NHS
Cornwall and
Isles of Scilly

Data protection 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: Data protection policy
Lead directorate: Transformation and partnerships
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 number	Revision date	Revision by	Nature of revisions
V1.0	April 2022	Head of information governance	Minor changes to job titles and committee names.
V1.0	17 May 2022	People and organisational governance committee	Policy ratified by the committee
V2.0	1 July 2022	Head of Information Governance	Rebadged to reflect transition to an Integrated Care Board.
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
V2.1	5 March 2025	SCW CSU IG Consultant	Review and update ahead of DSPT Toolkit

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

Contents

1. Introduction 5
2. Purpose 5
3. Definitions 5
4. Responsibilities 6
5. Related Policies and Documents 7
6. Related Legislation and Guidance 7
7. Overview of the Data Protection Act 2018 & the General Data Protection Regulations 7
8. Data Protection Principles 8
   - 8.1 Principle 1: Lawfulness, fairness and transparency 8
   - 8.2 Principle 2: Purpose limitation 8
   - 8.3 Principle 3: Data minimisation 9
   - 8.4 Principle 4: Accuracy 9
   - 8.5 Principle 5: Storage limitation 9
   - 8.6 Principle 6: Integrity and confidentiality (also known as Security) 9
   - 8.7 Accountability Principle 10
9. Employees 10
10. Disclosure of Personal Confidential Data 10
11. Rights of Individuals 11
   - 11.1 The right to be informed 11
   - 11.2 The right of access 11
   - 11.3 The right to rectification 12
   - 11.4 The right to erasure 12
   - 11.5 The right to restrict processing 12
   - 11.6 The right to data portability 13
   - 11.7 The right to object 13
   - 11.8 Rights in relation to automated decision making and profiling 14
   - 11.9 What to do if you receive such a request? 14
   - 11.10 National Data Opt-Out 15
12. Retention and Disposal of Information – Records Management 15
13. Reporting Data Protection Breaches 16
14. Data Protection Contractual Clauses 17
15. Data Protection by Design and Default 17
16. Data Protection Impact Assessments 18

17. Training Requirements 19
18. Monitoring Compliance and Effectiveness 19
19. Update and Review 19
Appendix 1 Regulatory Framework 20
Appendix 2: THE ICB Related Policy Documents 22
Appendix 3: Equality Impact Assessment 23
Aims, objectives and purpose of the policy 23
Differential impacts 24
Human rights values 26
Public Sector Value Act 2012 26
Equality impact assessment action plan 27

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 and information security. It also has a duty to comply with guidance issued by the Department of Health and Social Care (DH), the Information Commissioners Office (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the ICB. Penalties could be imposed upon the organisation, and/or ICB employees for non-compliance with relevant legislation and NHS guidance.

2. Purpose

This Data Protection policy aims to detail how the ICB meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are primarily based upon two key pieces of legislation: the Data Protection Act 2018 and the UK General Data Protection Regulations. However, other relevant legislation and appropriate guidance is also referenced.

It should be remembered that this policy relates to personal confidential information relating to the following areas:

- Patients and members of the public in contact with the ICB
- Employees/workers
- Providers of services, contractors or agency workers

Further advice on determining what constitutes personal data can be found on the ICO website here Information Commissioner's Office (ICO)

3. Definitions

Data controller: the person (or organisation) that collects personal data and decides on how to use, store or distribute that data.

Data processor: any person or organisation (other than an employee of the data controller) that processes personal data on behalf of the data controller.

Data subject or natural person: an individual who is the subject of the personal data.

Personal confidential data: data that relates to a living individual that can identify the individual from this data or other information in the possession of the data controller (for example name address, postcode or NHS number).

Sensitive personal data or special category data: data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, biometric or genetic information, sex life, criminal proceedings or convictions.

General Data Protection Regulation (GDPR): this is the legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR came into effect across the EU on 25 May 2018 and seeks to harmonise data protection legislation across the EU. The UK's Data Protection Act 2018 (DPA2018) encompasses the expectations and responsibilities outlined in the UK GDPR.

