Information Lifecycle Management policy

NHS Devon

Owner(s):	Directorate contact details:
Data Protection Officer	D-ICB.dataprotection@nhs.net

Approved by:	Date of formal approval:
Audit and Risk Committee	[08.02.2023] [Audit and Risk Committee]

Review date:	Date issued:	Version:
31.10.2023	[08.02.2023]	1.0

Document change history		
Version	**Date**	**Comments (i.e. reviewed/amended/approved)**
0.1	Oct 2022	Transferred from CCG policy
1.0	Feb 2023	Approved by Audit and Risk Committee

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. Purpose

1.1 This policy describes the ICB's approach to information, including legal obligations and NHS guidance. This policy will be supported by policies, procedures and guidance to enable staff to work legally at all times and in applying Caldicott principles.

1.2 The aim of the ICB's Information Lifecycle Management Policy is to ensure that ICB data is 'fit for purpose' at all times and provided on a 'right first time' basis through:

- a systematic and planned approach to records management covering records from creation to disposal;
- efficiency and best value through improvements in the quality and flow of information, and greater co-ordination of records and storage systems;
- compliance with statutory requirements;
- awareness of the importance of information and the need for responsibility and accountability at all levels; and
- appropriate archiving of records.

1.3 The benefits to the ICB are:

- Time saved both in filing and in retrieval of information;
- Decision-making and operations are properly supported and informed by relevant information;
- Record storage is more cost-effective because redundant records can be removed from filing and server space;
- Records are created and managed in compliance with and as required by legislation, standards and regulations;
- Accountability is demonstrated because the records provide reliable evidence of policy, decision making and actions/transactions;
- Duplicates and previous versions are removed as soon as possible;
- Records which the organisation judges to be no longer required are regularly and securely destroyed and the details documented in accordance with the IGA's Records Management Code of Practice;
- More proactive in sharing information and good practice.

2. Executive Summary

2.1 The ICB has developed an Information Lifecycle Management Policy which aims to ensure that the ICB will receive process and transmit information in a deliberate, controlled and secure manner.

2.2 The ICB is permitted to hold patient identifiable data for a number of purposes. Where this is permitted, it will be for specific reasons, such as Continuing Healthcare applications and process, individual funding requests, referral management, safeguarding, complaints management, in the application of the Caldicott principles and invoice validation, the information will be accessible only by those members of staff who have an identified need.

2.3 Corporate information will also be held securely but will be made more widely available across the ICB. Wherever possible, non-confidential information will be pro-actively released onto the ICB's website in the interests of openness and to meet the requirements of the Information Commissioner's Office's publication

scheme.

2.4 The ICB will look after all information securely and will operate according to legislation and NHS guidance.

3. Introduction

3.1 Information is a key asset, and its proper use is fundamental to the delivery of the ICB's obligations and objectives. Information has the most value when it is the right information, in the right place, at the right time.

3.2 The quality and accessibility of information has a significant influence on the functions of the ICB and the ICS. Lack of information or poor-quality information affects:

- Our ability to meet legislative and compliance frameworks from the Department of Health, for example the UK Data Protection Act 2018, Freedom of Information and the annual Data Security and Protection Toolkit
- Adherence to government initiatives and strategic programmes
- Quality and safety of care for our service users
- Effective use of resources (people, equipment, buildings, services)
- Effective management of services and service agreements
- Quality, effectiveness and efficiency of ICB operations
- Reputation of the ICB

3.3 This document sets out an overarching framework for integrating current records management and data quality initiatives, as well as recommending new ones to support the delivery of services provided by the ICB and its partners. It defines a strategy for improving the quality, availability and effective use of information in the ICB and provides a strategic framework for managing all information activities to ensure alignment with the Trust business strategies.

3.4 The Information Lifecycle Management Policy should be read in conjunction with other Data Protection policies.

3.5 Appendix 1 outlines the records that are covered by this policy.

3.6 Appendix 2 is a list of National and local programmes, initiatives, standards and frameworks that have a direct or indirect impact upon records management. This list is not exhaustive.

4. Scope of this Policy

4.1 This strategy relates to the following systems (information assets) and the information contained within the formats outlined in Appendix 1.

