being sent out containing single patient information must be sent in envelopes which will rip should an attempt be made to open them. These can be sent by normal post.

10.2. Bulk transfer of patient identifiable information (which means 50 personal details or more) must be placed in sealed envelopes or boxes, which will show if they have been tampered with before reaching their destination. They must then be sent using either the internal courier service, or by special delivery which will track each stage of the transfer.

10.3. Where full patient records are transferred, these must be despatched in sealed envelopes or boxes by internal courier, or by special delivery which will track each stage of the transfer.

11. Transporting sensitive documents

11.1. The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, availability and integrity during and after transportation or transmission, are adequate and appropriate.

11.2. When selecting the most suitable delivery option for documents it is important to pay strict attention to the information classification level and to any security risk to the information, such as mishandling and misuses, and also to the potential for theft inherent in each delivery option, delivery media and delivery location.

- If the transport medium is inappropriate for the sensitivity or value of the information being transported, it could facilitate the theft of the contents while in transit.
- If the transport medium used does not protect confidential data or does not protect from transit damage, information may be lost or at least delayed.

12. Transferring patient or person identifiable information electronically

12.1. Staff transferring information electronically using email must refer to the IT Security Policy and E-mail Usage Policy.

12.2. When sending PID via NHSMail to a non-secure email address, staff must ensure that they suitably encrypt the contents of the email by using [secure] in the subject line. For more information about non-secure email addresses, contact the Head of Information Governance (HOIG).

Appendix 1: Regulatory Framework

Information governance currently encompasses the following local, national and legal regulations:

- Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Confidentiality: NHS Code of Practice
- BS ISO/IEC 27000 series of Information Security Standards
- Caldicott Guardian Manual and Reviews 2006 and 2013
- Common Law Duty of Confidentiality
- Records Management: NHS Code of Practice
- Health and Social Care (Safety and Quality) Act 2015
- Access to Medical Records Act 1988
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Health and Social Care Act 2012 & Health and Social Care (Safety and Quality) Act 2015
- Information Security Management: NHS Code of Practice
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Public Interest Disclosure Act 1998
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Abortion Regulations 1991
- Mental Capacity Act 2005
- NHS Care Records Guarantee
- NHS Constitution
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974
- Re-Use of Public Sector Information Regulations 2005
- Data Security and Protection Toolkit

The above list is not exhaustive.

Appendix 2: NHS CIOS ICB related policy documents

This strategy should be read in conjunction with the following policies and documents:

- Information Governance Strategy
- Information Governance Policy
- Data Protection Policy
- Records Management Code of Practice
- Subject Access Request Policy
- Pseudonymisation Policy
- IT Security Policy and all linked policies
- Integrated Identity Management Policy
- Email Policy
- Disciplinary Policy and procedures
- Acceptable Use Policy
- Safe Haven Policy
- Data Quality Policy
- Business Continuity Plans
- Risk Management Strategy and Policy
- Incident Management Policy
- Freedom of Information Policy
- NHS C&IoS ICB's Privacy Notice
- Home Working Policy
- Information Sharing Protocols and Agreements
- Serious Incident Policy
- Confidentiality Code of Conduct for Employees
- NHS C&IoS ICB's Information Governance Handbook

This list is not exhaustive.

Appendix 3: Equality Impact Assessment

Name of policy to be assessed	Policies relating to Data Protection and Information Governance. Including: Confidentiality Code of Conduct, Pseudonymisation Policy, Data Protection Policy, Data Quality Policy, Safe Haven Policy, Information Governance Policy, Information Governance Strategy, Records Management Policy.		
Section	Information Governance	**Date of Assessment**	12/02/2019
Officer responsible for the assessment	Data Protection Officer	**Is this a new or existing policy?**	Existing
1. Describe the aims, objectives and purpose of the policy.			
The policies identified above outline how NHS C&IoS ICB will meet its legal obligations and NHS requirements and will provide documented evidence of continued commitment to the securing of both corporate and person identifiable information and processes that comply with confidentiality, General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018). The policies provide guidance to staff to ensure the consideration of legal responsibilities and the privacy of all individuals when processing data. The requirements within the Policies are primarily based upon the DPA 2018 which is the key piece of legislation covering security and confidentiality of personal information.			
2. Are there any associated objectives of the policy? Please explain.			
Associated objectives are NHS C&IoS ICB compliance with the Data Security Protection Toolkit, the attainment of the commitments in the NHS Constitution, Data Protection Act, General Data Protection Regulations, Human Rights Act, Care Records Guarantee and information security standards.			
3. Who is intended to benefit from this policy, and in what way?			
NHS C&IoS ICB staff will benefit from the implementation of robust information security controls to protect them and the information processed as part of the services provided. Patients will benefit from the provision and availability of high quality information and data which meets the Data Protection Act, Freedom of Information Act, Human Rights Act and Records Management: NHS Code of Practice.			