4. Responsibilities

The ICB has a legal duty to comply with the Data Protection Act (DPA) 2018 which encompasses the General Data Protection Regulations. The accountable officer is responsible for ensuring that the responsibility for data protection is allocated appropriately within the ICB and that the role is supported.

The ICB is responsible for the implementation of this policy and for ensuring that:

- All staff dealing with personal confidential data are aware of the need for compliance with the Act and associated provisions
- All staff are aware of the requirements of the Common Law Duty of Confidentiality as set out in the NHS Code of Practice on Confidentiality 2003
- The ICB is aware of the detailed provisions of the DPA 2018 and secondary legislation and of any subsequent guidance issued by the Department of Health and Social Care or by the Information Commissioner
- Processing of personal data in the ICB is compliant with the DPA 2018
- Notification to the Information Commissioner (where required) of processing of personal data by the ICB is up to date
- The appointment of a Data Protection Officer and the allocation of a director with responsibility for information risk is delegated appropriately
- Data quality accountability is incorporated within job descriptions
- Contracts include DPA 2018 compliant clauses, including additional rigour for those organisations acting as a joint data controller and/or data processor
- There is a scheduled and regular review of this policy

Information asset owners are responsible for understanding and addressing information governance risks relevant to the "information assets" that they own. They should have comprehensive procedures in place for ensuring the integrity and availability of the data they hold and process as well as identifying and correcting data errors.

Managers and information asset owners within the ICB are responsible for ensuring the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. The DPA 2018 introduced the concept of "data protection by design and default". Its aim is to ensure organisations consider, at the earliest stage, systems and processes which safeguard privacy and data protection principles right from the outset ('data protection by design') and, by default, they ensure personal data is processed with the highest privacy protection, for example only the data necessary is processed, a short storage period is maintained, there is limited accessibility so that personal data is not made widely available ('data protection by default').

All staff must adhere to ICB policies and procedures relating to the processing of personal information. Of equal importance is the appropriate retention and disposal of records in accordance with the ICB's records management policy.

All staff members are responsible for maintaining compliance with the data protection principles and for reporting non-compliance through the ICB incident reporting process. Support, guidance and training is available through the head of information governance (HOIG) who can be contacted on ciosicb.corporategovernance@nhs.net.

5. Related policies and documents

This policy should be read in conjunction with the policies set out in appendix 2.

6. Related legislation and guidance

The data protection policy should be read in conjunction with the legislation and national guidance listed in appendix 1.

7. Overview of the Data Protection Act 2018 & the General Data Protection Regulations

The GDPR seeks to harmonise data protection legislation across Europe. The approach of the GDPR is to ensure that organisations providing services or goods are required to comply with the GDPR should they process (hold, obtain, record, use or share) and information pertaining to an EU citizen. The DPA 2018 enshrines the expectations and responsibilities outlined within the GDPR within UK legislation.

The GDPR sets out specific rights of individuals and affirms that proactively organisations must assure themselves as to the use of, transfers of, and legal basis for processing of all the information they hold. Further, where new uses or processes for information are introduced, these must be subject to a Data Protection Impact Assessment (DPIA), and in certain circumstances, approval must be obtained by the

supervisory authority before that processing may commence. The supervisory authority for the UK is the Information Commissioner.

This legislation applies to all person identifiable information held in manual files, computer databases, videos and other automated media, about living individuals. The legislation dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff may result in disciplinary action.
The legislation also requires the ICB to register its information held manually and on computers and other automated equipment with the ICO. Part of the registration process is to ensure transparency exists so that individuals are aware of the purposes for holding their data, how it is used and to whom it may be disclosed.

Within the DPA 2018 an individual can request access to their personal information regardless of the media in which this information may be held / retained. The ICB has an Information Rights management policy and procedure for dealing with such requests.

