Text

Description automatically generated with medium confidence****

**Records Management Policy**

**February 2024**

|  |  |
| --- | --- |
| **Authorship:** | Information Governance Team - Humber & North Yorkshire Integrated Care Board |
| **Committee Approved:** | SIRO/ ICB Information Governance Group |
| **Approved date:** | April 2024 |
| **Equality Impact Assessment:** | November 2023 |
| **Target Audience:** | ICB and its Committees and Sub-Committees, ICB Staff, agency and temporary staff & third parties under contract |
| **Policy Number:** | ICB60 |
| **Version Number:** | 1.0 |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as ‘uncontrolled’ and as such may not necessarily contain the latest updates and amendments.**

**AMENDMENTS**

Amendments to the policy may be issued from time to time. A new amendment history will be issued with each change.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **New Version Number** | **Issued by** | **Nature of Amendment** | **Approving body** | **Approval date** | **Date published on website** |
| V1.0 | Executive Director of Corporate Affairs | New Policy | SIRO / ICB IGG | April 2024 | November 2024 |

Contents

[1 Introduction 4](#_Toc157709995)

[2 Purpose 4](#_Toc157709996)

[3 Scope of the Policy 4](#_Toc157710000)

[4 Duties/ Accountabilities and Responsibilities 4](#_Toc157710001)

[4.1 Duties within the organisation 5](#_Toc157710002)

[4.2 Responsibilities for approval 6](#_Toc157710003)

[5 Records Management System 6](#_Toc157710004)

[5.1 What is a record? 6](#_Toc157710025)

[5.2 Lifecycle of a Record: 7](#_Toc157710042)

[6 Consultation 14](#_Toc157710044)

[7 Training 14](#_Toc157710045)

[8 Monitoring Compliance 15](#_Toc157710046)

[9 Arrangements for Review 16](#_Toc157710047)

[10 Dissemination 16](#_Toc157710048)

[11 Associated Documentation 16](#_Toc157710049)

[12 References 16](#_Toc157710050)

[13 Appendices 17](#_Toc157710051)

[14 Impact Assessments 17](#_Toc157710052)

[14.1 Equality 17](#_Toc157710053)

[14.2 Bribery Act 2010 17](#_Toc157710054)

[14.3 General Data Protection Regulations (GDPR) 18](#_Toc157710055)

[Annex A - Definition/ Explanation of Terms 19](#_Toc157710056)

[Annex B](#_Toc157710057) - [Classification of NHS Information – Marking Guidance 21](#_Toc157710058)

[Annex C – Secure Disposal of Records 22](#_Toc157710059)

[Annex](#_Toc157710060) [D – Records Management Checklist 23](#_Toc157710061)

# Introduction

The organisation’s records are important sources of administrative, evidential and historical information, providing evidence of actions and decisions, and represent a vital asset to support the organisation’s 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.

All NHS records are public records under the terms of the Public Records Act 1958 2.3(1)-(2). The Act sets out broad responsibilities for everyone who works with such records and provides guidance and supervision. The Secretary of State for Health, all Health Authorities and NHS trusts and other NHS bodies have a statutory duty to make arrangements for the safe-keeping and eventual disposal of their records.

A records management system is a record-keeping system companies used to track, store, and organise their records. It manages records from creation until disposal, and it does this to assist teams in information governance, regulatory compliance, and risk management.

# Purpose

This policy applies to all records (corporate and health records) paper or electronic, that are held by NHS Humber and North Yorkshire Integrated Care Board (hereafter the ICB). The aim of this policy is to ensure uniformity across the organisation, and to ensure that records management practice throughout the ICB complies with relevant legislation and national standards. The main legislative areas and codes of practice are:

* NHSE Records Management Code of Practice: A guide to the management of health and care records 2023.
* Human Rights Act 2000
* Mental Health Act 1983
* NHS and Community Care Act 1990
* Public Records Act 1958 amended 1967
* The Adoption Act 1976
* The Caldicott Report 1997
* The Children’s Act 1989
* The Data Protection Act 2018
* The General Data Protection Regulation (EU) 2016/679 (GDPR)
* The Freedom of Information Act 2000
* The Health and Social Care Act 2022

This policy is based on NHS England [NHSE Records Management CoP 2023 (england.nhs.uk)](https://transform.england.nhs.uk/media/documents/NHSE_Records_Management_CoP_2023.pdf) & [The NHSE Corporate Records Retention & Disposal Schedule](https://www.england.nhs.uk/wp-content/uploads/2017/07/B1785-nhse-corporate-records-retention-and-disposal-schedule.pdf)

# Scope of the Policy

The policy applies to the NHS Humber and North Yorkshire ICB and all its employees and must be followed by all those who work for the organisation, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

