NHS
Bradford District and Craven
Clinical Commissioning Group

Records management and information lifecycle - policy and procedure

Key information

Responsible director:	Liz Allen, strategic head of organisation effectiveness
Clinical Lead:	Gill Paxton, associate director of quality and nursing (deputy caldicott guardian).
Author:	Senior corporate governance officer
Approval body:	Audit and Governance Committee
Date approved:	1 November 2021
Version:	V2
Review date:	Nov 2023

Version control

Version no.	Date	Author	Description	Circulation
V1.0	March 2020	Senior corporate governance officer	Full review and update for new CCG. Guidance taken from Leeds CCGs re approach to policy. Version approved by A&G Committee.	CCG wide
V1.1	November 2020	As above	Updated for accessible content standards.	Head of corporate governance
V1.2	March 2021	As above	Full review and update in light of the draft revision to the NHS records management code of practice (2020)	Records management group
V1.3	August 2021	As above	Further update in light of issue of the finalised NHS records management code of practice	Audit and governance committee

Version no.	Date	Author	Description	Circulation
			2021, including links to the document	
2	1 November 2021	As above	Approved at Audit and Governance Committee 01.11.2021	Intradoc

Contents

1. Introduction

Records management is the process by which organisations manage all the aspects of records they use, whether internally or externally generated and in any format or media type, from their creation or collection, through their life cycle to their eventual disposal.

A record is a piece of information produced or received in the initiation, conduct or completion of an institutional or individual activity. It comprises sufficient content, context and structure to provide evidence of the activity. It contains information that is worthy of preservation in the short, medium or long term.

The Records Management Code of Practice 2021 is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS and social care organisations in England. It is based on current legal requirements and professional best practice.

NHS Bradford District and Craven CCG records are important sources of administrative, evidential and historical information, providing evidence of actions and decisions, and represent a vital asset to support the CCG daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisation, to support services provided and securely store personal information of staff and members of the public. Good quality records also support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

This policy, procedure and supporting guidance provides the framework to enable the efficient and effective management of records.

Non-compliance with this policy will be investigated and may result in the matter being treated as a disciplinary offence under the CCG disciplinary procedure.

The records management code of practice 2021 can be found here;
https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

Information and documents in relation to records management is available on the intranet;
https://nhsbradfordcravenccg.intradoc247.cloud/about-us/teams/browse/1362

1.1 Policy statement

NHS Bradford District and Craven CCG is committed to records management and will create, keep and manage records and document in relation to our principal activities in compliance with the Records Management Code of Practice 2021.

2. Scope

This policy applies to all staff including CCG staff, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG.

It covers all clinical and non-clinical records created, received or maintained within the corporate functions of the CCG, regardless of format (e.g. paper, electronic (intranet, websites, social media), audio visual, text). These include (but are not limited to) records relating to the administration of either CCG, personnel, finance, estates, communications, complaints, legal, commissioning, continuing health care funding, individual funding, individual placements funding.

3. Legislation, guidelines and associated documentation

Records Management must be documented and implemented in line with Records Management Code 2021, and the following legislative and professional requirements:

- Data Protection Act 2018
- General Data Protection Regulation 2016
- The Health and Social Care Act 2008
- Human Rights Act 1998
- The Public Records Act 1958
- The Freedom of Information Act 2000
- Access to Health Records Act 1990
- The Caldicott Report and Information Governance Review 'Caldicott 2'
- Information: "To Share or not to Share" (the government response to the Caldicott Review
- NHS Digital: A Guide to Confidentiality in Health and Social Care
- National Data Guardian report
- NHS Care Record Guarantee
- The NHS Standard Contract and
- Other relevant legislation

All records holding personal identifiable information of any individual must be managed in accordance with the Data Protection Act 2018 (DPA), the General Data Protection Regulation (hereafter known as GDPR), Human Rights Act 1998 and the common law duty of confidence.

Corporate records may also be subject to the common law duty of confidence and may equally be classified as sensitive or non-sensitive in terms of their impact on the running of the business if lost or disclosed. However, in certain circumstances it may be appropriate to disclose certain non-personal information that has been classified as sensitive that is held by the CCG in accordance with the Freedom of Information Act 2000.