8. Data protection principles

As noted above, the DPA 2018 establishes the legislative requirements of the GDPR. Both affirm the following principles for the management of person confidential data (PCD):

8.1 Principle 1: lawfulness, fairness and transparency

- You must identify valid grounds (known as a 'lawful basis') for collecting and using personal data. As a health organisation the ICB may rely on consent for processing personal data.
- You must ensure that you do not do anything with the data in breach of any other laws
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned
- You must be clear, open and honest with people from the start about how you will use their personal data

8.2 Principle 2: purpose limitation

- You must be clear about what your purposes for processing are from the start
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law

8.3 Principle 3: data minimisation

You must ensure the personal data you are processing is:

1. Adequate – sufficient to properly fulfil your stated purpose
2. Relevant – has a rational link to that purpose, and,
3. Limited to what is necessary – you do not hold more than you need for that purpose

8.4 Principle 4: accuracy

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact
- You may need to keep the personal data updated, although this will depend on what you are using it for
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible
- You must carefully consider any challenges to the accuracy of personal data

8.5 Principle 5: storage limitation

- You must not keep personal data for longer than you need it
- You need to think about – and be able to justify – how long you keep personal data; this will depend on your purposes for holding the data
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes

8.6 Principle 6: integrity and confidentiality (also known as security)

- A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
  Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.

- You also must consider additional requirements about the security of your processing – and these also apply to data processors.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures and undertake any required improvements.

8.7 Accountability principle

There is an additional principle which relates to accountability. For each of the above, the data controller (the ICB) is responsible for, and must be able to evidence and demonstrate, compliance with the six principles above.

9. Employees

All employees are data subjects under the Act. As such, the data held by the ICB regarding employees is treated with the same importance and sensitivity as other personal data held by the organisation.

Any member of employees, current, past or potential (applicant) who wishes to have a copy of the information the ICB holds on them under the right of access provisions of the DPA 2018 may make an application to the Data Protection Officer of the ICB.

The Human Resources directorate will ensure all employees have valid contracts of employment which will include specific clauses for data protection and confidentiality, as well as maintaining the integrity and availability of personal information. Breaches of the Data Protection policy will be addressed through the ICB's disciplinary procedures and may need to be reported to the ICO and data subjects depending upon the degree of risk associated with the breach. A copy of the ICB's relevant information governance and HR procedures are available from the document library.

10. Disclosure of personal confidential data

Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, individuals also have the right to expect that their personal data will be properly protected. When sharing personal information, ICB staff must ensure that the principles (and rights of individuals) contained within the DPA2018, the GDPR, the Human Rights Act 1998, the caldicott review principles and the Common Law Duty of Confidentiality are upheld.

The disclosure of personal data can only be made where there is a legal basis for doing so. Members of staff should contact the HOIG if they are ever unsure about sharing personal data.

Please contact the HOIG for further advice prior to releasing any form of disclosure of personal information such as disclosure to the police, the media etc.

11. Rights of individuals

All individuals (staff, patients, anyone the ICB has information about) have the following rights under GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

11.1 The right to be informed

Articles 12, 13 and 14 of the GDPR relates to an individual's right to be informed. This is a key transparency requirement under the DPA 2018. Information provided to individuals must be clear and concise about how the ICB processes data (including personal data, pseudonymised data and anonymised data).

The information about the processing must be easily accessible (for example, via a website or published on a leaflet); be written in clear and plain language (particularly if addressed to a child) and provided free of charge. This is often referred to as a "privacy notice." This is available on the ICB website.

11.2 The right of access

The right of access is commonly referred to as 'subject access' or a 'subject access request'. This right gives individuals the right to request a copy of and / or to view their personal data held by an organisation. It helps individuals to understand how and why as an Integrated Care Board (ICB), we use their data and to provide reassurance that we are doing so lawfully. In addition, data can also be checked for accuracy.