- Management systems – finance, HR, commissioning
- Specialist applications, client management and risk management
- Statistical and performance analysis/prediction systems
- Communication and organizational tools – directories, web services,
- Systems for information sharing, collation and analysis

5. Records Management

Network Drives (S Drive) - Electronic Records and Personal Drives

5.1 ICB staff have access to the networks shared S:drive within which there are a number of shared folders, access to which is controlled by the relevant owner. In addition, most staff are provided with a personal Z:drive. The ICB has made a recommendation to all its staff that all electronic records, with appropriate access controls in place, should be saved on shared drives (S: Drive) and not stored on PC hard drives (OneDrive) or on private drives on the network. Shared drives have regular back-up copies scheduled and are undertaken on a daily basis by DELT Shared Services.

5.2 Personal drives should only be used for personal documentation i.e. annual leave, or work in progress which is not yet suitable for sharing with other staff. Documents which have not become records may thus be stored on the private drive, particularly in the early stage of development, but must be transferred to a shared drive once they are open to consultation or become records and may require access to other staff members.

5.3 Upon termination of employment, personal drives will be deleted, and PC hard drives may be checked, and any documents stored thereon may also be deleted or archived as necessary.

5.4 Although intended for personal use the ICB reserves the right to examine the content of a personal drive during or after termination of employment to locate and retrieve any ICB documentation, or records which may have been stored for longer than their purpose. NHS Mail accounts and personal folders of staff members who have left employment with the ICB will be deleted by Delt Shared Services Team after 3 months unless there are extenuating circumstances, for example, an Employment Tribunal claim or litigation case. This will ensure best utilisation of server space, as well as ensuring that records are not held in excess of their retention period. Access must be authorised by the ICBs Head of Digital and the Caldicott Guardian. Every effort will be made not to access or view any genuinely personal material.

Corporate Records

5.5 The majority of corporate records are created in electronic format and are stored in the appropriate folder on the ICB's shared drives, hosted by DELT Shared Services.

5.6 Access to electronic systems is given on completion and submission of the appropriate forms to DELT Shared Services via the appropriate owner.

5.7 The DELT Shared Services ensure information is backed up regularly and accessible at all times.

5.8 The ICB will be guided by the NHSX Records Management Code of Practice 2021 and NHS England's Retention Schedule and Disposal Guidance on the retention and disposal of its corporate records. A copy of this policy can be found on NHSX's website Records Management Code of Practice - NHSX or by contacting the Data Protection Team.

5.9 In relation to the clinical staff required to hold, use or store sensitive and patient

related information, e.g. Designated Safeguarding roles, Continuing Healthcare Team; the ICB will retain for a period of 8 years from last known contact, unless there is an outstanding complaint, incident, retrospective care review, etc., Children's records should be retained for the retention period for the records of children and young people. Mentally disordered persons, (within the meaning of the Mental Health Act 1983) 20 years after the last entry in the record or 8 years after the patient's death, if the patient died while in the care of the organisation. Clients with learning disabilities, see 'Learning difficulties - records of patients with' for guidance.

5.10 Electronic records are to be stored within the ICB's S:Drive whilst paper records are to be stored in a secure cabinet or secure archive facility through the Data Protection Team at d-icb.dataprotection@nhs.net – the ICB uses CareTrack as a clinical system and all records are stored here in line with data protection principles and contract. CareTrack is access controlled.

Employee Records

5.11 Staffs personnel records are held in a safe and secure environment by Human Resouces.

5.12 The ICB has implemented the Electronic Staff Record (ESR) for the central recording of staff information. There are robust processes around access to this personal and sensitive information which is managed by the owner.

ICB Website

5.13 The ICB's website aims to provide:

- information for the residents of Devon concerning the services commissioned
- information for stakeholders about the ways in which the ICB operates, including the strategies which will describe the direction of the ICB's travel
- a mechanism for the ICB to proactively disseminate information.

6. Costs, Savings and Risks

6.1 Considerable investment has already been made in knowledge and information management, through time and effort and the procurement of tools and systems (e.g. MS Teams, SharePoint). The ICB can only benefit from collaborating to identify more effective processes, better use of existing investments and optimum solutions to existing systems.

6.2 The ICB will benefit from increasing the quality and effectiveness of information management by turning time spent searching for information and/or correcting information into time spent applying it.