4. What outcomes are wanted from this policy?
That the information processed by NHS C&IoS ICB and its staff, in all formats, is of a high quality and is protected to the highest possible standards and available quickly, processed in line with legislation and all confidentiality requirements, Government standards and NHS Digital requirements.
5. What factors/ forces could contribute/ detract from the outcomes?
Staff awareness of the content of the policies and staff completing Information Governance training will contribute to information governance practices
6. Who are the main stakeholders in relation to the policy?
The main stakeholders are NHS C&IoS ICB Governing Body and its constitutional committees in order to meet its responsibilities. In addition, the Data Protection Officer, the Head of Information Governance, all staff as well as the Information Governance Sub Committee have key operating functions and responsibilities for implementing information governance throughout NHS C&IoS ICB. These policies are also important for Individuals in the community.
7. Who implements the policy, and who is responsible for the policy?
The Data protection Officer, Head of Information Governance and the Information Governance Sub Committee providing assurance and escalation to the Workforce Committee.
8. What is the impact on people from Black and Minority Ethnic Groups (BME) (positive or negative)?
Consider relevance to eliminating unlawful discrimination, promoting equality of opportunity and promoting good race relations between people of different racial groups. Issues to consider include people's race, colour and nationality, Gypsy, Roma, Traveller communities, employment issues relating to refugees, asylum seekers, ethnic minorities, language barriers, providing translation and interpreting services, cultural issues and customs, access to services.
The policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of racial groups. The standards of Information Governance, documents referenced in the policies and training will take account of the need to provide data in required formats or languages to ensure accessibility to all to ensure correct use and handling. The new data protection framework protects personal data ‘revealing racial or ethnic origin’ as a ‘special category of data’ and processing of it as ‘sensitive processing’.

How will any negative impact be mitigated?
A requirement of the information governance programme specifically relates to the provision of information in differing formats and evidence is collated to support this.
9. What is the differential impact for male or female people (positive or negative)?
Consider what issues there are for men and women e.g. responsibilities for dependants, issues for carers, access to training and employment issues, attitudes towards accessing healthcare.
The policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of sex.
How will any negative impact be mitigated?
There are no sections within the policies that distinguish between sexes.
10. What is the differential impact on disabled people (positive or negative)?
Consider what issues there are around each of the disabilities e.g. access to building and services, how we provide services and the way we do this, producing information in alternative formats and employment issues. Consider the requirements of the NHS Accessible Information Standard. Consider attitudinal, physical and social barriers. This can include physical disability, learning disability, people with long term conditions, communication needs arising from a disability.
The policies outline the importance of confidentiality and there should therefore be a positive impact on individuals with a disability as this information should not be shared without the express permission of the individual. The new data protection framework protects personal data 'concerning health' as a 'special category of data' and processing of it as 'sensitive processing'. Additional safeguards are provided throughout the new data protection policies. This may have an impact on those not capable of, or with varying capacity to, give consent, which is 'freely given, specific, informed and unambiguous', such as people with a learning disability.
How will any negative impact be mitigated?
Adjustments will be made for any member of staff with a disability requiring assistance to enable them to understand how to implement Data Protection to the necessary standards. The standards of Information Governance, documents referenced in the policies and training will take account of the need to provide data in any required format or language to ensure accessibility to all to ensure correct use and handling of corporate and personal information.

11. What is the differential impact on sexual orientation?
Consider what issues there are for the employment process and training and differential health outcomes amongst lesbian and gay people. Also consider provision of services for e.g. older and younger people from lesbian, gay, bi-sexual. Consider heterosexual people as well as lesbian, gay and bisexual people.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the sexual orientation of the individual should be protected. The new data protection framework protects personal data 'concerning sex life and sexual orientation' as a 'special category of data' and processing of it as 'sensitive processing'. The existing condition for processing personal data 'for the purpose of identifying or keeping under review the existence or absence of equality of opportunity' is newly expanded to include personal data concerning an individual's sexual orientation.
How will any negative impact be mitigated?
There are no sections within the policies that will negatively impact an individual due to their sexual orientation.
12. What is the differential impact on people of different ages (positive or negative)?
Consider what issues there are for the employment process and training. Some of our services impact on our community in relation to age e.g. how do we engage with older and younger people about access to our services? Consider safeguarding, consent and child welfare.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the age of the individual should be protected.
How will any negative impact be mitigated?
The policies, their content and implementation will not negatively impact those of differing ages.
13. What differential impact will there be due religion or belief (positive or negative)?
Consider what issues there are for the employment process and training. Also consider the likely impact around the way services are provided e.g. dietary issues, religious holidays, days associated with religious observance, cultural issues and customs, places to worship.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the impact on those with a religious affiliation or belief should be positive. The new data protection framework protects personal data regarding 'religious or philosophical beliefs' as a 'special category of data' and processing of it as 'sensitive processing'.