An individual and/or their legal representative are the only people who can request access to their personal data processed by the ICB. All requests should be sent to the corporate governance team and there is a strict one calendar month period for providing this information.

11.3 The right to rectification

Individuals have the right to have inaccurate personal data rectified (Article 16 of the GDPR). The GDPR does not give a definition of the term accuracy. However, the DPA 2018 states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact. Steps may have already been taken to ensure that the personal data was accurate when obtained but this right imposes a specific obligation to reconsider the accuracy upon request.

However, altering medical records is complex. Individuals should be able to report factual inaccuracies or question the content of the medical records but they do not have the right to alter their contents because they are upsetting or they disagree with them.

You cannot alter a record that is an accurate representation of the situation at the time the record was written. However you can make an additional note to record that the individual disagrees with the opinion.

Once again, changes requested should be rectified within 30 days. If, following due consideration, the ICB choose not to make the requested changes, it must notify the individual accordingly providing its rationale. This is only likely to happen in exceptional circumstances. As with any matter of data protection, should the individual disagree with the decision made by the ICB, they are entitled to complain to the Information Commissioner.

11.4 The right to erasure

Individuals have the right to have personal data erased (Article 17 of the GDPR). This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances.

Please note the right to erasure does not apply for direct healthcare information processed by the ICB. Consent is not a legal basis for processing personal data for direct care in the NHS and therefore this right does not apply. (The lawful basis is typically one of the following: legitimate interests, public tasks, vital interests or legal obligation.)

The lawful basis for processing an employee’s personal data is typically performed via the contract mechanism established as part of their recruitment process. However, consent does apply for some aspects of employment and additional information held for purposes other than direct care.

11.5 The right to restrict processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how the data has been processed. In most cases, it will not be required to restrict an individual's personal data indefinitely, but it will be necessary to have the restriction in place for an identified period of time.

11.6 The right to data portability

The right to data portability gives individuals 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.

The right to data portability applies when:

- The lawful basis for processing the information is consent or for the performance of a contract; and
- Processing is being carried out by automated means (such as excluding paper files).

Examples of where this right may be exercised include the history of website usage or search activities, traffic and location data; or 'raw' data processed by connected objects such as smart meters and wearable devices.

This right is not applicable to standard healthcare records such as those relied upon by GPs or hospitals. At this point in time, it is unlikely to apply to ICB activities.

11.7 The right to object

Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask the ICB to stop processing their personal data.

Individuals can object if the processing is for:

- a task carried out in the public interest
- the exercise of official authority vested in you
- your legitimate interests (or those of a third party)

In these circumstances, the right to object is not absolute and any refusal to do so needs to be fully explained to the individual.

If processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

An individual can ask that the ICB stop processing their personal data for direct marketing at any time. The ICB does not undertake direct marketing at the time of writing this policy.

11.8 Rights in relation to automated decision making and profiling

Automated individual decision-making and profiling is a decision made by automated means without any human involvement. Examples of this include an online decision to award a loan, a recruitment aptitude test which uses pre-programmed algorithms and criteria, etc.

GDPR restricts organisations from making solely automated decisions, including those based on profiling, which have a legal or similarly significant effect on individuals.

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

There is particular applicability here to data processed by Artificial Intelligence (AI) which may involve automated decision-making. If unsure, please consult your HOIG.

11.9 What to do if you receive such a request?

If you receive a request for personal information or rectification and deletion of information, please ensure you:

1. Acknowledge the request from the individual
2. Contact the HOIG immediately who will log the request and instigate the appropriate next steps
3. Stop any processing of the individual’s data whilst a decision is made
4. Document the decision you make and the reasons for it
5. Confirm the outcome and rationale with the HOIG so that they may inform the individual and explain if they are dissatisfied, they are able to make a complaint to the ICO.

The HOIG will be able to advise you on the steps to making an appropriate decision regarding the request you have received.

As noted above, decisions need to be made and communicated to the individual within one calendar month. If the individual is dissatisfied with the outcome of their request, they can complain to the ICO.