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

# Duties/ Accountabilities and Responsibilities

## Duties within the organisation

**Chief Executive**

The Chief Executive has ultimate responsibility for the implementation of the provisions of this policy as the accountable officer with responsibility for the management of the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

The ICB has a particular responsibility for ensuring that it meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

**Executive Director of Clinical and Professional / Caldicott Guardian**

The NHS Humber and North Yorkshire ICB Caldicott Guardian is the conscience of the organisation and is responsible for confidentiality of person identifiable information as designated in the Caldicott report and for the information governance agenda which incorporates data protection legislation, ensuring patient identifiable information is shared in an appropriate and secure manner according to the [The Caldicott Principles - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/the-caldicott-principles).

**Executive Director of Corporate Affairs/ Senior Information Risk Owner (SIRO)**

The SIRO is responsible for approving and implementing national and local guidelines on information management. The SIRO also ensures that all information risks are documented and mitigated when applicable. Furthermore, the SIRO manages all record issues, including electronic media, in accordance with ICB policy. The SIRO reports to the ICB Board and Chief Executive regarding information risk management.

**Director of Governance/ Board Secretary/ Data Protection Officer (DPO)**

The DPO is responsible for ensuring the organisation is correctly protecting individuals’ personal data according to current legislation.

The DPO has expert knowledge and will monitor compliance with data protection legislation, providing advice and assistance with regards to the completion of Data Protection Impact Assessments, and Data Sharing Agreements etc.

The DPO is responsible for acting as a contact point for the Information Commissioner’s Office (ICO), members of the public and NHS Humber and North Yorkshire ICB staff on matters relating to information governance and the protection of personal information. The DPO assists in implementing essential elements of the legislation such as the principles of data processing, data subjects’ rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches.

**Senior Information Governance Manager**

Overall responsibility for the Records Management Policy and implementation lies with the NHS Humber and North Yorkshire ICB Senior Information Governance Manager and the Corporate Affairs Team who have delegated responsibility for managing the development and implementation of records management procedural documents.

The ICB Senior Information Governance Manager is responsible for co-ordinating, publicising, implementing, and monitoring the records management processes and reporting issues or concerns to the ICB Information Governance Group. The Senior Information Governance Manager is also responsible for putting systems in place to maintain the Information Asset Register. All new collections of records should be notified to the Information Governance Team for recording in the Information Asset Register.

**Directors/Senior Managers**

Senior Managers are responsible for the quality of records management within the ICB. All line managers must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is, 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 in accordance with these records management procedures are developed, documented and made available to all staff. They are responsible for ensuring that the retention and disposal guidance is reflected in local records management process and followed.

**Information Asset Owners**

Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs have responsibility for appropriate records management, including retention and disposal of information when no longer required. They must provide assurance that information risk, including records management is being managed effectively in respect of the information assets they are responsible for.

**Staff**

All staff 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.

## Responsibilities for approval

The Senior Information Risk Owner under advisement from the ICB Information Governance Group is responsible for approvals.

# Records Management System

## What is a record?

A record is any noted information, in any form, created or received in either paper based or electronic format and maintained by the organisation in the transaction of its business or conduct of affairs and kept as evidence of such activity. It is important to remember that any record held by the organisation may be disclosed to the public if requested under the Freedom of Information Act 2000.

* **Corporate records (non-clinical)** - provide evidence of actions and decisions and represent a vital asset to support daily functions, operations, audit, and legal requirements. Records support policy formation and managerial decision-making protect the interests of the organisation, staff, and our population. Records support consistency, continuity, efficiency, and productivity and help deliver organisational priorities in consistent and equitable ways. Corporate records may be classified as sensitive or non-sensitive in terms of their impact on the running of the business if lost or disclosed. For further information on classification please see Annex B.
* **Health records (clinical) -** are also a key component of corporate documentation and are a vital asset to support delivery of safe and effective care to the ICB’s population. Although not a provider of care, the ICB will utilise health records to deliver certain duties and responsibilities (Continuing Healthcare, safeguarding, complaints, for example).
* **Email Records / Electronic Communication -** Email is a key communication tool and is not designed as an appropriate solution for long term file storage. Therefore, all emails that are records of business activity and/or a formal record of a transaction should be saved to an appropriately named folder on shared network drive. Keeping all emails will result in a significant storage burden to your organisation and information may become difficult to locate due to the size of files and attachments being stored.

NHS Mailboxes and Mailbox Archives should not be used for the long-term storage of email records. Staff should perform regular housekeeping in their Mailboxes so that transitory and spam type emails are disposed of. Managers shall ensure all required email records are transferred from a staff leaver’s Mailbox to the approved store.

