Confidentiality & Data Protection Act policy

NHS Devon

Owner(s): *Matthew Spry, Data Protection Officer*	Directorate Contact Details: *D-ICB.dataprotection@nhs.net*	
Approved by: *Data Protection Steering Group (DPSG)*	Date of formal approval 01 July 2022	Review Date: *July 2023*
Date Issued: 05 July 2022		Version 1.0
All policies are held centrally by Governance: d-icb.governance@nhs.net		

Document Change History:		
Version	**Date**	**Comments (i.e. reviewed/amended/approved)**
1.0	01.07.22	
2.0		

Equality, diversity and inclusion statement

NHS Devon ICB 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,
Post: Patient Advice and Complaints Team,
FREEPOST EX184,
County Hall,
Topsham Road
Exeter EX2 4QL

Contents

Section	Title	Page
1	**Introduction**	4
2	**Purpose**	4
3	**Scope**	4
4	**Legislative Framework**	4
	Data Protection Act 2018	4
	NHS Guidance	5
	Data Protection Principles	6
	Rights of the Data Subject	7
	Subject Access Requests	8
5	**Roles and Staff Responsibilities**	8
	Accountable Officer	9
	Caldicott Guardian	9
	Senior Information Risk Owner	9
	Privacy Officer	9
	Data Protection Steering Group	9
	Data Protection Officer	9
	Line Managers	10
	All Staff	10
6	**Monitoring of Compliance**	11

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. As a part of the NHS, we are obligated to follow the NHS Confidentiality Codes and also comply with the Caldicott Principles. As an employer, we have obligations of confidentiality and under data protection principles concerning our staff.

2. Purpose

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.

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 personally identifiable information 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.

4. Legislative Framework

Data Protection Act 2018

4.1 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 particular 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.

4.2 The Act, which should be read alongside the EU General Data Protection Regulation (GDPR), replaced the Data Protection Act 1998 on the 25th May 2018, to coincide with the adoption of Regulation (EU) 2016/679. The GDPR has direct effect across all EU member states and has already been passed. This means organisations will still have to comply with this regulation and we will still have to look to the GDPR for most legal obligations.

4.3 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.

4.4 The legislation listed below also refers to issues of security and/or confidentiality of personal identifiable information/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

NHS Guidance

4.5 *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.

4.6 *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.

4.7 *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.

4.8 *Records Management: Code of Practice for Health and Social Care. July 2016*
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.

Caldicott Principles

4.9 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.

Data Protection Principles

4.10 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

4.11 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.

4.12 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.

4.13 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

4.14 The ICB has to 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.

4.15 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

4.16 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.

4.17 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.

4.18 For further guidance please refer to the ICB's Information Lifecycle Management Policy.

Principle 6

4.19 All information relating to identifiable individuals must be kept secure at all times. 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.

4.20 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 Bi-monthly.

Rights of the Data Subject

4.21 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.

Subject Access Requests

4.22 Individuals have a right to apply for access to health, employment and other type of information held about them on computer and indexed paper records. These requests are made under the provisions of the Act and the following points should be considered:

- Responsibility for dealing with a subject access request lies with the "data controller".
- Requests have a legal time limit of one calendar month in which to respond.
- Requests can be made both verbally, and in writing. If the request is made verbally, it must be followed up in writing, to provide a clear trail of correspondence. No charges can be made for a Subject Access Request, unless it is manifestly unfounded or excessive.

4.23 When responding to a request, the individual must be advised:

- What their data is being used for.
- Who their data is being shared with.
- How long the data will be kept, and how the organisation made this decision.
- Information on their rights to challenge the accuracy of the data held, to have it deleted, or to object to its use.
- Their right to complain to the UK Supervisory Authority (ICO).
- How their data was obtained.
- Whether their data is used for profiling or automated decision making.
- Whether their data has been transferred to a third country, and the security measures used to protect the transfer, if it was.

4.24 The data controller is the legal entity that determines the purposes for which and the manner in which personal data is processed and disclosed. The Data Protection Officer, SIRO or Caldicott Guardian for the ICB will verify and authorise all disclosures. The Data Protection Officer is also responsible for ensuring that Subject Access Requests pertaining to patients and staff are dealt with and that an adequate process is in place to handle Subject Access Requests within the requirement of the Act.

4.25 Individuals have a right to seek compensation from the relevant data controller for any breach of the Act which may cause them damage and/or distress. The ICB's complaints procedures take account of complaints which may be received because of a breach or suspected breach of the Act.

5. Roles and Staff Responsibilities

5.1 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 Act. 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.

Accountable Officer

5.2 The Accountable Officer of NHS Devon Clinical Commissioning Group has overall responsibility within the organisation for compliance with data protection 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.

Caldicott Guardian

5.3 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.

Senior Information Risk Owner

5.4 The Senior Information Risk Owner (SIRO) for the ICB is the Board Secretary. 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 Security and Protection Steering Group (DPSG)

5.5 The DPSG for the ICB is chaired by the SIRO and supported by the Data Protection Officer. The 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.

Data Protection Officer

5.6 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 Digital 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 disclosures of individual personal information.

Line Managers

5.7 Managers will ensure that all staff including contractors, bank, voluntary and other agency staff:

- 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 Subject Access 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

5.8 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.

5.9 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 kept safe and secure at all times.
- 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. Monitoring of Compliance

6.1 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.

6.2 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.

6.3 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.