6.3 To continue creating and storing information individually rather than collectively as a ICB will lead to greater risk in having to recover, reconstruct or do without information in future, which could incur disproportionately high costs in terms of value, resources and time.

6.4 Incomplete or inaccessible information is a risk to the quality and safety of care to

our service users and the effective and efficient delivery of services.

6.5 The ICB currently uses Crown Records located in Exeter for their archiving and secure disposal of archived records. Access to their services, whether that is retrieval of archive material for review, archiving of new material or archiving boxes, and barcodes is through d-ICB.dataprotection@nhs.net

6.6 See appendix 4 for further guidance for records retention pathway.

7. Monitoring Compliance and Effectiveness

Improvement Plan

7.1 Information Governance is about managing information for the benefits of service users, our partners, staff and the public and the quality of that information is just as important for their care, and funding of that care which is dependent upon the accuracy of information as the systems that manage it. Therefore, the work plan to support the Information Lifecycle strategy is integrated into the Data Protection Framework, Strategy & Action Plan.

7.2 This plan will include:

- Improving data quality to support performance reporting, service change and service delivery;
- Undertake a corporate records audit;
- Use the data mapping flow audit and the corporate records audit to highlights areas of risk and develop an action plan to mitigate the risk;
- Continue to audit the Information Asset Register to reduce high risk areas;
- Ensure Information Asset Owners are aware of the responsibilities around quality, training, business continuity, etc;
- Proactively disseminate information to meet legislative requirements through the ICB's website;
- Manage the archiving of records efficient and effectively both on and off site;
- Improve the flow of information within the ICS;
- Provide training and support to staff to support new ways of managing information which will improve efficiency and reduce duplication;
- To review and archive folders and files on the Shared Drives.

Delivery of the policy

7.3 All aspects of this policy will be delivered through the Data Protection Framework, Strategy & Action Plan and related strategies, policies and procedures, and through annual assessment of Information Governance through the Data Security and Protection Toolkit, which is reported through the Data Protection Steering Group, agreed by the Senior Information Risk owner (SIRO) and the Senior Leadership Team.

Monitoring of the policy

7.4 Performance will be monitored by the Data Protection Steering Group using reports generated by the group members, plus the requirements of the Data Security and Protection Toolkit. Formal reports on these topics are regularly presented to the Senior Leadership Team by the Data Protection Team.

8. Related Strategies and Policies

8.1 The Data Protection Steering Group will produce strategies, policies and guidance on areas of Information Governance as required, including but not restricted to:

- Information Lifecycle Management Policy
- Confidentiality and Data Protection Policy

9. Covid-19

9.1 In Mar 2020, the Secretary of State for Health and Social Care released **'Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002'**. The purpose of this Notice is to require organisations to process confidential patient information for the purposes set out in Regulation 3(1) of COPI to support the Secretary of State's response to Covid-19 (Covid-19 Purpose). "Processing" for these purposes is defined in Regulation 3(2) and includes dissemination of confidential patient information to persons and organisations permitted to process confidential patient information under Regulation 3(3) of COPI. **Data received for Covid-19 purposes is retained separately from other ICB business as usual work in readiness for guidance to its longer-term retention.**

9.2 See appendices 4 and 5 for guidance relating to the retention of records for Covid-19 and Test and Track purposes.

Appendix 1

Records covered by this Policy

A record is information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business. (Ref - BS ISO 15489-1)

An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees – including consultants, agency or casual staff. (Ref - DoH Records Management: NHS Code of Practice)

A corporate record is anything that contains information relating to how the organisation conducts its business on a day-to-day basis including service planning and provision, finance, estates, human resources, IM&T, purchasing/supplies. For detailed guidance on the definition of a corporate record, its retention period and disposal guide please refer to NHS England's Corporate Records Retention & Disposal Schedule & Guidance.

Corporate records include the following:

- Administrative records (including personnel, estates, financial and accounting records; notes associated with complaint handling);
- Photographs, slides and other images
- Microform (i.e. fiche and film)
- Audio and video tapes, cassettes, CD-ROM, DVD, etc
- E-mails,
- Correspondence i.e. letters, memos, file notes
- Minutes/notes of meetings,
- Diaries
- Digital records
- Computerised records

The ICB's records will be securely held in the most appropriate format in accordance with the NHS Records Retention Schedule and NHS England's Corporate Records Retention & Disposal Schedule & Guidance.