How will any negative impact be mitigated?
The policies, their content and implementation will not negatively impact those with a religious affiliation or belief.
14. What is the impact on marriage of civil partnership (positive or negative)? NB: this is particularly relevant for employment policies
This characteristic is relevant in law only to employment, however, NHS C&IoS ICB will strive to consider this characteristic in all aspects of its work. Consider what issues there may be for someone who is married or in a civil partnership. Are they likely to be different to those faced by a single person? What, if any are the likely implications for employment and does it differ according to marital status?
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the impact on marriage or civil partnership status of the individual should be positive.
How will any negative be mitigated?
The policies do not negatively impact those who are married or in a civil partnerships.
15. What is the differential impact who have gone through or are going through gender reassignment, or who identify as transgender?
Consider what issues there are for people who have been through or a going through transition from one sex to another. How is this going to affect their access to services and their treatment when receiving NHS care? What are the likely implications for employment of a transgender person? This can include issues such as privacy of data and harassment.
The policies outline the legal basis for collecting sensitive information, limits how and when it may be shared and when it should be destroyed. They also outline the expectations of staff to maintain confidentiality.
How will any negative impact be mitigated?
No negative impact has been identified for those who gone through or are going through gender reassignment, or who identify as transgender.
16. What is the differential impact on people who are pregnant or breast feeding mothers, or those on maternity leave?

This characteristic applies to pregnant and breast feeding mothers with babies of up to six months, in employment and when accessing services. When developing a policy or services consider how a nursing mother will be able to nurse her baby in a particular facility and what staff may need to do to enable the baby to be nursed. Consider working arrangements, part-time working, infant caring responsibilities.
The Data Protection Policy includes the requirement for training of all staff to Information Governance standards. Information Governance training and all documentation will remain available to staff on maternity leave or on return from maternity leave. Knowledge and skills following maternity leave will be updated using the mandatory training requirements. Staff are required to maintain the code of confidentiality and therefore under these policies are expected not to share information relating to pregnancy or maternity leave without the consent of the individual. The new data protection framework protects personal data 'concerning health' as a 'special category of data' and processing of it as 'sensitive processing'. Additional safeguards are provided throughout the new data protection framework.
How will any negative impact be mitigated?
There is nothing in the policies which would negatively impact those who are pregnant or on maternity leave.
17. Other identified groups:
Consider carers, veterans, different socio-economic groups, people living in poverty, area inequality, income, resident status (migrants), people who are homeless, long-term unemployed, people who are geographically isolated, people who misuse drugs, those who are in stigmatised occupations, people with limited family or social networks, and other groups experiencing disadvantage and barriers to access.
No negative impact has been identified for these groups. However there may be a positive impact in that the policies set out how personal information should be handled and how long it should be retained. The policies also set out the requirements for staff to maintain a code of confidentiality. We also acknowledge and will work with individuals who, in order to exercise their rights, may need to speak rather than write to the CCG formally.
How will any negative impact be mitigated?
No negative impact has been identified.
18. How have the Core Human Rights Values been considered in the formulation of this policy/strategy? If they haven't please reconsider the document and amend to incorporate these values. • **Fairness;** • **Respect;**

- **Equality;**
- **Dignity;**
- **Autonomy**

The requirements and principles of the Data Protection Act, which is linked to the Human Rights Act, have been taken into account when writing these policies, including the individual rights of data subjects. Fairness in informing individuals of the uses to be made of their data in a fair processing notice have been produced, respect for privacy, dignity and choice have been written into all Information Governance Policies.

19. Which of the Human Rights Articles does this document impact?

The right:	**Yes / No:**
• To life	No
• Not to be tortured or treated in an inhuman or degrading way	No
• To liberty and security	No
• To a fair trial	No
• To respect for home and family life, and correspondence	Yes
• To freedom of thought, conscience and religion	No
• To freedom of expression	No
• To freedom of assembly and association	No
• To marry and found a family	No
• Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention	Yes
• To peaceful enjoyment of possessions	No

a) What existing evidence (either presumed or otherwise) do you have for this?

All documentation produced as part of the Information Governance programme of work has taken account of the Human Rights Act and this has been referenced where necessary.

20. How will you ensure that those responsible for implementing the Policy are aware of the Human Rights implications and equipped to deal with them?

The Act has been referenced within the policies and procedures produced and any monitoring of compliance will include the awareness of patients and staff having a right to privacy, dignity, respect and choice.
21. Describe how the policy contributes towards eliminating discrimination, harassment and victimisation.
By setting out how personal information will be handled and stored and the expectations of staff in these matters information should not be held for the purposes of discrimination, harassment and victimisation. The policies also allow for individuals to rectify information where it is believed to be held incorrectly.
22. Describe how the policy contributes towards advancing equality of opportunity.
The policies describe how and when information should be collected, stored and for how long. This should mean that the organisation does not hold inappropriate information about people without a considered business reason. The code of confidentially sets out how staff should treat information in their care.
23. Describe how the policy contributes towards promoting good relations between people with protected characteristics.
The policies set out how information both personal and corporate will be managed by the organisation. If the policies are followed then those individuals with protected characteristics should be positively impacted as sensitive data can only be collected within a lawful basis and then must be kept confidential.
24. If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services or the working environment for that group of people.
The policies can be provided in multiple formats if necessary.
25. Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
Not applicable
26. If the negative impacts identified have been unable to be mitigated through amendment to the policy or mitigating actions, explain what your next steps are.
Not applicable.