Confidentiality & Data Protection Act policy

NHS Devon

Version	3
Policy Sponsor	Chief Communications and Corporate Affairs Officer
Policy Lead	Company Secretary
Approved by	Chief Communications and Corporate Affairs Officer and Director of Operational Finance
Approved on	13/12/2023
To be reviewed by	13/12/2025

Document change history (to add rows, copy and paste)			
Date	**Change**	**Version number of policy**	**Comments**
25/01/2023	Policy Amendment	2.1	Updated by SCW IG Service following review
18/10/2023	Policy Amendment	3	Policy Review by SCW IG service – new template adopted. 5.3.1 8th Caldicott Principle added. Change from NHS Digital to NHS England throughout. New paragraph regarding consent added to policy.

Equality, diversity and inclusion statement

NHS Devon is committed to the promotion of equal opportunities, addressing health inequalities and fostering of good relations between people protected under the terms of the Equality Act 2010, the Health and Social Care Act 2012 and Human Rights legislation. We are equally committed to the elimination of unlawful discrimination, harassment and victimisation. To demonstrate this commitment, we develop, promote and maintain policies, strategies and operating procedures. Every effort is made to ensure that patients, employees, contractors or visitors do not experience discrimination; either directly or indirectly, because of their vulnerability; disadvantage; age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion and belief; sex (gender) or sexual orientation.

All staff must comply with this policy. Compliance must reflect our organisational commitment to and policy on, equality, diversity and inclusion. In addition, each manager and member of staff involved in implementing this policy must give due regard to the needs of those protected under law.

If you, or any other groups, believe you are discriminated against under the terms of the Equality Act, the Health and Social Care Act 2012 or Human Rights legislation by anything contained in this document; or you need this document in an alternative format, for example, large print, Braille, Easy read or other languages; please contact our Patient Advice and Complaints Team (PACT):

Tel: 0300 123 1672
Email: pals.devon@nhs.net

Contents

1. Introduction

1.1 The ICB processes information about individuals, including patients and staff. As an organisation, we are therefore required to comply with the Data Protection Act 2018 and UK GDPR. As a part of the NHS, we are obligated to follow the NHS Confidentiality Codes and comply with the Caldicott Principles. As an employer, we have obligations of confidentiality and under data protection principles concerning our staff.

1.2 1.2 The role of the ICB is to support the commissioning of healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the ICB will uphold the NHS Constitution. This policy is important because it will help the people who work for the ICB to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

2. Purpose and objectives

2.1 This policy aims to detail how the ICB meets its legal obligations and NHS requirements concerning confidentiality and information security standards. This policy provides reference and guidance as outlined by the Data Protection Act 2018 and other legislation.

2.2 This policy aims to detail how the ICB meets its legal obligations and NHS requirements concerning confidentiality and information security standards. This policy provides reference and guidance as outlined by the Data Protection Act 2018, UK GDPR 2021, and other legislation.

2.3 Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources, and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2.4 Information Governance (IG) looks at the way the NHS handles information about patients, staff, contractors, and the healthcare provided, with consideration of personal and confidential information. Without access to information, it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- IG Management
- Confidentiality and Data Protection Legislation assurance

- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

The aims of this document are to maximise the value of organisational assets by ensuring that information is:

- **H**eld securely and confidentially
- **O**btained fairly and efficiently
- **R**ecorded accurately and reliably
- **U**sed effectively and ethically
- **S**hared appropriately and lawfully

To protect the organisation's information assets from all threats, whether internal or external, deliberate, or accidental, the ICB will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained, and tested
- Information security training will be available to all staff

3. Scope

3.1 All teams and employees within the organisation have a duty under the Act to hold, obtain, record, use, and store all Personal Confidential Data necessary to perform their role in a secure and confidential manner. All processing of personal data by, or on behalf of the organisation must be in accordance with the seven Data Protection Principles. In addition, for patient data, the Caldicott Principles must also be followed.