Further information regarding these rights can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

11.10 National data opt-out

The latest opt-out model introduces a single national data opt-out choice for patients to say if they do not want their identifiable data used for research or planning purposes. It allows individuals to register their choice online, using a system being designed by NHS Digital, or by using a non-digital alternative. All health organisations are required to advise patients appropriately and they are expected to uphold these patient choices accordingly.

There are 2 types of opt-out:

Type 1 opt-out: medical records held at your GP practice – opting out means the information held as part of a patient's GP medical record will only be used for the purpose of their individual care

Type 2 opt-out: information held by NHS Digital – opting out means the confidential information held by NHS Digital will not be shared for purposes other than a patient's individual care.

This is now referred to as the national data opt-out and applies to health and care system information held in England. It does not apply to records held in Scotland, Wales or Northern Ireland.

More information is available here: Overview – Choose if data from your health records is shared for research and planning - NHS (www.nhs.uk)

12. Retention and disposal of information – records management

Maintaining the confidentiality, integrity and availability of personal information is essential. Of equal importance is how long information is held for and how it is safely disposed of. This ensures Principle 5 'storage limitation' is complied with - see section 8.5 above.

The benefits of effective records management are:

- Protecting business critical records and improving business resilience
- Ensuring information can be found and retrieved quickly and efficiently
- Complying with legal and regulatory requirements

- Reducing the risk for litigation
- Minimising storage requirements and reducing costs

It should be remembered records management applies to all ICB activities, not just those relating to personal and confidential information. The ICB records management policy therefore includes the retention and disposal periods for the following areas:

- Health and social care records
- Staff records and occupation health
- Procurement – includes contracts and both successful and unsuccessful tenders
- Corporate governance – for example minutes, policies, incidents, destruction certificates.
- Communications – for example press releases, consultation and engagement, website
- Financial records – for example accounts, expenses, transactions, salary and pensions
- Legal, complaints and information rights – for example litigation, FOI requests, subject access requests, complaints, intellectual property

A copy of the records management policy is available on the document library and further advice is available from the HOIG.

Staff should also remain mindful when managing staff personnel files (p-files) ensuring information is appropriately filed, providing access to a p-file as part of a subject access request or informal or formal disciplinary and grievance investigations. In such cases, staff are requested to contact the HR team for advice.

13. Reporting Data Protection breaches

Each personal data breach must be reported to the HOIG as soon as it becomes apparent. Working with the responsible team, the HOIG will consider the breach in terms of the likelihood and severity of any risk to people's rights and freedoms. In accordance with the GDPR, all breaches considered high risk must be reported to the ICO within 72 hours reported via the data security and protection toolkit (DSPT), and as part of that process, a decision will also be taken on the appropriateness of informing the individuals involved. All the relevant information and the resulting decisions and actions will be incorporated within the ICB's caldicott guardian's log. Breaches should be reported using the following email address: ciosicb.corporategovernance@nhs.net.

The ICB has a duty to record and report data breaches made by their own staff as well as breaches by other organisations who have shared information inappropriately. For further information on breaches and incident management please consult the Incident Management Procedure, accessible within the Document Library.

14. Data Protection contractual clauses

The ICB is responsible for obtaining appropriate contractual assurance in respect of compliance with information governance (IG) requirements from all bodies that have access to ICB information or conduct any form of information processing on its behalf. This is particularly important where the information is about identifiable individuals as this is a legal requirement. The assurance sought from each organisation can be in the form of their self-assessment under the DSPT or via affirmation of their compliance with the DAP2018/GDPR.

All contractors or support organisations (including non-clinical staff) with access to personal data (that the ICB is the data controller for) must be identified and appropriate clauses for inclusion in contracts must be developed. Please note the majority of ICB formal contracts are based upon the standard NHS contract which stipulates information governance requirements.