Other forms of electronic communication such as **Microsoft Teams** is to be used as an effective way to collaborate effectively with colleagues, conduct meetings, instant messaging but it is not designed as a long-term document storage/ management system. As with emails, any recordings/documents that are records of business activity and/or formal records should be saved to the appropriate named folder on the shared network drive.

All records holding personal identifiable information of any individual must be managed in accordance with the current Data Protection Legislation, Human Rights Legislation, and the Common Law Duty of Confidence.

## Lifecycle of a Record:

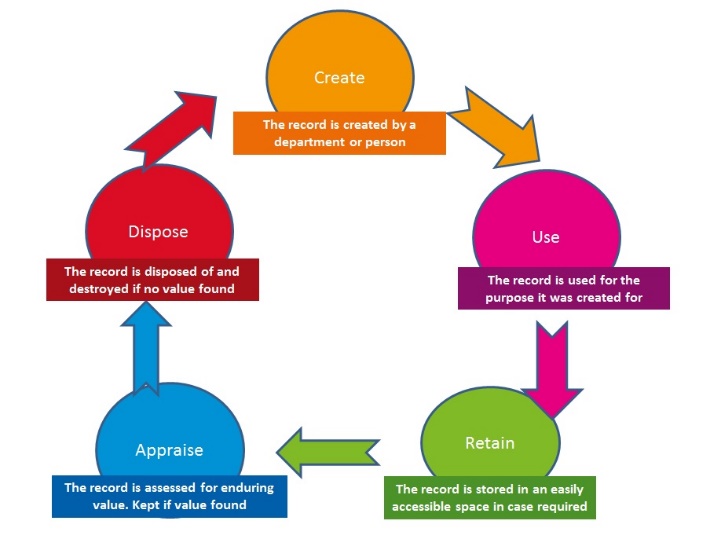
The Records Management Code of Practice 2021 (updated 2023) provides detailed advice on records management relating to specific types of records for example, transgender records, protected persons health records and adopted persons records including how long to keep different types of records. The latest version of the guidance is published by NHS England and is available at: [Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) . The [NHSE Records Retention & Disposal Schedule](https://www.england.nhs.uk/wp-content/uploads/2017/07/B1785-nhse-corporate-records-retention-and-disposal-schedule.pdf) provides detailed guidance on the management of corporate records. These documents are based on current legal requirements and professional best practice.

A service may have various record types classified differently, with each being created and accessed differently. A record that is deemed confidential or private is to have stringent security controls this includes storing, handling and includes when a record needs to be transferred out of the ICB.

Once a record is created it needs to be managed through its life cycle as outlined in diagram 1. An audit trail for who has accessed, amended the record, and any movement of the record needs to be tracked to enable the record to be traced and as up to date at any point.

Information Asset Owners, Service Managers and Line Manager are responsible for ensuring that there is a documented records management process in place within their areas. This should document how records are managed, indexed and how destruction dates are managed.

Diagram 1 – Life cycle of a record



**Create**

When creating a record or setting up a folder it is good practice to build the agreed destruction dates. This could include:

* Destruction dates noted within headers/footers.
* Dates tagged onto the end of file names.
* Dedicated electronic filing systems can be used that ask for a destruction date when a file is uploaded; and
* Destruction dates listed within filing index with annual review to action.

**Folder creation** - Each directorate/team should establish a clear folder structure that meets the organisation’s and directorate/department’s business needs that is easily understood by staff. 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. Staff should refrain from naming folders or files with their own name except for separate secure personnel folders.

It is a legal requirement that personal information/business or corporate sensitive information is stored securely, separate secure folders should be set up with appropriate restrictions.

**File Naming Convention** – Each Directorate should nominate staff to establish and document file naming conventions in line with national archives advice, i.e.

⦁ Give a unique name to each record,

⦁ Give a meaningful name which closely reflects the records contents,

⦁ Express elements of the name in a structured and predictable order,

⦁ Locate the most specific information at the beginning of the name and the most general at the end,

⦁ Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version). Staff should avoid lengthy file names and should not name the file after the author / creator / owner and should avoid non-specific or generic terms i.e., ‘General Correspondence’ or ‘Miscellaneous’.

**Classification** - the ICB protective marking scheme is based on the Cabinet Office [Government Security Classifications](https://www.gov.uk/government/publications/government-security-classifications) defined protective marking scheme which is used by both central and local government. Under the NHS Protective Marking Scheme 2014, patient data is classed as ‘NHS Confidential’.

**Version Control:** A system of version control must be implemented to enable staff to know that they are working the latest/ correct version of the documentation. This may be in form of a version number and date or by use of document creation date.

