NHS
Cornwall and
Isles of Scilly

Information Governance 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 Governance policy
Lead directorate: Corporate governance
Lead team: Information governance
Document type: Policy
Subject category: 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. Minor factual changes.
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	19 February 2025	IG Consultant/ Senior IG Consultant (SCW CSU)	Review and update ahead of DSP Toolkit submission

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

Contents

1. Introduction 4
2. Scope of the Policy 4
3. Purpose of the Policy 4
4. Information Governance Principles 5
5. Confidentiality & Data Protection 6
6. Information Sharing 6
7. Risk Management and Information Security 7
8. IG Incident Reporting & Management 8
9. Change Management 8
10. Records and Information Management 8
11. Information Quality 9
12. Responsibilities 9
13. Training and Awareness Requirements 10
14. Implementation plans and monitoring effectiveness 10
15. Update and review 11
16. Related policies referred to in this document 11
17. Consultation on this policy 11

Appendix 1: The Ten National Data Security Standards 12
Appendix 2: legal and regulatory framework 15
Appendix 3: ICB related policy documents 16
Appendix 4: Equality impact assessment 17

1. Introduction

1.1. Information Governance (IG) is a framework to manage information appropriately.

1.2. For personal information, IG ensures confidentiality and security as well as that processes are in place to ensure appropriate standards of quality and ethical use.

1.3. Corporate information and records must also be managed appropriately, where possible to be provided to the public to ensure transparency and accountability.

1.4. Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning, delivery and performance management

1.5. It is of paramount importance to ensure that information is efficiently and securely managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

1.6. Information Governance (IG) encompasses the following areas:

- Data protection, confidentiality and compliance with legislation
- The Caldicott principles
- Information security and cyber security
- Records management and data quality
- Business operations and management
- Business intelligence – including 'big data', procurement and finance

2. Scope of the Policy

2.1. This document is applicable to all staff, volunteers, contractors and third parties who work on behalf of the ICB.

3. Purpose of the Policy

3.1. The purpose of this policy is to describe a system that ensures NHS Cornwall and Isles of Scilly Integrated Care Board (ICB) meets its responsibilities for the management of its information assets and resources.

3.2. This IG policy framework ensures the following objectives are achieved:

- Information will be organised and managed in accordance with mandated and statutory standards and kept confidential where necessary.

- Ensure the ICB's employees understand their own responsibilities regarding Information Governance.
- Ensure the ICB's compliance with legal and regulatory frameworks will be achieved, monitored and maintained.
- All information risks will be identified and mitigated and in accordance with the ICB's Corporate Risk Management Strategy.
- Support the lawful sharing and disclosure of information to support care and the public interest.

3.3. **Legal Framework** - The ICB adheres to several legal obligations regarding the use and security of personally identifiable information, detailed in Appendix 3.

3.4. **Regulatory Framework** - Based on the legislation in Appendix 2, the NHS mandates compliance with information governance regulations through a national programme. Organisations must meet and evidence performance against the Data Security and Protection (DSP) Toolkit.

4. Information Governance Principles

4.1. The ICB upholds a balance between openness and confidentiality in information management. It prioritises safeguarding personal information for patients and staff, supporting IG principles, public accountability, and lawful, controlled sharing of patient information with health organisations and agencies when in the public or patient's interest.

4.2. Accurate, timely, and relevant information is vital for quality healthcare delivery. Managers and clinicians are responsible for ensuring high-quality information and its effective use in decision-making.

4.3. This IG policy encompasses five interconnected areas:

- **Openness**: Ensures non-confidential information is accessible to the public and patients, with clear procedures for queries and media engagement. Aligns with the Freedom of Information Act, NHS Constitution, and Data Protection Act.
- **Legal Compliance**: Safeguards patient and staff information in compliance with legal requirements like the Data Protection Act, Freedom of Information, and Health and Social Care Act, while facilitating lawful information sharing.
- **Information & Cyber Security**: Implements secure management of information assets, risk assessments, and staff training. Monitors and investigates security incidents, adhering to BS ISO/IEC 27001 standards.
- **Quality Assurance**: Sets policies for information quality, promotes data accuracy at the point of collection, and supports national data standards through training and procedures.