15. Data protection by design and default

To increase accountability and focus, 'data protection by design and default' is now a legal requirement under the GDPR. Organisations must be able to demonstrate how they are complying with its requirements and obligations.

The key is to consider data protection issues from the start of any processing activity and adopt appropriate policies and measures which meet the expected requirements. Whilst not an exhaustive list, the following provides examples of areas to consider:

- Minimising the processing of personal data
- Pseudonymising personal data as soon as possible
- Ensuring transparency in respect of the functions and processing of personal data
- Enabling individuals to monitor the processing, and/or,
- Creating (and improving) security features

The underlying concepts are expressed in the 7 'foundational principles':

1. 'Proactive not reactive; preventative not remedial' - take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact.

2. 'Privacy as the default setting' - design any system, service, product, and/or business practice to protect personal data automatically

3. 'Privacy embedded into design' - embed and ensure data protection forms part of the core functions of any system, service or business practice

4. ‘Full functionality – positive sum, not zero sum’ - also referred to as ‘win-win’, look to incorporate all legitimate objectives whilst ensuring you comply with your obligations, such as avoid trade-offs

5. ‘End-to-end security – full lifecycle protection’ - put in place strong security measures from the beginning and extend this security throughout the whole ‘data lifecycle’, such as retention and disposal of records is just as important

6. ‘Visibility and transparency – keep it open’ - ensure business practices or technology can be independently verified with ease

7. ‘Respect for user privacy – keep it user-centric’ - keep the interest of individuals paramount in the design and implementation of any system or service

For more information regarding data protection by design and default refer to HOIG.

16. Data protection Impact Assessments

Data protection Impact Assessments (DPIAs) are a tool required by the GDPR to build DPA 2018 compliance into projects and initiatives. They are a legal obligation for high risk projects and must be shared in advance (and before processing commences) with the ICO if an organisation is unable to mitigate the high risks. For medium or lower risk areas they provide an approach that helps comply with legal obligations.

DPIAs are intended to build in “privacy by design” and are also intended to prevent privacy related problems from arising, by:

- Considering the impact on privacy at the project start
- Identifying ways of minimising any adverse impact
- Building this into the project as it develops as regular reviews shall be undertaken

It is expected that a DPIA is used to capture how data will be processed within the ICB and should be completed where any project or proposal will:

- Introduce a new or additional piece of IT that will relate to the management of personal confidential data (PCD)
- Introduce a new process that requires the use of PCD where it has previously been conducted anonymously
- Involve a change in how the ICB will handle either (a) large amounts of PCD about an individual, or (b) PID about a large number of individuals
- The ICB Data Protection Impact Assessment policy and procedure are available through the document library for this purpose.

17. Training requirements

The Data Protection Officer has responsibility for maintaining training and awareness of confidentiality and information security issues for all staff. However, the ICB's Caldicott Guardian is also able to provide advice on the sharing of, and access to PCD.

All new starters must undertake data security training as part of their induction process. Information governance training, also referred to as data security and awareness training, is mandatory and must be completed annually. The preferred method is through one of the e-learning modules available through ESR.

Some staff members are required to undertake additional information governance training as appropriate to their role. A data security and protection training needs analysis is reviewed by the head of information governance each year as part of the DSPT framework.

18. Monitoring compliance and effectiveness

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

- DSPT
- Audit(s) completed by the ICB internal auditors
- Information asset registers and the mapping of data flows
- Reports from Royal Cornwall NHS Hospital Trust (RCHT) and Cornwall Partnership NHS Foundation Trust (CFT) who support THE ICB in discharging their responsibilities under the DPA 2018
- Testing undertaken regarding pseudonymisation and any risks associated with the re-identification of personal data
- Information governance contractual arrangements
- Caldicott guardian log – the information governance breaches
- Data protection impact assessments

The ICB should also regularly use spot checks to ensure data protection and information governance guidance is being followed. The results of staff spot checks and actions taken when non-compliance is identified will be reported to the information governance sub-committee and will also inform the staff training and the training needs analysis.