**Indexing and Filing:** Each Directorate should establish and document a clear and logical filing structure that aids retrieval of records. The register or index is a signpost to where paper corporate records are stored, e.g. the relevant folder or file, however, it can be used as a guide to the information contained in those records. The register should be arranged in a user-friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear logical names that follow the organisation’s or directorate’s naming convention.

The filing structure for electronic records should reflect the way in which paper records are filed to ensure consistency. Filing of corporate records to local drives on PCs and laptops is not appropriate, files must be saved to the departmental network, to ensure only authorised access is available and that appropriate backups are taken. Likewise, the filing of key organisational paper records or clinical records in desk drawers is not appropriate, departmental accessible secure storage should be used.

**Record Referencing** - Each Directorate should establish and ensure compliance to a document referencing system that meets its business needs and is easily understood by staff members that create, file or retrieve records held in any media. Several types of referencing can be used, e.g. alpha-numeric, alphabetic, numeric or keyword. The most common of these is alpha-numeric, as it allows letters to be allocated for a business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the records are kept and identify the record by reference to date and format.

**Records Inventory-** It is recommended that each directorate/team establish a log or register to aid the retrieval of folders/files. These should be reviewed annually to determine if record has reached is retention period. A separate Information Asset Register will be held which lists systems/information assets holding or sharing personal/business corporate sensitive information and data flows.

**Use**

**Mailing Records**

Care should be taken when posting out any records and when choosing a mailing option, staff should consider the following:

* Do you have the correct mailing address?
* Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?
* Will the record be protected from damage, unauthorised access or theft?
* Does the mail provider offer ‘track and trace’ options and is a signature required on delivery?
* When there is an urgent request for a record, i.e., clinical record, it may be necessary to use a taxi service to ensure prompt delivery. Staff should ensure that a recognised taxi operator is commissioned to undertake this service and that the record is made totally secure for the journey.

**Emailing Records**

Confidentiality can be compromised, especially when using internet-based email systems. Employees will therefore not send business sensitive/confidential/patient or staff identifiable information outside the NHS via the internet (including to their own home). This policy strictly prohibits emails being set up to automatically be forwarded to non-NHS email accounts since there can be no way of filtering out emails which contain confidential/patient or staff identifiable information. Personal/business sensitive information must only be sent using an approved method of security and suitable encryption.

Although the Health and Social Care Network (HSCN) is private, it is regarded as an ‘open relay system’. The network is a transport mechanism for data and as such does not encrypt (or similarly protect) the data transmitted. Users of the network are required to apply such methods of information confidentiality and integrity as are appropriate to the data transmitted and the applications used.

An approved method of transmitting sensitive/confidential/patient or staff identifiable information. The following email groups can also be utilised to transmit data securely:

.gov.uk, .gov.scot, .police.uk, .pnn.police.uk, .cjsm.net, .scn.gov.uk

Only communication between @nhs.net and @nhs.net and any of the groups above will retain data encryption. In order to send secure emails to other email addresses you must use [secure] at the front of your email subject. Further guidance can be found here: [Guidance for sending secure email (including to patients) - NHS Digital](https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email)

**Transferring Records**

Where it is necessary to transfer documents to another department or organisation, a data transfer agreement must be completed**.** To eliminate lost or misplaced records, it is essential that tracking systems are used on all filing systems, with the following information being recorded:

* The item reference number or other identifier, i.e., file path to the document.
* The file title.
* The name of the person who created the document, including unit or department.
* The date when the document/file was withdrawn from the system.

Safeguarding Children Policy and Guidance is in place regarding transfer and tracking of records where there are child welfare concerns.

In order to reduce the amount of paper generated and consequent storage needed, electronic systems should be put into place where practicable. Using an electronic tracking system, rather than a manual system, can be more efficient – speeding up information retrieval times, reducing misfiling and the problems associated with the use of absence markers.

Where it is necessary to transport confidential records to a different location the following protocol should be followed:

* In general, records should never be left unattended in a vehicle unless it would be totally impractical not to do so. If records must be left in unattended cars, they must always be kept in a locked boot or covered luggage area.
* Records should be enclosed in envelopes or opaque wallets and sealed for transit.
* Records that may be damaged in transit should be enclosed using suitable padding or containers.
* For larger quantities, records should be placed in suitable boxes or containers for their protection.
* Each transit container should be addressed clearly and marked ‘Confidential’, with the sender’s name and address on both back and front of the transit container.
* Records should be packed carefully into vehicles to ensure that the movement of the vehicle will not damage them.
* Vehicles must be fully covered in order that records are protected from exposure to weather, excessive light and other risks such as theft.
* No other materials that could cause risks to records (such as chemicals) should be transported with records.
* Safety of staff must be taken into account when transporting records.

