NHS
Cornwall and
Isles of Scilly

Information rights 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: Information rights 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: Information Governance Steering Group
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 Number	Revision date	Revision by	Nature of revisions
V1.0	5 April 2022	Head of information governance	Minor change to office address. Change organisation name to NHS Cornwall and Isles of Scilly Integrated Care Board (CIOS).
V1.0	17 May 2022	People and organisational governance committee	Policy ratified by the committee
V2.0	1 July 2022	NHS Cornwall and Isles of Scilly Integrated Care Board (ICB)	Policy adopted by NHS Cornwall and Isles of Scilly ICB
V3.0	7 March 2025	SCW CSU	Reviewed and expanded to include all information rights under UKGDPR ahead of CAF DSPT 2024-25
V4.0	21 April 2026	Corporate Governance Team	Minor changes to email addresses and team contacts

You can request any document published on our website in alternative formats. Email our engagement team for more information.

Contents

1. Introduction 4
2. Purpose 4
3. Individual rights under UK GDPR 4
4. Responding to requests 7
5. Other requests 8
6. Responsibilities 8
7. Should you be unhappy with a response 10
8. Implementation plans and monitoring effectiveness 10
9. Update and review 11
10. Other relevant policies 11
Appendix 1: Legal and regulatory framework 11
Appendix 2: Equality impact assessment 13
Aims, objectives and purpose of the policy 13
Differential impacts 13
Human rights values 15
Public Sector Value Act 2012 15
Equality impact assessment action plan 16

1. Introduction

NHS Cornwall and Isles of Scilly Integrated Care Board (ICB) has a legal obligation to comply with all appropriate legislation in respect of data/information management and IT security. It also has a duty to comply with guidance issued by the Government, the Department of Health, NHS England, NHS Digital, the Information Commissioner, and other advisory groups to the NHS as well as guidance issued by professional bodies.

Data Protection legislation provides individuals with a number of different information rights, including;

- Right of access, commonly referred to as 'subject access'
- Right to be informed
- Right to erasure
- Right to restriction
- Right to object
- Right to data portability
- Rights around automated decision-making and profiling

These rights allow an individual or their representative to have a degree of control over the management of their personal data as well as other supplementary information held by the organisation.

Members of the public can view the types of information processed and reasons for information processing by the ICB by visiting: Privacy notice - NHS Cornwall and Isles of Scilly (icb.nhs.uk)

2. Purpose

This policy explains how the individuals can exercise their rights to the ICB, typically by the submission of a written request either by post or email. To note – requests can also be made verbally under the legislation.

This policy provides an outline of the requirement for ICB staff to ensure that an appropriate response, action or disclosure is made to data subjects in line with Data Protection Act 2018.

This policy explains to staff what the legal requirements are for the ICB to respond to requests and what the legal rights of individuals are under Data Protection Act 2018.

This policy applies equally to personal data, and special categories of personal data, that may be used to administer the provision of healthcare services, to inform research or to manage and administer the ICB workforce, and all other business functions of the ICB.

3. Individual rights under UK GDPR

The different rights set out under Data Protection legislation are covered in detail within the ICB's Data Protection Policy. This can be found within the Document Library.

Right to be informed
Articles 12, 13 and 14 of UK GDPR relate to an individual's right to be informed. Organisations have an obligation to be transparent about what data they process, where why and who it is shared with

Right of access (Art 15)
Often referred to as a 'Subject Access Request' – this right gives individuals the right to request a copy of and/or to view their personal data where it is held by an organisation.

Right to rectification (Art 16)
Individuals have the right to have inaccurate personal data rectified. This right is not absolute and in relation to medical records, only applies where the information is found to be incorrect or untrue. A request for rectification will not be successful simply because a data subject does not agree with what is written.

Right to erasure (Art 17)
Individuals have the right to be 'forgotten' and have their personal data erased. To note – this does not apply for direct healthcare information processed by the ICB

Right to restrict (Art 18)
Individuals have the right to restrict the way in which their personal data is processed in certain circumstances. This can involve limiting it's use or limiting access to it.

Right to data portability (Art 20)
Individuals have the right to receive personal data they have provided to a data controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

Right to object (Art 21)
Individuals have the right to object to the way in which their personal data is processed – it allows for an opportunity to ask the ICB to stop processing their personal data though it has limited applicability dependent on the lawful basis for processing.

Rights in relation to automated decision-making and profiling
UK GDPR restricts organisations from making solely automated decisions, including those based on profiling which have a legal or significant effect on individuals.