19. Update and review

This policy will be reviewed in 3 years, but will be updated and re-considered sooner, if needed.

Appendix 1 regulatory framework

Data protection and 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.
All legislation can be found here: Legislation.gov.uk

The following are the main publications referring to security and confidentiality of personal identifiable information:

HSCIC: guide to confidentiality 2013
Caldicott Review 2013
ICO Employee code of practice
Records management: NHS code of practice 2016

ISO/IEC 27001:2005 and 17799:2005 information security standard
Further guidance can also be found via the DSPT (Data Security and Protection Toolkit (dsptoolkit.nhs.uk)).

Appendix 2: ICB related policy documents

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

Information governance strategy
Information governance 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
ICB privacy notice
Home working policy
Information sharing protocols and agreements
Serious incident policy
Confidentiality code of conduct for employees
ICB information governance handbook
Data privacy impact assessment policy and procedure

This list is not exhaustive.
ICB policies can be found here: Policies and procedures - NHS Cornwall and Isles of Scilly (icb.nhs.uk)

Appendix 3: equality impact assessment

Name of policy or service to be assessed: Data protection policy
Department or section: Information governance
Date of assessment: 05/08/2022
Person(s) responsible for the assessment: Head of information governance
Is this a new or existing policy? Existing

Aims, objectives and purpose of the policy

Describe the aims, objectives, and purpose of the policy.
This policy identified above outlines how the 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, UK General Data Protection Regulations (UKGDPR) and the Data Protection Act 2018 (DPA 2018). The policy provides guidance to staff to ensure the consideration of legal responsibilities and the privacy of all individuals when processing data. The requirements within the policy are primarily based upon the DPA 2018 which is the key piece of legislation covering security and confidentiality of personal information.

Who is intended to benefit from this policy, and in what way?
The 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.

What outcomes are wanted from this policy?
That the information processed by the 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.

What factors or forces could contribute or detract from the outcomes?
Staff awareness of the content of the policy and staff completing data security awareness training will contribute to information governance practices

Who are the main stakeholders in relation to the policy?
The main stakeholders are the ICB Board and its constitutional committees to meet its responsibilities. In addition, the data protection officer, the HOIG, all staff as well as the information governance subcommittee have key operating functions and responsibilities for implementing information governance throughout the ICB. These policies are also important for individuals in the community.

Who implements the policy, and who is responsible for the policy?
The data protection officer, HOIG and the information governance subcommittee providing assurance and escalation to the audit committee.

Differential impacts

Does this have a positive or negative impact on people from an ethnic minority background? How will any negative impact be mitigated?
The policy reflects 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 policy 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'.

Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?
The policy supports 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.

What is the positive or negative differential impact on people from the perspective of disability? How will any negative impact be mitigated?
The policy outlines 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. 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.

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?
The policy supports 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.

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
The policy supports 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.

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
The policy supports 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'.

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?
The policy supports 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.

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?
The policy outlines the legal basis for collecting sensitive information, limits how and when it may be shared and when it should be destroyed. It also outlines the expectations of staff to maintain confidentiality.

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?
The data protection policy includes the requirement for training of all staff to information governance standards. Data security awareness 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.

Are they any other identified groups? How will any negative impact be mitigated?

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, to exercise their rights, may need to speak rather than write to the ICB formally.

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?
The requirements and principles of the Data Protection Act, which is linked to the Human Rights Act, have been considered when writing this policy, including the individual rights of data subjects. Fairness in informing individuals of the uses of their data in a fair processing notice has been produced, respect for privacy, dignity and choice have been written into all information governance policies.

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?
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.

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.

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.

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 policy also allows for individuals to rectify information where it is believed to be held incorrectly.

Describe how the policy contributes towards advancing equality of opportunity.
The policy describes 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.

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
The policy sets 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.

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.
The policy can be provided in multiple formats if necessary.

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: 5 August 2022

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

Date: 5 August 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.