**Duplicate Records**

Care must be taken to minimiseduplicate information across systems. When various versions of documents are produced prior to agreement of a final version, unless there is a reason to keep these, they should no longer be retained. Preceding documents should be retained if the undated version contains significant major changes to content, as this will form the version history of the document.

Where different versions are to be retained a version control mechanism must be implemented.

Records containing personal information should only be retained if the purpose for holding the information applies.

Documents shared for comments should, where practical, be shared through a collaborative platform or via a link to reduce the number of versions of the same document. The final version, once approved, should remain with the team to which it relates, and any duplicates should be destroyed.

Careful consideration should be given to how meeting papers are stored and shared and where practical, there should be a centralised system available to all. There will be exceptions to this due to the sensitive nature of some committees such as Remuneration Committee or Safeguarding Groups.

**Digital Records**

Digital records must remain authentic and reliable, retaining their integrity, accessibility and usability over time despite advances in digital technology including software upgrades which can leave other applications unusable.

All patient and confidential information should be stored on the organisation’s area within the network drives/ SharePoint sites in a folder with restricted access so only the people that require access to the information to carry out their jobs can access the information. Sharepoint Asset Owners can set up their own security groups, however, if further support is required, please contact the relevant IT service desk.

**Retain**

**Storing Records**

Wherever possible, the ICB should move to digital records. Appropriate technical and organisational measures should be taken against accidental loss or destruction of, or damage to data (held either manually or electronically). Due to environmental factors care should be taken to ensure that wherever possible essential manual (particularly clinical) records are stored above waist level. Electronic records should be stored on approved systems which are regularly backed-up.

Storage and access to records containing clinical or personal and sensitive information must be securely protected e.g., lockable cabinets or by means of password control and associated access levels. All electronic information **should** be where possible, stored in a Connecting for Health system (e.g., SystmOne) using a Smartcard and role-based access contract based on RA01 and RA02 forms. Electronic information should not be:

* + Stored on the local drive of the PC, this includes encrypted PCs unless approval has been given by the Information Governance Group
  + Stored on the local hard drive of any home IT equipment.

For any patient and confidential information stored on the network drives/ SharePoint site, these should be held in a folder with restricted access so only the people that require access to the information to carry out their jobs can access the information.

**Storage Solutions**

**Off-Site Storage**

Records should only ever be taken off site with the appropriate approval and in accordance with Policies and guidance. These require staff to give the highest priority to the security of these records held off site, especially in the case of confidential records.

Where a number of records need to be carried during the day and they cannot practicably and securely remain with the member of staff transporting them then they must be locked out of sight in the boot of the car, during appointments. NB/ This method of storage is only to be used for the short term, records must never be left in the boot of the car for long periods of time or overnight. All records removed from the boot of the car must be carried in a secure container e.g. lockable briefcase.

If records are to be taken home, the records must be stored securely in accordance with the staff members’ Professional Code of Conduct and this policy in conjunction with other Information Governance Policies and guidance. It is essential that any such records are logged out of the department, using the implemented tracking system to ensure that records removed are trackable at all times.

**Portable Storage Devices**

The use of portable storage devices to store organisational information must be by exception and authorised by your Line Manager/Director. If using portable storage, information should only be stored on encrypted devices and these devices should not be used to store personal confidential data.

In all circumstances information should only be stored on encrypted portable storage devices for short periods of time. Any master documents should be held on the network drives/ SharePoint sites and records should be transferred back to/ synchronised with HNY ICB’s main storage facilities at the earliest opportunity.

**Personal Drives**

The ICB encourages staff to minimise the use of personal drives and to store business information in a collaborative, accessible place.

**Cloud Based Storage**

A data protection impact assessment should be undertaken before cloud-based storage solutions are implemented and consideration given to the guidance published by the Information Commissioner’s Office: [Cloud computing | ICO](https://ico.org.uk/for-the-public/online/cloud-computing/)

Any cloud-based storage solutions which will be used to store patient data must only be hosted within territories deemed to be GDPR adequate by the UK Government, as listed by the Information Commissioner's Office (ICO) international data transfers guidance. Procurement of any cloud-based storage solutions must be via the SBS framework, staff should contact the ICB Contracting Team for further information and support: [hnyicb.contracts@nhs.net](mailto:hnyicb.contracts@nhs.net)

**Archive Storage**

As the need for quick access to particular manual records reduces, it may be appropriate to move the less frequently used material out of the immediate work area and into archive storage. Given the limited storage space within the current ICB estate off-site archive storage is preferred. For records which require archiving please contact Corporate Affairs on [hnyicb.corporateaffairs@nhs.net](mailto:hnyicb.corporateaffairs@nhs.net) to arrange any facilitation of storing records off-site.