3.2 This policy encompasses such data processing activities as patient administration/payment, employee, and staff administration, purchasing, invoicing and treatment planning, payroll and the use of manual records relating to individuals whose information may be held within the organisation. This list is not exhaustive.This policy applies to all staff of NHS Devon

4. Definitions

To assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents

Terms	Definition
Personal Data (Derived from the UK GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (Derived from the UK GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition Their sexual life or gender identity
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to NHS Devon ICB or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

5. Legislative Framework

5.1 **Data Protection Act 2018**

5.1.1 The Data Protection Act 2018 (the Act) regulates the "processing" (which broadly means the obtaining, using, holding, and disclosing) of data relating to individuals. "Data" includes computerised files and manual records forming part of a relevant filing system i.e., a structured set of paper records from which one can readily extract information on an individual. The Act only applies to living people, although the requirements of the Access to Health Records Act 1990, which covers both living and deceased patients, is also applicable to the ICB.

5.1.2 The Act, which should be read alongside the UK General Data Protection Regulation 2021 (UK GDPR), replaced the Data Protection Act 1998 on the 25th of May 2018, to coincide with the adoption of Regulation (EU) 2016/679.

5.1.3 The Act dictates that information should only be disclosed on a need-to-know basis, for legitimate reasons connected with the ICB's business or through a defined legal requirement. 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 can be considered a disciplinary offence.

5.1.4 The Legislation stipulates that there shall be accountability which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. There must also be appropriate measures and records in place to be able to demonstrate compliance.

5.1.5 The DPA 2018 provides conditions for the processing of any personal data. It also makes a distinction between personal data and special categories of personal data.

5.1.6 The legislation listed below also refers to issues of security and/or confidentiality of personal confidential data.

- Data Protection Act 2018
- Police and Criminal Evidence Act 1984
- Access to Medical Reports Act 1988
- Access to Health Records 1990
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000

- Health and Social Care Act 2001
- NHS Act 2006
- Health and Social Care Act 2012
- UK GDPR 2021

5.2 NHS Guidance

5.2.1 Confidentiality: NHS Code of Practice. November 2003

The Code's purpose is to provide guidance to the NHS and NHS related organisations on patient confidentiality issues. It also considers ways of obtaining and using patient information to comply with Data Protection legislation, current and planned.

5.2.2 Supplementary Guidance: Public interest disclosures. November 2010

This document expands upon the principles set out within the Department of Health's key guidance Confidentiality: NHS Code of Practice. The document is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest.

5.2.3 Data security and protection requirements 2019/20

Document outlining action expected from health and care organisations in 2019/20, to implement recommendations by the National Data Guardian. ICBs, as discrete NHS organisations responsible for their corporate IT services, must comply with the requirements set out in this document. As commissioners of GP IT services, ICBs must ensure commissioned GP IT providers are contractually required to comply with these requirements.

5.2.4 Records Management: Code of Practice for Health and Social Care. 2021

This Code is a key component of information governance arrangements for the NHS. It sets out the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.

5.3 Caldicott Principles

5.3.1 These are specific requirements highlighted within the Caldicott principles that apply to patient identifiable information. The ICB will adhere to these principles.

1. Justify the purpose.
2. Don't use patient identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient-identifiable information.
4. Access to patient identifiable information should be on a strict need-to-know basis.
5. Everyone with access to patient identifiable information should be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is

used.

5.4 Data Protection Principles

5.4.1 There are seven principles of good practice within the Data Protection Act 2018. These are normally referred to as the Data Protection Principles.

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (principles 1-6).

Principles 1,2 & 3

5.4.2 The Act requires that all organisations process data lawfully, fairly and in a transparent manner in relation to the data subjects, which includes NHS patients and ICB staff. Transparency requires that all processes are fair and lawful, and only collected for specified, explicit and legitimate purposes. To this end, data subjects must be made aware of why the NHS needs information about them, how it is used and to whom it may be disclosed. Patients will be notified by providers at the point of care as well as by the ICB via a Fair Processing Notice (FPN) published on the ICB's website. Patient information leaflets and posters will also be produced as required and made available in the relevant patient areas in primary and secondary care across the ICB. All ICB staff will be notified during induction, as well as via communications from the Data Protection team. As a way of showing transparency, NHS Devon ICB publishes a Privacy Notice which explains how personal data is used and can be found on our website https://onedevon.org.uk/download/privacy-notice/?wpdmdl=1479&refresh=63d003cd618d51674576845

5.4.3 The Act requires every data controller who is processing personal information to register with the Information Commissioner. The ICB will notify the Information Commissioner's Office (ICO) of its data processing intentions and the subsequent registration will be renewed annually. The ICB will also register the details of its Data Protection Officer. All registrations can be viewed online via a publicly available Register of Data Controllers held by the ICO. The ICB's registration number is

ZA517803.