- **Records Management**: Establishes effective record-keeping policies, aligning with NHS Code of Practice standards, with regular audits and staff training.

5. Confidentiality & Data Protection

5.1. The ICB regards all identifiable personal information relating to patients as confidential and will ensure that its employees comply with NHS Code of Practice on Confidentiality.

5.2. The ICB will maintain a privacy notice, or fair processing notice, which details how the ICB processes personal data including what personal data is held, for what purpose it is processed and who it is shared with and what governs that processing.

5.3. The ICB will establish and maintain procedures/protocols to ensure compliance with the Data Protection Act, Human Rights Act and the common law of confidentiality.

5.4. The ICB will promote effective confidentiality and security practice to its staff through policies, procedures and mandatory training.

5.5. The ICB will protect patient data by ensuring that when used for secondary purposes (i.e. not for the direct care of the patient), this data is protected by a combination of effective anonymisation, Safe Haven principles or procedures and Pseudonymisation.

5.6. The ICB will use pseudonymised, anonymised or de-identified patient data for specified commissioning purposes and to analyse and inform better health care decisions for individuals and the community when required to do so.

5.7. The ICB will adhere to the NHS England and NHS Digital Confidentiality codes of conduct by complying with the Confidentiality and Data Protection Assurance standards set out in the NHS Information Governance Toolkit.

6. Information Sharing

6.1. The ICB will establish and maintain protocols for the controlled and appropriate sharing of patient information with other agencies and third parties, taking account of relevant legislation (e.g., Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

6.2. The ICB will engage with partner organisations to support appropriate information sharing which ensures that the patient and public can exercise choice as well as ensuring they are kept informed about proposed uses and sharing of their information.

6.3. Key responsibilities for IG will be included in contracts and service level agreements between the ICB, partner organisations, and external providers and suppliers.

6.4. The ICB will put arrangements in place to ensure specific information sharing contracts are signed with contractors and other third parties and are regularly monitored.

6.5. Where information (patient or otherwise) is used or shared for direct care purposes, it must be ensured by staff that it is only the minimum amount necessary to achieve the intended purposes. Where use carries risk to individuals, consideration should be given to the completion of a Data Protection Impact Assessment (DPIA). Advice and guidance should be sought from the HOIG.

7. Risk Management and Information Security

7.1. Information security has three basic components. These are:

- **Confidentiality** - Access to information must be confined to those with specified authority to view the data.
- **Integrity** - Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to specification and in the way the current user believes them to be operating.
- **Availability** - Information must be available and delivered to the right person when it is needed.

7.2. Certain categories of information e.g. personal or organisation sensitive information will be kept secure and made available to only those who need it.

7.3. Access to ICB information systems, such as email, databases, the internet, network, and records of the ICB, are provided to staff for business purposes. All access and use must be appropriate and in line with the discharge of their duties.

7.4. The ICB is committed to ensuring that all information for which it is responsible and that of its' partners, hosted bodies, which relates to patients, clients and staff, is processed, protected, and disclosed appropriately to provide improved healthcare and decisions for patients.

7.5. The ICB will establish and maintain policies for the effective and secure management of its information assets and resources. The policies will ensure that all information and data is held in a consistent and systematic manner that ensures its confidentiality, availability, and integrity throughout its lifecycle.

7.6. All ICB, information Assets will be protected by appropriate information security measures.

7.7. Information risks to each information asset will be identified and mitigated and where necessary serious risks will be added to the Corporate Risk Assurance Framework in line with the ICB' s Risk management Policies and Procedures.

8. IG Incident Reporting & Management

8.1. The ICB will manage and report IG incidents in line with the NHS England guidance on reporting IG incidents.

8.2. The ICB will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of information security and confidentiality.

8.3. All employees will be required to report all actual or suspected IG breaches to ensure that lessons are learned, and processes and procedures reviewed.

9. Change Management

9.1. Any change processes within the ICB will take consideration of the requirements to ensure the appropriate and effective information management within the ICB.

9.2. The ICB will ensure that change is undertaken in a structured and systematic manner that ensures information governance issues are dealt with in a timely, proportionate, and appropriate manner.

9.3. All new projects or changes to systems will be subject to privacy impact assessment to identify potential IG risks at the earliest stage of the project lifecycle as possible.