An inventory of all documents sent to storage should be compiled so that the archive company can electronically track the record back to the organisation.

**Appraise**

The management of records, particularly digital records require constant, continual effort, and should not be underestimated. The ICB is expected to have a rolling audit and appraisal of records and record keeping in line with best practice standards.

Records should be kept only for as long as they are required subject to an appraisal process to determine whether they are still in use or are of permanent archival value. The ICB has adopted the retention periods for health and non-health records as set out in the NHS Records Management Code of Practice and the NHS Corporate Records Retention and Disposal Schedule. A schedule within these guidance documents sets out the minimum periods for which various records created within the NHS should be retained or reviewed for continued retention either due to their ongoing administrative value, as a result of statutory requirement or for situations such as public inquiries. It also provides guidance on dealing with records which have ongoing research or historical value and should be selected for permanent preservation as archives and transferred to a Place of Deposit approved by the National Archives.

Where it is difficult to determine a retention period for a record the Information Governance Team ([hnyicb-ery.ig@nhs.net](mailto:hnyicb-ery.ig@nhs.net)) can advise.

The retention of records for longer than the recommended period must be discussed with the organisation’s Senior Information Governance Manager and, with their agreement, may be justified in writing for ratification by the Caldicott Guardian and/or SIRO.

Service Managers and Line Managers should appraise records in line with their agreed records management process within their areas. However, when appraising records, the following guidelines should be followed:

* Decisions should be considered in light of the need to preserve records whose use cannot be anticipated fully at the present time, but which may be of value to future generations.
* Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry on the document.
* Where documents are considered for permanent preservation, advice should be sought from the Senior Information Governance Manager to establish an appropriate place of deposit.
* The provisions of Article 5 (e) of the General Data Protection Regulation must be complied with (personal data is not kept for longer than necessary).

There will be one of three outcomes from appraisal:

* + dispose or destroy/ delete.
  + continued retention – this will require justification and documented reasons.
  + permanent preservation.

A plan will ensure regular archiving takes place of both manual and electronic records. This plan will include review dates for determining those records to be selected for permanent preservation, destroyed or retained for research or litigation purposes.

Comprehensive records should be retained when long-term storage is used and will include specification of destruction dates.

An annual appraisal process will be initiated by the Information Governance Team as part of the Information Asset management requirements for the Data Security and Protection Toolkit.

**Dispose**

All appraisal resulting in a decision to dispose of a record needs to be justified, follow policy or guidance, and be documented and approved by the relevant board, committee or group of the organisation. Each Directorate should agree their appraisal decision making process.

Disposal does not necessarily mean destruction of those records, they could be transfered to another organisation/ team or Place of Deposit (POD). There are occasions, particularly with Health Records, when records need to be passed onto a third party who will then be responsible for the disposal of the record within their retention and disposal procedures. However, details must be retained by HNY ICB of such movement of records. See [Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) for further information around POD.

The destruction of records is an irreversible act and as such all options must be given proper consideration before destruction is undertaken. Records may contain sensitive and confidential information; it is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures their complete illegibility.

The ICB has made provision for the destruction of paper records, which in most cases is undertaken by an approved contractor. As part of the contracting process for disposal of records the HNY ICB must satisfy itself that the methods used throughout the process provide adequate safeguards against accidental loss, or disclosure of data. External contractors will be required to sign a confidentiality agreement and produce written certification as proof of destruction.

The disposal of documents held in electronic format must be completed by a method which ensures that the information cannot be retrieved from the electronic media on which it was held. This can be done on site, or via an approved contractor. Destruction of files and/or electronic media must be undertaken by the IT Department to ensure that all records to be destroyed are done securely.

Where there is no requirement for permanent preservation, records will normally be destroyed as soon as possible after the expiry date of the minimum retention period.

An inventory of disposal/destruction should be kept.

* + Destruction – due process followed/agreed and inventory kept by Corporate Governance Team
  + Disposal – transferred to another organisation/team – kept by original team (IAO)
  + Disposal – Place of Deposit – approval obtained and inventory kept by Corporate Governance Team.

**National inquiry**

Particular attention should be paid to retention of records which may be required for National Inquiries e.g., the COVID Inquiry. Guidance is to err on the side of caution and preserve any relevant documents. However, this does not remove the need for good record keeping taking place.

The expectation remains the same for good records management whether this be for a public inquiry or business as usual. It will more than likely be necessary to search for and identify relevant records, so it is essential that all records are appropriately saved and will be easily accessible. This should facilitate a consistent departmental system of creating and storing records to enable information to be effectively and efficiently maintained, so that up to date and reliable records are available to staff on a need-to-know basis, as and when required.

# Consultation

All stakeholders such as ICB SIRO/DPO, Executive Lead IG and FOI Teams, involved in developing, implementing, management, and monitoring records management have been engaged in the development of this policy.

# Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test. This will be provided for new staff at induction and must be completed within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff and this should be discussed with staff members’ line manager as part of the Personal Development Review process where training needs are analysed.

All staff, including temporary staff and agency staff, students and any other personnel that may be required to use systems should be made aware of their responsibilities for record-keeping and records management through generic and specific training programmes and guidance.

All HNY ICB staff should be fully trained in record creation, use and maintenance, commensurate to their roles, including having an understanding of what should be recorded and how it should be recorded and the reasons for recording it. Staff should know:

* how to validate the information with the patient or the carer or other records to ensure they are recording the correct data;
* why they are recording it;
* how to identify, report and correct errors;
* the use of the information and records;
* what records are used for and the importance of timeliness, accuracy and completeness;
* how to update and add information from other sources.

# Monitoring Compliance

All departments must appraise their records and audit their records management systems annually, firstly to ensure that information has been recorded on the corporate Information Asset Register and secondly to review controls within the systems to ensure that they remain appropriate and adequate to protect the information held within the system.

Audits will:

* Identify all records management systems in use and ensure they are recorded on the organisation’s Information Asset Register.
* Identify areas of operation that are covered by the organisation’s policies and identify which procedures and/or guidance should comply to the policy.
* Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records and use a subsidiary development plan if there are major changes to be made.
* Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
* Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

A checklist has been developed at Annex D to assist managers in the development of effective records management systems.

Failure to comply with the standards and appropriate governance of information as detailed in this policy and supporting procedure can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance for which individuals are responsible for.

Failure to maintain these standards can result in criminal proceedings against the individual.

Any breach of confidentiality resulting from using email for persona/ business sensitive/ confidential/ patient or staff identifiable information will be investigated. Misuse of the systems and the information held may be subject to investigation and disciplinary proceedings.

# Arrangements for Review

This Policy will be reviewed within 3 years from the date of implementation. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

# Dissemination

The policy will be disseminated by being made available on the ICB website and highlighted to staff through staff communications, and by managers. **Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the HNY ICB’s disciplinary procedure.**

# Associated Documentation

* Information Governance Framework & Strategy
* Data Protection & Confidentiality Policy
* IT & Information Security Policies
* Privacy by Design
* Data Protection Impact Assessment Procedure
* Subject Access Request
* Information Governance Staff Handbook
* Incident Policy

This list is not exhaustive.

# References

* Records Management Code of Practice 2023
* Mental Health Act 1983
* NHS & Community Care Action 1990
* Public Records Act 1958
* Access to Records  Act 1990
* NHS Care Records Guarantee
* The Adoption Act 1976
* The Children’s Act 1989
* UK General Data Protection Regulation
* Data Protection Act 2018
* The Common Law Duty of Confidentiality
* The Freedom of Information Act 2000
* Privacy and Electronic Communications Regulations
* Confidentiality: NHS Code of Practice (Department of Health)
* Health and Social Care (Safety and Quality) Act 2015
* Caldicott Principles
* The Public Interest Disclosure Act 1998
* Human Rights Act 2000

# Appendices

Annex A – Definitions / Explanation of Terms

Annex B - Classification of NHS Information – Marking Guidance

Annex C - Secure Disposal of Records

Annex D - Records Management Checklist

# Impact Assessments

## Equality

NHS Humber and North Yorkshire ICB is committed to creating an environment where everyone is treated equitably and the potential for discrimination is identified and mitigated. It aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

An EQIA has been completed and as a result of performing the analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics.

## Bribery Act 2010

NHS Humber and North Yorkshire ICB has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010. Under the Bribery Act 2010 there are four criminal offences:

* Bribing or offering to bribe another person (Section 1)
* Requesting, agreeing to receive or accepting a bribe (Section 2)
* Bribing, or offering to bribe, a foreign public official (Section 6)
* Failing to prevent bribery (Section 7)

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an office.

All individuals should be aware that committing an act of bribery they may be subject to a penalty of up to 10 year imprisonment, an unlimited fine, or both. They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable disciplinary action by Humber and North Yorkshire Integrated Care Board, whether or not the breach leads to prosecution. Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

It is the duty of every member of staff to speak up about any genuine concerns in relation to criminal activity, breach of legal obligation, miscarriage of justice, danger to health and safety or the environment and the suspected cover up of any of these in the workplace. To raise any suspicions of bribery and/or corruption please contact Executive Director of Finance. Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire email: [Nikki.cooper1@nhs.net](mailto:Nikki.cooper1@nhs.net) or mobile 07872 988939 or Head of Anti-Crime Services on 07717 356707 / email [steven.moss@nhs.net](mailto:steven.moss@nhs.net).