5.4.5 In practice, ICB uses patient data for investigating incidents arising from primary and secondary care for uses allowed under section 251 of the NHS Act 2006 CHC funding applications and GP referrals to secondary care. Additionally, the ICB receives pseudonymised patient information from the Data Services for Commissioners Regional Office (DSCRO) South-west for non-direct care purposes. The ICB needs to plan and commission healthcare services in its local area through analysis of actual and projected use of services across all parts of the care economy. This modelling requires access to information about care provided to patients, their hospitals stays and patient journeys but without accessing personal confidential patient data. This service allows the ICB to plan and commission those healthcare services in its local area using the services provided through the DSCROs.

Principle 4

5.4.6 The ICB must ensure that all information held on any media is accurate and up to date. The Data Quality Group will provide assurance regarding the accuracy of the ICB's data by implementing validation routines, some of which will be system specific, and details must be provided of these validation processes to the system/information users. Users of software will be responsible for the quality (i.e., Accuracy, Timeliness, and Completeness) of their data by carrying out their own data quality audits and participating as required in any data quality assurance processes.

5.4.7 Staff should ensure that the information held by the ICB is kept up to date during contact with patients by requesting that they validate the information held.

Principle 5

5.4.8 All records are affected by this principle regardless of the media in which they are held, stored and retained. The Information Governance Alliance's "Records Management – Code of Practice for Health and Social Care" and NHS England's Retention Schedule and Disposal Guidance provides comprehensive guidance for ICBs.

5.4.9 The fifth data protection principle makes it clear that data should not be kept for longer than necessary. Where "clear" data (i.e., patient identifiable) is processed by the ICB it should be held in clear form for as short a time as possible. Clear data should be pseudonymised or anonymised before use wherever possible.

5.4.10 For further guidance please refer to the ICB's Information Lifecycle Management Policy and the Records Management Code of Practice (2021)

Principle 6

5.4.11 All information relating to identifiable individuals must be always kept secure. The ICB will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction, and

damage to this information. Details of this are within the Information Security Policy.

5.4.12 ICB staff must report without delay to the information governance team, via Datix (accessible via a desktop link) all potential data security breaches, regardless of severity. All incidents will be assessed and where necessary reported via the Data Security and Protection Toolkit. Breaches will be reported to the ICB's Audit Committee bi-annually and DSPG quarterly.

5.5 Rights of the Data Subject

The Act affords individuals the following rights:

- The right to be informed.
- The right of access.
- The right to restrict processing.
- The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.
- The right to erasure.
- The right to object to processing.
- The right to rectification (Where inaccuracies have been found).
- The right to Data portability (Where the lawful basis for processing is consent).
- The right to raise a concern.

5.6 Subject Access Requests

The ICB maintains clear procedures and arrangements for handling requests for information from the public and members of staff. Please refer to the ICB Individual Rights Policy and Standard Operating Procedure in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.

5.7 Consent

5.7.1 NHS Devon rarely relies on consent under the UK GDPR for processing any personal data. However where this is the case it is documented in the organisations Data Flow Maps (DFMs). The Data Flow Maps contain columns identifying which legal basis the flow of data is covered by under UK GDPR. The DFMs also contain a column on the common law duty of confidentiality. Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are required to complete all columns in the DFMs and provide details on their consent processes.

5.7.2 Any team that documents consent (under GDPR or common law) has the process reviewed by the Data Protection Team.

5.7.3 For further guidance on consent please visit the ICOs website: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/ or NHS England's website: Consent and confidential patient information - NHS Transformation Directorate (england.nhs.uk)

6. Roles and Staff Responsibilities

6.1 Every member of staff, whether employed, self-employed, consultant, locum, contractor, or agency, has individual responsibility for compliance with this policy and the requirements of the Data Protection Act 2018. The following roles have additional responsibilities as set out below. Failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action. In some cases, serious breaches such as unlawful obtaining or disclosure of personal information may result in criminal prosecution.