The records management policy should be read in conjunction with the following CCG documents:

- information governance framework
- confidentiality & data protection policy
- freedom of information and environmental information regulations policy and procedures
- email policy
- information asset owner handbook
- information governance user handbook

In addition, the following CCG documents are particularly relevant to records management

- safe transfer procedures and guidance
- disposal of confidential waste procedure
- secure storage of records guidance*

- creation and maintenance of records structures guidance*
- CCG file naming conventions guidance*
- records retention guidance*

*The above starred information can be found in the 'records management CCG staff guidance document'

4. Policy aims and organisational standards

The aim of this policy is to ensure that the CCG:

- protects the content, context and structure of records to meet business needs and stakeholder requirements
- promotes recordkeeping practices and systems so far as practicable, to comply with guidance from the information commissioner (ICO), NHS institutions, professional standards and including ISO 549: 2016 and BS 10008: 2014 and the NHS Data Security & Protection Toolkit
- clearly defines responsibilities and accountability for records and all users appropriately and adequately trained in records management requirements
- operates records management procedures and practices that conform to applicable legislation and guidance

4.1. Organisational standards for records management:

1. A register of CCG information assets and flows of personal data is maintained – this includes all records management systems and facilitates the maintenance of records.

2. Records are available when needed – this is to facilitate the effective continuity of day to day business, and enable a reconstruction of activities or events that have taken place;

3. Records can be securely accessed - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist. This access must be limited to staff on a need to know basis;

4. Records can be interpreted - the context of the record can be interpreted; who created or added to the record and when during which business process, and how the record is related to other records;

5. Records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;

6. Records can be maintained through time – the qualities of availability, accessibility, interpretation and organisational worth can be maintained for as long as the record is needed, and on occasion permanently, despite changes of format;

7. Records are secure - from unauthorised or inadvertent alteration or erasure, and that access and disclosure are properly controlled, and ensure that audit trails will track all use and changes. Staff are confident that organisational records management procedures support them in their professional duty to protect the confidentiality of the records, as appropriate. To ensure that records are held in a robust format which remains readable for as long as records are required;

8. Records should be protected by a contingency or business continuity plan – protection needs to be in place for all types of records that are vital to the continued functioning of the organisation. Based on an assessment of risk and following the corporate approach documented plans should be drawn up, tested and reviewed.

9. Records are retained and disposed of appropriately and securely- using consistent, secure and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and

10. Staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management i.e. IAO/IAA training, data security training.

5. Records management procedure

5.1. Registration on the corporate information asset register and data flow map

It is vital that the CCG know at all times what information assets it maintains, what information those records constitute and where the information flows from and to.

The CCG will establish and maintain mechanisms through which directorates and their business functions can register all of their information assets and flows of personal data. This includes records management systems and inventories of records. The information asset register will record;

- records being maintained and their location
- the information asset owner and the information asset administrators for each information asset
- systems used to maintain and store the records
- retention periods
- information security measures put in place

The data flow map will record (for all flows of personal data):

- controller and processor of the flow
- legal basis for processing
- methods for transmitting data
- information security measures in place

I. In accordance with the Records Management Code of Practice 2021, the types of records that should be recorded on the CCG information asset register include:

- personnel records
- clinical records
- financial papers
- estates papers
- service provision records
- performance monitoring
- policy papers (reports, correspondence, etc.)
- minutes and circulated papers etc. of meetings
- complaints papers and correspondence

- research and development papers

This list is not exhaustive.

II. where a record collection identified or created contains personal confidential information, the data flow map must also be completed. This enables the CCG to assess how it uses personal data, ensure that this is undertaken on a legal basis and ensure appropriate controls are put in place to securely protect the confidentiality of that information.

III. registration of an information asset and data flow will be achieved by the allocation of a unique identifier on the register.

IV. registration systems should be monitored regularly and reviewed at least annually to ensure that systems continue to operate effectively and efficiently and meet the needs of users.