In order to assist the ICB to deal with requests efficiently, any individual who wishes to make a request should:

- Clearly mark the purpose of the request regarding their personal information as a SAR or otherwise (though any formal request regarding personal information will be treated as such)
- Include the date on the request
- Include name and any aliases if relevant
- Include up to date contact details
- Include any relevant reference numbers, such as your NHS number
- Explain as much as possible what information is being requested and any additional information which may help the ICB identify which members of staff might hold the information
- Provide any relevant details or dates which the information may relate to
- Indicate desired method of receipt for response to the request

Ideally, all requests for personal information should be made in writing using the form available on the ICB website Subject access request form and emailed to ciosicb.dsar@nhs.net or by post to:

Information Governance Team
NHS Cornwall and Isles of Scilly Integrated Care Board
Part 2S, Chy Trevail
Dunmere Road
Bodmin
PL31 2FR

Requests will also be accepted if made verbally, either in person or over the phone.

When the ICB acknowledges requests, we will inform requestors of the date a response can be expected. In very exceptional circumstances the ICB may need extra time to consider your request and have the right to extend by an extra two months. If this is the case, requestors will be informed within the first 30 days.

The ICB will advise if we do not hold any relevant personal information but will normally provide copies of any information requested.

When the ICB has responded to a request for information relating to a specified time period, a response for any subsequent requests will only be provided for differing periods of time.

When the ICB receives a request from a legal representative/advocate or someone acting on behalf of the data subject, consent will be required. This must be a hard copy signature explicitly consenting to the release of the data subject information indicated in the request. the data subject must make it clear where the response should be sent. However, the ICB may request additional documented proof of identity and confirmation of the request from the data subject.

The response letter will also reference the requestor's right to complain to the ICO

Should requesters of information require a response to be provided in a particular language, format or method, including easy read format, then this need will be met by the ICB wherever possible making use of translation services available.

Information is typically provided in a printed copy when responding by post and PDF document when responding by email. When an email response is provided to a requester email account the information will pass across the open network. The ICB can encrypt the PDF document, on request, using secure software which will require a password to be set up by the requester on receipt of the email. Once the password is set up and entered, the encrypted document can be opened.

4. Responding to requests

Requests may arrive into the ICB by post or email and the ICB has 30 days from the date of receipt to:

If a SAR:

- Gather information from all work areas
- Collate the information gathered
- Appraise and apply any legal exemptions which may apply such as for third party content, legal privilege or information which has the potential to cause harm
- Remove duplication where necessary
- Redact and respond

If an alternative rights request:

- Consider the scope of what has been asked for
- Assess what information is held and where
- Consider appropriate actions to take
- Provide a suitable response

The response clock begins ticking on the day of receipt and a response must be provided by the same date of the following month.

For example:

1. If the ICB receives a request on 14 May, the time limit starts from the same day. The ICB will have one month to reply which means a response will be sent by or on 14 June.
2. The day of receipt is regarded as day one of the countdown. However, requests received after office hours, 5.00pm on Friday evening, will not activate the response clock until the following Monday morning when office hours begin again.
3. If the response date falls on a Saturday, Sunday or Bank Holiday, the 30 days ends on the next working day.

All information rights requests relating to personal information, regardless of the format or method of requests, received into the ICB must be sent to the Head of information governance (HOIG) immediately in order that the process can begin.

Specific details of receipt and response date requirements will be contained within the operating procedure for SARs and can also be found on the Information

Commissioner website https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/

VERIFYING IDENTITY

If ICB has doubts about the identity of the person making the request we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. We will take into account what data we hold, the nature of the data, and what we are using it for.

We will let the individual know without undue delay that we need more information from them to confirm their identity. We do not need to comply with the request until we have received the additional information.

Examples of suitable documentation are:

- Valid Passport
- Driving Licence
- Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old) or a Medical Card

5. Other requests

REQUESTS FOR DECEASED INDIVIDUALS RECORDS

While UK GDPR only applies to living individuals, The Access to Health Records Act 1990 (AHRA) provides a small cohort of people with a statutory right to apply for access to information contained within a deceased person's health record.

Individuals who have a right of access under the AHRA are defined under Section 3(1)(f) of the Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.

The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record.

Access to Health Records requests should be responded to within 40 calendar days and there can be no charge for the request.

For more information, contact the Head of Information Governance (HOIG).

6. Responsibilities

This policy applies to all staff, or those working on behalf, or representing the ICB in the management of all personal data that is collected, stored, processed and destroyed by the ICB.

Breaches of this policy may be managed through the ICB disciplinary policy and procedure, which is available on the ICB document library along with all other associated policies.