Chief Executive Officer	The Chief Executive Officer has ultimate accountability for the strategic direction and operational management of NHS Devon, including compliance with all legal, statutory and policy requirements. The development of, implementation of, and compliance with this policy is delegated to the Caldicott Guardian, Senior Information Risk Officer and Data Protection Officer, whose details are set out below.
Policy Sponsor	The Policy Sponsor is responsible for: • ensuring that policy is appropriate for consideration for approval; • endorsing this policy ahead of submission for approval; • with the Policy Lead, maintaining and updating procedures/protocols and other supporting documents for this policy;
Policy Lead / Author	It is the responsibility of the Policy Lead / author to: • ensure as far as possible that the policy is in line with Department of Health and Social Care guidance, legal requirements and advice from clinical bodies; • to complete a QEIA and Implementation Plan where required • undertake a fair and proportionate consultation period with the relevant stakeholders as part of the document's development • to ensure that the policy is in alignment with NHS Devon's strategy and values • ensure that the policy is developed, approved, disseminated and monitored as set out in the document; with Policy Sponsors, maintaining and updating procedures / protocols and other supporting documents for this policy.
Caldicott Guardian	The Caldicott Guardian for the ICB is the Chief Nursing Officer who is responsible for safeguarding the confidentiality of patient

	information. In conjunction with the Senior Information Risk Owner (SIRO), the Caldicott Guardian will oversee all disclosures of individual personal information with particular attention being paid to extraordinary disclosures. The Caldicott Guardian for the ICB can be contacted on d-icb.caldicottguardian@nhs.net.
SIRO	The Senior Information Risk Owner (SIRO) for the ICB is the Chief Communications and Corporate Affairs Officer. The SIRO will ensure that the Senior Management Team and Accountable Officer of the ICB is kept up to date and briefed on all data protection and security issues affecting the organisation. Day to day management and ensuring compliance is delegated to the Data Protection Officer.
Privacy Officer	The Privacy Officer ensures that records are only being accessed where there is a legitimate relationship and permission to view, or under appropriate emergency protocols.
Data Protection Officer	The Data Protection Officer is the lead for the ICB in all matters relating to Data Security and Data protection. The role of the Data Protection Officer includes: • overseeing the policies and procedures required by the Act and subsequent regulations, NHS requirements and the Caldicott Principles. • reviewing the ICB's Data Protection registration. • acting as first point of contact for training, advice and support for all staff on matters relating to data security and Protection, which may arise within the organisation. • overseeing the Data Security and Protection Toolkit submissions. • to ensure appropriate notification in compliance with the Data Protection Act is maintained such as the fair processing notice. • dealing with enquiries about data protection issues. • advising and training staff on their data protection responsibilities in conjunction with the Caldicott Guardian responsibility for advising on actual or potential breaches of confidentiality and recommending remedial action. • ensuring the organisation has an action plan for achieving Data Protection related requirements within the NHS England Data Security and Protection Toolkit. • ensuring the ICB has procedures in place to comply with relevant Department of Health best practice guidance such as Confidentiality and Records Management code of practice. • liaising with external organisations on data protection matters. • the development and implementation of information sharing protocols.

	• overseeing all Individual Rights Requests and Access to health records Act disclosures is
Data Protection Steering Group (DPSG)	The DPSG for the ICB is chaired by the DPO and supported by the Caldicott Guardian and SIRO. DPSG has the following responsibilities: • monitoring Data Security & Protection Toolkit submissions by the ICB. • ensuring that policies are developed and updated in line with legislation, contractual requirements, and NHS requirements, as updated from time to time. • identifying any new information (e.g., national guidance, staff or patient feedback) that may trigger review and amendment of policies before the due date. • identifying individuals and groups who must be aware of/work within the confines of this policy and agreeing appropriate dissemination. • advising on training requirements. • ensuring that sufficient resources are provided to support the requirements of the policy and on-going Information Governance agenda.
Audit and Risk Committee	NHS Devon's Audit Committee has responsibility for overseeing and reporting to the ICB Board and for providing assurance on governance and risk management, IG, research governance and equality and diversity issues.
Information Asset Owners and Administrators	To raise the profile of IG throughout the ICB and to provide local 'champions', the ICB has established a network of Information Asset Owners and Administrators IAAs are directly accountable to the IAOs and indirectly to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets and for ensuring all staff complete IG training. This role is in addition to their duties and should be fully supported by their manager and recognised in their job description. IAO's and IAAs also, on an annual basis, are responsible for local assessment of data collections to establish an Information Asset Register (IAR) and Data Flow Map (DFM) which forms a record of processing activity (ROPA) and audit staff compliance with information handling requirements. This important task provides an ICB wide inventory to inform the annual registration with the ICO and highlights potential risk areas that may need risk management intervention. Information assets should include any operating systems, infrastructure, business applications, off the shelf products, services, user-developed applications, records, and information held.