5.2. Implement secure records storage and access arrangements

Appropriate secure storage must be implemented for the type of information held and media it is held on. Access to the information must be controlled on a need to know basis.

Please see further information available in the 'records management CCG staff guidance' document available on the intranet.

https://nhsbradfordcravenccg.intradoc247.cloud/about-us/teams/browse/1362

5.3. Creation and maintenance of records structures

Local records management procedures must be documented to guide staff in how to create and maintain records, including naming conventions, version control and data quality, this applies to both manual and electronic systems.

Please see further information available in the 'records management CCG staff guidance' document available on the intranet.

https://nhsbradfordcravenccg.intradoc247.cloud/about-us/teams/browse/1362

5.4. Transporting, transferring and sending records

All records and documents, including all portable medial, must be transported and transferred securely.

Please see the safe transfer procedure & guidance and the email policy. Also, further information available in the 'records management CCG staff guidance' document available on the intranet.

https://nhsbradfordcravenccg.intradoc247.cloud/about-us/teams/browse/1362

5.5. Records retention and review:

The Records Management Code of Practice 2021 sets out minimum statutory retention periods for key corporate documentation which must be followed and can be accessed here:

https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

Please see further information available in the 'records management CCG staff guidance' document available on the intranet.

https://nhsbradfordcravenccg.intradoc247.cloud/about-us/teams/browse/1362

Retention periods are recorded within the information asset register for all information assets.

It is vital to highlight the importance of actively managing records which are stored in off-site storage. This will ensure that the CCG maintain a full inventory of what is held off-site and retention periods are applied to each record and a disposal log is kept.

Any records transferred to the CCG at the end of a service contract must be logged on the CCG information asset register and (where appropriate) data flow map.

5.6 Types of CCG records

5.6.1 Complaints

Where a patient or service user complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Complaint information should never be recorded in the clinical record.

5.6.2. Records at contract change

Once a contract ends, any service provider still has a liability for the work they have done and, as a general rule, at any change of contract the records must be retained until the time period for liability has expired.

In the standard NHS contract, there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision upon termination of the contract. It is also the case that after the contract period has ended; the previous provider will remain liable for their work. In this instance, there may be a need to make the records available for continuity of care or for professional conduct cases.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also be a consideration to identify the legal entity which must manage the records.

Where the content of records is confidential, for example health records, it may be necessary to inform the individuals concerned about the change.

Where there is little impact upon those receiving care, it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes may require individual communications or obtaining explicit consent. Although the conditions of the Data Protection legislation may be satisfied in many cases there is still a duty of confidence which requires a patient or client (in some cases) to agree to the transfer.

5.6.3 Continuing health care record

Continuing healthcare records can be split into two parts:

• Care record - The care record is the information relating to a patient/service user's care that enables the CHC panel to determine eligibility for CHC based on an assessment of needs.

• Administrative record - The Administrative Record is the information used by the CCG to ensure the CHC process runs effectively – an example being appointment letters asking the patient/service user to attend a panel. CCGs require access to health and care information to determine a patient/service user's entitlement (once the CCG has been notified).

5.6.4. Individual funding requests (IFRs)

Similar to Continuing Healthcare, IFR cases are mainly administrative records, but also contain large amounts of personal/confidential patient information and as such, should be treated in the same way as CHC records.

5.6.5 Staff records

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the information collected through the recruitment process and this will include the job advert, application form, evidence of the right to work in the UK, identity checks and any correspondence relating to acceptance of the contract.

5.7. Secure records disposal

All confidential records must be disposed of in a secure manner to render the information illegible and non-retrievable.

See also the disposal of confidential waste procedure

5.8. Incident reporting

All incidents or near misses relating to records management must be reported in accordance with the CCGs incident reporting policy.

6. Roles and responsibilities

Records management should be recognised as a specific corporate responsibility within the CCG. It should provide a managerial focus for records of all types and formats, including electronic records throughout their lifecycle.

All individuals who create, receive or use records in any form of media have records management responsibilities*.* Furthermore, any record that any individual working for on behalf of the CCG creates is a public record and may be subject to both legal and professional obligations, including compliance with relevant legislation.