10. Records and Information Management

10.1. The ICB will promote information quality and effective records management through policies, procedures/user manuals and training and ensure that information is fit for purpose and that collection and processing is cost effective.

10.2. All information will be managed and held within a controlled environment. This includes personal data of patients and staff, patient level data (non-identifiable) as well as corporate information. This applies to records; information and data regardless of format, in addition to legacy data held by the organisation.

10.3. All staff within the ICB are committed to a systematic and planned approach to the Management of Records within the organisation, from their creation to their ultimate disposal.

10.4. Records will be disposed efficiently when no longer needed. ICB will comply with the NHS records Management Code of Practice.

10.5. Administrative systems contain vital records on which patient care and service provision depend. ICB will ensure that staff are fully aware of the measures that are necessary to comply with current Records Management best practice.

10.6. All information will be used, created, and managed in a professional and business-like manner. It must be accessible to the Organisation on a long-term basis and must be stored in a systematic and consistent manner.

10.7. As employees create information, they are doing so on behalf of the ICB, for example when sending emails. All employees are accountable for the information they create for its appropriateness and accessibility.

11. Information Quality

11.1. The ICB will establish policies procedures protocols and guidance to ensure that all information and data processed, held, and managed is of the highest quality in terms of completeness, accuracy, relevance, accessibility, and timeliness supported by process that validate and ensure its reliability.

11.2. Wherever possible, information quality must be assured at the point of collection. Data standards will be set through clear and consistent definition of data items, in accordance with NHS and national standards

12. Responsibilities

12.1. **The ICB Board** - It is the role of the ICB board to define the ICB's policy in respect of IG, taking into account legal and NHS requirements. The board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

12.2. **The Chief Executive** – The Chief Executive is responsible for ensuring that sufficient resources are available to support the implementation of Information Governance procedures to ensure compliance with legal and professional requirements and the NHS Information Governance requirements.

- As the accountable officer for the ICB, the Chief Executive has overall accountability for IG in the ICB and is required to provide assurance, through the statement of internal control (SIC), that all risks relating to information are effectively managed

12.3. **The SIRO** - The nominated Senior Information Risk Owner (SIRO) will act as an advocate for information risk at board level and via any internal discussions. The SIRO is responsible for providing written advice to the accountable officer on the content of the annual SIC regarding information risk.

12.4. **The Head of Information Governance (HOIG)** is responsible for raising awareness throughout the ICB regarding the requirements of the DSP Toolkit, for ensuring mandatory standards are met and providing support to ICB staff and work streams.

- Support, guidance and training is available through the HOIG who can be contacted via ciosicb.corporategovernance@nhs.net.

12.5. **The Information Governance Steering Group (IGSG)** is responsible for overseeing day to day IG issues. It ensures the annual IG work plan is maintained and monitored against the requirements of the Data Security and Protection (DSP) Toolkit through the co-ordination of different work streams such as developing and maintaining policies, strategies, structures, procedures and guidance and raising awareness of IG. The committee also ensures annual assessments and submissions of the Toolkit are undertaken. The IGSG is accountable to the Audit Committee.

12.6. **All Managers** within the ICB are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

12.7. **All staff,** whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day-to-day basis.

13. Training and Awareness Requirements

13.1. Staff will be made aware of this policy through training and induction for new staff.

13.2. Information Governance Training will be included as part of mandatory induction for new staff.

13.3. The IG Lead will be responsible for producing awareness material to be published as part of staff bulletins and to be published on ICB's intranet.

14. Implementation plans and monitoring effectiveness

14.1. The Senior Management will be responsible for monitoring and implementing this policy.

14.2. Staff guidance, protocols and procedures will be developed and made accessible to staff as part of the implementation of this policy.

14.3. Information risk assessments will be regularly carried out to ensure that the policy framework is fully implemented.

14.4. As part of implementing this policy in the ICB the following standard procedures/protocols will be put in place;

- **Staff Confidentiality Code of Conduct -** to set out the standards expected of staff in maintaining the confidentiality of patient information;
- **Staff Access Control and Password management Procedures -** sets out procedures for the management of access to computer-based information systems;
- **Data Transfer Procedures -** sets out procedures around the secure transfer of data, collecting consent and maintaining confidentiality within ICB including the use of safe havens;

- **Incident management Procedures** - sets out the procedures for managing and responding to a security breach;
- **Business Continuity Procedures** - sets out the procedures in the event of system failure;
- **Portable Device Staff Guidelines** - provides guidance for staff use on the use of portable devices.