	The IAA's will be briefed on IG developments and receive specific training. Support in the role is available at any time from the IG Team. An IAO and IAA forum has been established for IAOs and IAAs to attend and chaired by the DPO to discuss all requirements that the IAOs and IAAs need to complete and to brief the forum on all IG matters.
Line Managers	Line managers have a responsibility to ensure their staff comply with NHS Devon policies and standards within their areas of responsibility. Line manager: • are instructed in their Data Security & Protection responsibilities and complete Data Security & Protection training specific to their job role. • are trained in the secure use of computer systems/media. • are aware of their data protection obligations, this policy and associated procedures /guidelines and any updates. • are able to identify and know how to deal with Individual Rights Requests and Freedom of Information requests. • know how to access and store personal identifiable information, both in manual and electronic records. • ensure no unauthorised staff are allowed to access any computer system utilised by the organisation. • ensure access control of all staff as described within the Information Security Policy. • ensure current documentation is regularly maintained for all critical job functions to ensure continuity in the event of individual unavailability.
All Staff	Employed or engaged staff have a duty to comply with NHS Devon policies and standards as outlined in their contracts of employment and codes of conduct. Every member of staff (including agency, bank, locums, volunteers, contractors, non-contract and student placements) will, in the course of their work, process and/or have access to with confidential and/or personal information whether relating to staff, patients or their carers, businesses, family or friends or any other individuals connected to the organisation in some way. All staff are required to: • be made aware of and adhere to this policy, associated procedures/guidelines and all related systems and processes. • attend data protection (or relevant Information Governance) training as appropriate. • ensure that all personal identifiable information is accurate, relevant, up to date and used appropriately, both electronic and manual records including the use of databases. • ensure that all person identifiable information is always kept safe and secure.

	• have signed a contract of employment, a contract for services or a non-disclosure agreement (as applicable) that includes confidentiality, information security and data protection clauses. • understand that breaches of this policy will be investigated by formal disciplinary procedure (or contractual enforcement if appropriate) which may lead to dismissal and/or legal action. Staff should also ensure that they keep their HR information up to date and notify the relevant HR team or their line manager of any relevant changes.

6.2 Data Protection by Design and By Default

The Data Protection Officer (DPO) should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the ICB Senior Information Risk Owner (SIRO) and the Information Asset Owners (IAOs).

All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA and seek review from the IG Team for the ICB prior to approval or further work.
The ICB will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

The UK GDPR requires organisations to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is data protection by design and by default and it means that the ICB integrates data protection into all our processing activities and business practices, from the design stage right through the lifecycle.
Data protection by design is about considering data protection and privacy issues upfront and at the beginning of every processing activity. This helps to ensure that the ICB is compliant with UK GDPR.

7. Implementation

7.1 All staff will be informed of the approval of the Policy via the Staff Bulletin which will provide a link to the document on the NHS Devon Intranet.

7.2 NHS Devon Senior Managers, or their designated representatives, will implement this policy by:

- Notifying all staff of its existence. New staff will be informed of this policy as part of their induction.
- Destroying all superseded paper-based versions of the policy and electronic versions retained in their area.
- Having adequate knowledge of, and / or access to, all relevant legislation in order to ensure that compliance with such legislation is maintained.
- Discussing with staff as part of their regular one-to-ones how they seek to achieve their individual objectives around policy review and maintenance.

8. Approval and Review

8.1 This policy will be reviewed annually, or sooner if required, in order to ensure that it is current, relevant and reflects the strategic aims, objectives, organisational structures and responsibilities of NHS Devon.