The HOIG, Data Protection Officer duties are to:

- Act as the central point for receipt and management of information rights
- Ensure the identity of the requester is appropriate to the request, taking account of any ongoing relationship between the ICB and the individual
- Ensure that where requests are made on behalf of data subjects that the appropriate checks are made regarding identity, consent and addresses for responses
- Acknowledge receipt of the request and provide to the requester with an expected response time
- Ensure relevant teams are contacted to undertake timely, robust and comprehensive searches
- Ensure the collation of all information provided by staff in all formats in a timely manner
- Review the content of all information provided by staff to ensure appropriate content and removal of duplication where necessary
- Ensure the application of exemptions where necessary for example removal of third party personal information, legal privilege, removal of information with the potential to cause harm
- Ensure the provision of a response to the requester in a requested format or method of provision

Managers will ensure that staff:

- Understand and adhere to the principles of the Data Protection Act 2018 and associated legislation as provided within the annual information governance training
- Who receive information requests send them to HOIG immediately
- Perform a thorough search for information when requested by HOIG and provide it within the timescale set out in that request

Staff are expected to:

- Have knowledge of this policy and adhere to the Data Protection Act 2018 and caldicott principles, in accordance with their employment contract clauses and data security training
- Send any information rights requests to the HOIG immediately (any verbal requests for information must also be directed to the HOIG)
- Ensure that a thorough search of all information storage areas takes place in response to any request from the HOIG
- Respond promptly to requests for information from the HOIG within the stated timeframe to ensure the ICB can respond within the 30 day deadline

All staff should be aware that due to the timescales involved in dealing with requests for information, it is sometimes necessary during prolonged staff absence to access

individual accounts such as email to carry out searches and retrieve the required information.

The Data Protection Act provides for penalties that could be imposed upon the ICB or its employees for non-compliance with relevant legislation and NHS guidance. Data protection and confidentiality both form part of staff contractual clauses and are always applicable, even after the contract has terminated.

Under no circumstances should staff delete any person identifiable information after receiving a SAR.

Staff have the same rights under the Data Protection Act as any member of the general public and are therefore entitled to make a SAR for their own information.

7. Should you be unhappy with a response

In the event that a requestor is unhappy with a response to their Information Rights Request provided by the ICB, they should contact HOIG and request a review of the request and response to allow this to be resolved informally.

If a requestor believes that personal information is missing or has not been provided, they should clearly list, in writing, what other information they think the ICB hold. This will help with a review of records.

In the event that an informal complaint resolution cannot be reached internally, the Information Commissioners Office (ICO) has a general duty to investigate complaints from members of the public who believe that an organisation has failed to respond correctly to an information rights request. Requestors can make a complaint to the ICO in writing to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Fax: 01625 524510

Make a complaint | ICO

8. Implementation plans and monitoring effectiveness

Compliance with this policy will be monitored through the information governance sub-committee (IGSC) and the audit committee. Relevant requirements include:

- Data security and protection toolkit
- Audit(s) completed by ICB internal auditors
- SAR Log – all requests received and actions

- Quarterly SARs Report

All information rights requests received will be logged and reported to the IGSC in an anonymised or statistical format.

Breaches of this policy will be managed, where appropriate, through the ICB disciplinary policy and procedure, which is available on the ICB document library along with all other associated policies.

As requests continue to be dealt with, audit of response times and process reviews will take place and any new learning will be incorporated into future versions of this document.

9. Update and review

This policy will typically be reviewed in three years, but will be re-considered and updated sooner, if needed. Ongoing review will take place to ensure effectiveness, taking account of any learning from requests and responses dealt with.

10. Other relevant policies

There is a wide range of legislation and policies which link to this policy which can be found in Appendix 1.

Appendix 1: Legal and regulatory framework

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

Data Protection Act 2018
General Data Protection Regulations
Data Protection Policy
Information Governance Policy
Freedom of Information Act 2000
Freedom of Information Policy
Human Rights Act 1998
Access to Health Records 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
Electronic Communications Act 2000
Environmental Information Regulations 2004

Health and Social Care Act 2012
Information security management: NHS code of practice
Information security policy
Acceptable use policy
Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
Mental Capacity Act 2005
NHS constitution
Public Records Act 1958
Data security and protection toolkit
Email policy

The above list is not exhaustive.

ICB policies can be found here: Policies and procedures - NHS Cornwall and Isles of Scilly (icb.nhs.uk)

All legislation can be found here: Legislation.gov.uk

The Information Commissioner website is a useful source of advice and guidance: https://ico.org.uk/your-data-matters/official-information/

Appendix 2: Equality impact assessment

Name of policy or service to be assessed: Subject access request policy
Department or section: Information governance
Date of assessment: 16 December 2022
Person(s) responsible for the assessment: Beverley Gallagher
Is this a new or existing policy? Existing

Aims, objectives and purpose of the policy

Describe the aims, objectives, and purpose of the policy.
The policy outlines the ICB's legal obligations under Data Protection Act 2018 and provides documented evidence of the organisational commitment to dealing with requests for personal information appropriately, efficiently and in compliance with legislation.