15. Update and review

This policy will typically be reviewed in 3 years but can, should legislation change, be re-considered sooner, if needed.

16. Related policies referred to in this document

There are a wide range of policy documents which support this policy which can be found in appendix 3

17. Consultation on this policy

This policy was reviewed and updated when the ICB was established. Consultation on a draft of the policy was carried out via staff bulletin and circulation to senior management prior to ratification. Previous versions of the policy have included review by local security management specialists and the IGSC. No major changes have been made to policy content since those consultations took place as IG standards have remained the same.

Appendix 1: The Ten National Data Security Standards

Data Security Standard 1 - personal confidential data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.

Personal confidential data is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and expertise is on hand to help them make sensible judgments. Staff are trained in the relevant pieces of legislation and periodically reminded of the consequences to patients, their employer and to themselves of mishandling personal confidential data.

Data Security Standard 2 - understand your responsibilities

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

Data Security Standard 3 - training

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised DSP Toolkit.

All staff complete an annual security module, linked to 'CareCERT Assurance'. The course is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

Leadership obligation 2 – process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses

Data Security Standard 4 - managing data access

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff should not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc.).

Data Security Standard 5 - process reviews

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it is not being done properly.

Data Security Standard 6 - responding to incidents

Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

All staff are trained in how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. [The Board] understands that it is ultimately accountable for the impact of security incidents and bear the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

Data Security Standard 7 - continuity planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

A business continuity exercise is run every year as a minimum, with guidance and templates available from [CareCERT Assurance]. Those in key roles will receive dedicated training to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.

Leadership obligation 3 – technology: ensure technology is secure and up-to-date

Data Security Standard 8 - managing unsupported systems

No unsupported operating systems, software or internet browsers are used within the IT estate.
Guidance and support is available from CareCERT Assurance to ensure risk owners understand how to prioritise their vulnerabilities. There is a clear recognition that not all unsupported systems can be upgraded and that financial and other constraints

should drive intelligent discussion around priorities. Value for money is of utmost importance, as is the need to understand the risks posed by those systems which cannot be upgraded. It is about demonstrating that analysis has been done and informed decisions were made.

Data Security Standard 9 - IT protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

[CareCERT Assurance] assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes. There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

Data Security Standard 10 - accountable suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

IT suppliers understand their obligations as data processors under the GDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall 'attack surface'. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.

From 2024-25, the ICB as a Category 1 organisation must complete a CAF aligned Data Security and Protection Toolkit (DSPT). Previously, the ten National Data Security Standards formed the basis for the DSPT, which has now transitioned to the Cyber Assessment Framework.

Appendix 2: legal and 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
- Common Law Duty of Confidentiality
- Records Management 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

Appendix 3: ICB related policy documents

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

- Information Governance strategy
- 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
- ICB privacy notice
- Home working policy
- Information sharing protocols and agreements
- Serious incident policy
- Confidentiality code of conduct for employees
- 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 4: Equality impact assessment

Name of policy or service to be assessed: Information Governancepolicy
Department or section: Governance
Date of assessment: 23 August 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.
The policies identified above outline 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, 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

Who is intended to benefit from this policy, and in what way?
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?
Major incident involving the use of information or data could detract from attaining normal Information Governancecontrols. Staff awareness of the content of the policies and staff completing Information Governancetraining will contribute to Information Governancepractices and will detract from outcomes if not adhered to.

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 head of information governance, all staff as well as the Information Governancesub committee have key operating functions and responsibilities for implementing Information Governancethroughout the ICB.
These policies are also important for Individuals in the community.

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

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 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'.

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 policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of sex.

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

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 policies support the protection of all 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 policies support the protection of all 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. The policy applies to all staff regardless of age.

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 policies support the protection of all 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 policies support the protection of all 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 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 including employees.

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. 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 all 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 other identified groups. However there may be a positive impact in that the policies set out how all 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?

N/A

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 and associated policies also allow 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 and its associated 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.

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

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 and its associated policies 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: 24 August 2022

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

Date: 24 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.