Where electronic data is sent to the ICB by NHS Digital, the ICB recognises that this is not the original data and so the ICB will only retain this for as short a period of time as possible and for only as long as can be justified.

National and local programmes, initiatives, standards and frameworks

The Public Records Act 1958
All NHS records, and those of NHS predecessor bodies, are public records under the terms of the Public Records Act 1958. The Act sets out broad responsibilities for everyone who works with such records and provides for guidance and supervision by the Keeper of Public Records.

Freedom of Information Act 2000
The organisation should carry out a records audit to determine what records it holds, the locations of the records and whether they need to be kept – this should lead to a review of the organisation's retention schedules and provide information for its publication scheme. There is a duty imposed on organisations to supply information in a timely fashion – currently within 20 working days.

The Environmental Information Regulations 2004
As with the Freedom of Information Act the organisation needs a robust records management programme. The requirements of the two pieces of legislation are similar so it is advised that organisations deal with requests in a like manner. The main difference is that requests for environmental information need not be in writing.

The Re-use of Public Sector Information Regulations 2005
Employees responsible for re-use issues should work closely with those responsible for FOI for several reasons:

- An information audit is required for both pieces of legislation to determine the records held and the locations of those records
- Information available for re-use and the terms and conditions of re-use can be included within the organisation's publication scheme
- If a request is made for access and re-use, the processes need to be co-ordinated so that the access issue is dealt with before permission to re-use is granted.

The Lord Chancellor's Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000
This code sets out the practices that organisations should follow in relation to the creation, keeping, management and destruction of their records.

Data Security and Protection Toolkit
This annual requirement ensures that Information Quality and Records Management arrangements are incorporated within broader information governance arrangements.

NHSLA Risk Management Standards for NHS Trusts
Most healthcare organisations are regularly assessed against these NHSLA risk management standards which have been specifically developed to reflect issues which arise in the negligence claims reported to the NHSLA. There is a set of risk management standards for each type of healthcare organisation incorporating organisational, clinical, and health & safety risks.

Department of Health Code of Practice: Records Management
A guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

Ministry of Justice
The Ministry of Justice is responsible for freedom of information policy in the UK, and for development of the framework for the Act including the provision of guidance and best practice to public authorities and information applicants.

National Archives
The National Archives produces standards and guidance on all aspect of record management within the public sector.

NHS Constitution
This has many commitments on information including the right of access to your own health records which will always be used to manage your treatment in your best interest.

Covid-19: Notice under Regulation 3(4) of the Health Service Control of Patient Information (COPI) Regulations 2002
This requires organisations to process confidential patient information for the purposes set out in Regulation 3(1) of COPI to support the Secretary of State's response to Covid-19 (Covid-19 purpose).

Policy Checklist

Please Delete once the policy is approved. For any further queries or guidance on policy drafting, please contact EMAIL

Topic	Question	Y/N	Comments
Title	Is the title clear and unambiguous?		
	Is it clear whether the document is a strategy, policy, protocol, procedure, integrated care pathway or guidelines?		
Rationale	Are reasons for development of the document stated?		
Development Process	Is the method described in brief?		
	Are people involved in the development identified?		
	Has a reasonable attempt has been made to ensure relevant expertise has been used?		
Content	Is the objective of the document clear?		
	Is the target population clear and unambiguous?		
	Are the intended outcomes described?		
	Are the statements clear and unambiguous?		
Evidence Base	Is the type of evidence to support the document identified explicitly?		
	Are key references adequately cited?		
	Are supporting documents referenced?		
	Does the document identify which committee/group will approve it?		
Compliance Monitoring	Are there measurable standards to support the monitoring of compliance with and effectiveness of the document?		
Review Date	Is the review date identified? If so is it acceptable?		
Responsibility	Is it clear who will be responsible for this policy – including compliance monitoring and review?		
The policy may require consultation if it has a significant effect on staff or service users i.e. HR policies will need to be presented to the Staff Forum. The following questions relate to the Consultation process.			
Consultation	Is there evidence of consultation with People and users?		
	Has the consultation with staff and/or service users been sufficient to gather the necessary feedback?		
	Has the joint Workforce Development/staff Forum approved the document?		