9. Monitoring compliance and effectiveness

9.1 This policy and associated appendices and procedures will be monitored by the Data Security and Protection Steering Group. It is also expected that both Internal and External Audit will review this policy and any associated policies and procedures.

9.2 The ICB will ensure that all staff are aware of the policies and requirements regarding data protection and appropriate training arrangements will be made available via ESR and bespoke in-house training relevant to team and individual needs. All ICB staff will also receive data security & protection training as part of the overall induction process.

9.3 Any member of staff current, past or potential (applicant) who wishes to have a copy of their employment information under the subject access provision of the Data Protection Act will need to contact ICB and will dealt with by the Data Protection Team. There are subject access procedures outlining the process to follow to deal with such requests.

10. Quality & Equality Impact Assessment (QEIA)

NHS Devon ICB is committed to the promotion of equal opportunities, addressing health inequalities, and fostering of good relations between people. This means ensuring local people have access to timely and high-quality care that is provided in an environment which is free from unlawful discrimination. It also means that the ICB will tackle health inequalities and ensure there are no barriers to health and wellbeing.

We are equally committed to the elimination of unlawful discrimination, harassment, and victimisation. To demonstrate this commitment, we develop, promote, and maintain policies, strategies, and operating procedures. Every effort is made to ensure that patients,

employees, contractors, or visitors do not experience discrimination; either directly or indirectly, because of their vulnerability; disadvantage; age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion and belief; sex (gender) or sexual orientation.

All staff must comply with this policy. Compliance must reflect our organisational commitment to and policy on, equality, diversity, and inclusion. In addition, each manager and member of staff involved in implementing this policy must give due regard to the needs of those protected under law.

If you, or any other groups, believe you are discriminated against under the terms of the Equality Act, the Health and Social Care Act 2012 or Human Rights legislation by anything contained in this document; or you need this document in an alternative format, for example, large print, Braille, Easy read, or other languages; please contact our Patient Advice and Complaints Team (PACT):

Tel: 0300 123 1672
Email: pals.devon@nhs.net,
Post: Patient Advice and Complaints Team,

NHS Devon Integrated Care Board
Aperture
Pynes Hill
Rydon Lane
Exeter
Devon
EX2 5AZ

NHS Devon ICBs' equality, diversity and human rights work is underpinned by the following:

- NHS Constitution 2015.
- Equality Act 2010 and the requirements of the Public Sector Equality Duty of the Equality Act 2010.
- Human Rights Act 1998.
- Health and Social Care Act 2012 duties placed on ICBs to reduce health inequalities, promote patient involvement, and involve and consult the public.

11. References

Other related policy documents

- NHS England Codes of Practice

  https://digital.nhs.uk/codes-of-practice-handling-information/confidential-information

- Department of Health Code of Practice
  https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- Health and Social Care (Safety and Quality) Act 2015
  http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted
- All ICB Policies, procedures and guidance relating to the management and processing of information within the organisation

Legislation and statutory requirements

- Data Protection Act 2018
- Police and Criminal Evidence Act 1984
- Access to Medical Reports Act 1988
- Access to Health Records 1990
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2001
- NHS Act 2006
- Health and Social Care Act 2012
- UK GDPR 2021

Best practice recommendations and other key guidance

Confidentiality: NHS Code of Practice. November 2003
The Code's purpose is to provide guidance to the NHS and NHS related organisations on patient confidentiality issues. It also considers ways of obtaining and using patient information to comply with Data Protection legislation, current and planned.

Supplementary Guidance: Public interest disclosures. November 2010
This document expands upon the principles set out within the Department of Health's key guidance Confidentiality: NHS Code of Practice. The document is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest.

Data security and protection requirements 2019/20
Document outlining action expected from health and care organisations in 2019/20, to implement recommendations by the National Data Guardian. ICBs, as discrete NHS organisations responsible for their corporate IT services, must comply with the requirements set out in this document. As commissioners of GP IT services, ICBs must ensure commissioned GP IT providers are contractually required to comply with these requirements.

Records Management: Code of Practice for Health and Social Care. 2023
This Code is a key component of information governance arrangements for the NHS. It sets out the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.