The responsibilities of specific roles are set out below.

Chief officer

Overall accountability for records management across the CCG lies with the chief officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents

Caldicott guardian

The CCG Caldicott guardian is the conscience of the organisation and is responsible for ensuring that national and local guidelines on the handling of confidential personal

information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Senior information risk owner (SIRO)

The CCG SIRO is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of information are in place. The SIRO is responsible to the governing body for ensuring that all information risks are recorded and mitigated where applicable. The CCG SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this policy.

Data protection officer (DPO)

The data protection officer has a particular responsibility in ensuring that the CCG meets its legal responsibilities with regards to compliance with the Data Protection Act 2018 and GDPR.

Strategic director of organisation effectiveness

Overall responsibility for the records management policy and implementation lies with the strategic director of organisation effectiveness who has delegated responsibility for managing the development and implementation of records management procedures.

Strategic head of assurance

The strategic head of assurance is responsible for supporting the strategic director of organisation effectiveness and for co-ordinating, publicising, implementing and monitoring records management processes and reporting issues or concerns to the audit and governance committee. This includes putting systems in place to maintain the information asset register and data flow map for update by information asset owners and administrators.

Information asset owners (IAO) – associate leadership team

An IAO is an individual within an organisation that has been given formal responsibility for the security of an asset (or assets) in their particular work area. They are responsible for the maintenance of the confidentiality of that asset, ensuring that access to the asset is controlled and that the information is securely kept. They provide assurance that any risks to the information asset are managed effectively. IAOs are directly accountable to the SIRO.

Within the CCG, the role of IAO has been delegated to associate the associate leadership team.

Information asset owners are responsible for the quality of records management within the CCG must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is to say, they must have an up-to-date knowledge of the laws and guidelines concerning confidentiality and data protection.

All departments/business functions must identify all record management systems and ensure that appropriate records management operating instructions / templates in accordance with these records management procedures are developed, documented, reviewed and made available to all staff.

Information asset administrators (IAA)

Information asset administrators have delegated responsibility for the operational use of an asset and are specified on the information asset register for each information asset.

Providing support to the IAO, the IAA is the individual or one of a number who uses the information asset on a day to day basis. They will generally be more familiar than the IAO with the information, any systems and any risks in their area. This may include responsibilities for:

a) ensuring IG policies and procedures are followed;
b) ensuring the principles of and responsibilities for data quality;
c) recognising actual or potential data security incidents;
d) ensuring that Information asset register and data flow maps are accurate and kept up to date; and
e) resolving system issues, including managing and auditing user accounts i.e. setting users up with logons to the system with appropriate access rights according to their role. Audits of user accounts should be undertaken on a defined periodic basis.

All staff

All staff are responsible for the records they create or use in the course of their duties and are required to act in accordance with the principles of this policy as it relates to the management of information throughout its lifecycle.

At all times staff should discharge their duties in accordance with the law, ensuring that the confidentiality and security of information is maintained and that any disclosure is appropriate and provided to an authorised recipient. In this they are supported by the information governance framework, procedures and best practice guidance.

Staff handling personal confidential information must remember they have a common law duty of confidence to patients and other employees and a duty to maintain professional ethical standards of confidentiality.

7. Implementation, training and awareness

The policy will be disseminated by being made available on the intranet, and highlighted to staff through newsletters, team briefings and by managers.

Information asset owners (IAO) and information asset administrator (IAA) are responsible for the implementation of this policy and for supporting staff participation in adequate training and ensuring processes/procedures are documented to ensure robust records management.

All staff are required to undertake data security and protection mandatory training on an annual basis. More specialist information governance training requirements for specific roles are set out in the IG training needs analysis.

8. Monitoring and audit

All information asset owners must ensure the review of their records management systems at least annually, firstly to ensure that they have all been recorded on the information asset register and data flow map and secondly to review controls within the systems and ensure that they remain appropriate and adequate to protect the information held within the system. It is suggested IAOs undertake this review at the same time the information asset register and data flow map is subject to its formal annual update.

The output from the formal review and update of the CCG information asset register and data flow map is reported formally to the SIRO on an annual basis.