Who is intended to benefit from this policy, and in what way?
Policy is intended for staff and public guidance

What outcomes are wanted from this policy?
Clear description of legal obligation for reader understanding of who is allowed to ask for what and what the timescale is which needs to be met by the organisation when a request is received. An organisational statement of intent to meet its legal obligation. Staff guidance in dealing with requests for information both internally and from the general public.

What factors or forces could contribute or detract from the outcomes?
Timeframe for meeting requests for information could be missed if staff do not understand the quick turnaround needed from them to allow the organisation to meet its obligations.

Who are the main stakeholders in relation to the policy?
Main stakeholders are the ICB, its staff and members of the public requesting information held about them.

Who implements the policy, and who is responsible for the policy?
Head of information governance and information governance subcommittee.

Differential impacts

Does this have a positive or negative impact on people from an ethnic minority background? How will any negative impact be mitigated?
There are no differential impacts from this policy as every request is dealt with in the same way and will follow internal process, regardless of who it is from. Should there be a need for an individual to receive a response in a particular language, format or method, then this need will be met by the organisation wherever possible. Should requests require a specific language, format or method of response, use will be made of translation services available, technology/electronic/hard copy provision of the information and any external guidance available.

Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?
No impact has been identified for this protected characteristic. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of disability? How will any negative impact be mitigated?
There are no differential impacts from this policy as every request is dealt with in the same way and will follow internal process, regardless of who it is from. Should there be a need for an individual to receive a response in a particular language, format or method, then this will be met by the organisation wherever possible. Information can be provided in easy read format if needed or provided in differing languages making use of any translating services needed. As part of the redaction and review process consideration would also be given to the potential of harm to the individual. There are no aspects of the policy which have a negative impact on people with a disability. Where redaction process has been rigorous, individuals have the right to redress.

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual? How will any negative impact be mitigated?
There are no differential impacts in this policy for people of differing sexual orientation. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
There are no positive or negative differential impacts in this policy for people of any age. Information can be provided in easy read format if needed or provided in differing languages making use of any translating services needed. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
There are no positive or negative differential impacts in this policy for people of any religion or belief. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies. How will any negative impact be mitigated?
There are no positive or negative differential impacts in this policy for people regardless of marital status. No negative impact identified.

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary, or gender fluid? How will any negative impact be mitigated?
There is no differential impact on people from the perspective of gender re-assignment. No negative impact identified

Does this have a positive or negative impact on people who are pregnant, breast feeding mothers, or those on maternity leave? How will any negative impact be mitigated?
There is no differential impact on people from the perspective of pregnancy and maternity. No negative impact identified.

Are they any other identified groups? How will any negative impact be mitigated?
No differential impact on other identified groups has been identified. No negative impact identified to be mitigated.

Human rights values

How have the core human rights values of fairness, respect, equality, dignity, and autonomy been considered in the formulation of this policy, service, or strategy?
Reference to the legislation is included within the document. Data Protection Act 2018 and therefore data subject rights take account of rights under the Human Rights Act Article 8.

Which of the human rights articles does this document impact?

☐ To life
☐ Not to be tortured or treated in an inhuman or degrading way
☐ To liberty and security
☐ To a fair trial
☒ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience, and religion
☐ To freedom of expression
☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☐ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?
Review of the Human rights statement and guidance has taken place and consideration made of the articles.

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?
Reference to the Human Rights Act is contained within the document.

Public Sector Value Act 2012

NHS Cornwall and Isles of Scilly is committed and obliged to fulfil the requirements of the Public Sector Social Value Act 2012. This Act requires the organisations to

consider how services commissioned or procured might improve the economic, social, and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system, and community.
The policy includes the requirement for staff to complete mandatory data security awareness training which increases skills and maintains employment with the ICB. Content of data protection standards ensure that local systems used for processing information are scrutinised and audited for security and integrity providing the right information in the right place at the right time including the provision of information in response to subject access requests.

Describe how the policy contributes towards eliminating discrimination, harassment, and victimisation.
N/A

Describe how the policy contributes towards advancing equality of opportunity.
N/A

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
N/A

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and or the working environment for that group of people.
N/A

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
N/A

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.
N/A

Equality impact assessment action plan

Issue to be addressed	Action required	Responsible person	Timescale for completion	Action taken
N/A	N/A	N/A	N/A	N/A

Comments on action plan:
N/A

Signed (completing officer): Head of information governance

Date: 21 December 2022

Signed (head of department or section): Head of information governance

Date: 21 December 2022

Please ensure that a signed copy of this form with the policy is sent to both the corporate governance team and equality and diversity lead.