Any incidents or near misses relating to records management will be reported to the audit & governance committee.

9. Policy review

This policy will be reviewed every two years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance.

These procedures will be retained in line with the Records Management Code of Practice 2021 retention schedules.

10. Public Sector Equality Duty

The Equality Act 2010 includes a general legal duty to:

- eliminate unlawful discrimination, harassment victimisation and any other conduct prohibited under the Act
- advance quality of opportunity between people who share a protected characteristic and people who do not share it
- foster good relations between people who share a protected characteristic and people who do not have it

The protected characteristics are:

- age
- disability
- gender reassignment
- marriage or civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

Public bodies have to demonstrate due regard to the general duty. This means active consideration of equality must influence the decisions reached that will impact on patients, carers, communities and staff.

It is no longer a specific legal requirement to carry out an equality impact assessment on all policies, procedures, practices and plans but, as described above, the CCG do need to be able to demonstrate they have paid due regard to the general duty.

This policy sets out how the CCG ensure records are managed legally, efficiently and effectively. It is not believed that this policy will impact on or affect differently or adversely any of the groups with protected characteristics.

11. Appendices

Appendix a - Definitions

Term	Definition
Assembly	A collection of records. Maybe a hybrid assembly meaning where electronic and paper records are contained in one folder.
Class	Class is a subdivision or an electronic classification scheme by which the electronic file plan is organised, e.g. subject area. A class may either be sub-divided into one or more lower level classes. A class does not contain records. See folder
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Data controller	The GDPR defines a data controller as: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controllers make decisions about processing activities.
Data Processor	Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Declaration	Declaration is the point at which the document (i.e. the record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.
Disposition	Manner in which a record is disposed of after a period of time. It is the final stage of the record management in which a record is either destroyed or permanently retained.
Document	The International Standards Organisation (ISO) standard 5127:2017 now states ‘recorded information shall be treated as a unit in a documentation process regardless of its physical form or characteristics’

Term	Definition
Electronic document	Information recorded in a manner that requires computer or other electronic device to display, interpret and process it. This includes documents (whether text, graphics or spreadsheets) generated by software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in Electronic Data Interchange (EDI). An electronic document can contain information as hypertext connected by hyperlinks.
Electronic record	An electronic record is an electronic document which has been formally declared as a corporate record. A typical electronic record consists of both electronic content (one or more components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied.
Users (end users)	This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is a source of much or the material which constitutes the record. Since records systems tend to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of the quality and accountability.
File plan	The full set of classes, folders and records together make up a file plan. It is a full representation of an organisation, designed to support the conduct of the business, and meet the records management needs.
Folder	A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records (or markers where applicable). Folders are allocated into a class.
Information asset owner (IAO)	An IAO is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core information governance requirement the all Information Assets are identified and that the business importance of those assets is established.

Term	Definition
Information asset administrator (IAA)	An IAA is usually an operational manager who is familiar with information risks in their business area. Their primary role is to support the IAO to fulfil their responsibilities and ensure that policies and procedures are followed, recognise actual or potential serious incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information lifecycle management	Information lifecycle management is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction. Records Management policies and procedures form part of the information lifecycle management, together with other processes, such as, a records inventory, secure storage, records audit etc.
Metadata	Metadata can be defined as data about data. Metadata is structured, encoded data that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Examples of metadata: title, dates created, author, format, etc.
Naming convention	A naming convention is a collection of rules which are used to specify the name of a document, record or folder.
Protective marking	Protective marking is a metadata field applied to an object to show the level of security assigned to an object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.
Record	A record in records management terminology may not be the same as a record in database terminology. A record for the purposes of this document is used to denote a ‘record of activity’ just as a health record is a record of activity of a patient’s NHS contact. A record may be any document, email, web page, database extract or collection of these which form a record of activity. A record of activity for a database extract may therefore include a collection of health records. A formal definition 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.’ (ISO 15489-1:2016, Information and Documentation. Records Management)

Term	Definition
Safe haven	Safe Haven is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure person identifiable, confidential and/or sensitive information can be received, stored and communicated safely and securely.