The LCFS or Executive Director of Finance should be the contact for any suspicions of fraud. The LCFS will inform the Chief Finance Officer if the suspicion seems well founded and will conduct a thorough investigation. Concerns may also be discussed with the Executive Director of Finance or the Audit Committee Chair.

If staff prefer, they may call the NHS Fraud & Corruption Reporting Line on 0800 028 40 60 between 8am – 6pm Monday – Friday or report online at [www.reportnhsfraud.nhs.uk](http://www.reportnhsfraud.nhs.uk). This would be the suggested contact if there is a concern that the LCFS or Chief Finance Officer themselves may be implicated in suspected fraud, bribery or corruption.

Due consideration has been give to the Bribery Act 2010 in the development (or review, as appropriate) of this policy document and no specific risks were identified.

## General Data Protection Regulations (GDPR)

The UK General Data Protection Regulation (GDPR)/ Data Protection Act 2018 includes the requirement to complete a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals. Consideration should be given to any impact the policy may have on individual privacy; please consult NHS Humber and North Yorkshire ICB Data Protection Impact Assessment Policy. If you are commissioning a project or undertaking work that requires the processing of personal data, you must complete a Data Protection Impact Assessment.

The ICB is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the Data Protection & Confidentiality Policy and related policies and procedures.

# Annex A - Definition/ Explanation of Terms

**Assembly:** A collection of records. May be 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.

**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**: Data is a collection of facts from which information is constructed via processing or interpretation.

**Data Quality**: Data quality is a measure of the condition of data based on factors such as accuracy, completeness, consistency, reliability and whether it's up to date.

**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 5127/1 states ‘Recorded information shall be treated as a unit in a documentation process regardless of its physical form or characteristics’.

**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 interchange. 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.

**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**: Information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

**Information Asset Owner (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 that all Information Assets are identified and that the business importance of those assets is established.

**Information Asset Administrator (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.’ (BS ISO 15489.1, Information and Documentation. Records Management).

**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.

**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 tends 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.

# Annex B – Classification of NHS Information – Marking Guidance

**NHS CONFIDENTIAL –** appropriate to paper and electronic documents and files containing person-identifiable information, including service users, staff and any other sensitive information.

**NHS PROTECT - Discretionary** marking that may be used for information classified below NHS Confidential but requiring care in handling. Descriptors may also be used as required.

|  |  |
| --- | --- |
| **Table of descriptors that may be used with ‘NHS CONFIDENTIAL’ or ‘NHS PROTECT’ marking** | |
| **Category** | **Definition** |
| **Appointments** | Concerning actual or potential appointments not yet announced |
| **Barred** | Where: -  -there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or  -disclosure would constitute a contempt of court (information the subject of a court order) |
| **Board** | Documents for consideration by an organisation’s Board of Directors, initially in private.  (Note: This category is not appropriate to a document that could be categorised in some other way) |
| **Commercial** | Where disclosure would be likely to damage a (third party) commercial undertaking’s processes or affairs. |
| **Contracts** | Concerning tenders under consideration and the terms of tenders accepted. |
| **For Publication** | Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date. |
| **Management** | Concerning policy and planning affecting the interests of groups of staff.  (Note: Likely to be exempt only in respect of some health and safety issues.) |
| **Patient Information** | Concerning identifiable information about patients. |
| **Personal** | Concerning matters personal to the sender and/or recipient. |
| **Policy** | Issues of approach or direction on which the organization needs to take a decision (often information that will later be published) |
| **Proceedings** | The information is (or may become) the subject of, or concerned in a legal action or investigation. |
| **Staff** | Concerning identifiable information about staff. |

# Annex C – Secure Disposal of Records

When it has been determined that record(s) have reached the retention period then it must be recorded in a register of disposal and appropriate management authorisation for destruction obtained.

**Register of Destruction of Records**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Description of Records identified for Destruction & Dates covered and volume.** | **Retention Period checked against Records Management CoP. Y/N** | **Destruction authorised by.** | **Date and Method of Destruction** | **Certificate of obstruction obtained and filed.** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Annex D – Records Management Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **System Requirement** | **Description** | **Complete**  **Y/N** |
| **1.** | **Registration of the Records Management System on the Corporate Information Asset Register** | All records management systems in place, including databases and spreadsheets should be registered on the organisation Information Asset Register. The Information Asset Owners and Administrators should be identified and recorded for each information asset registered. |  |
| **2.** | **Determine the Records Management System** | Clear determination of aims and requirements, and information flows will assist in effective design of consistent recording and secure storage and use of information. |  |
| **3.** | **Implement secure records storage** | Appropriate secure storage must be implemented for the type of information held and media it is held on. |  |
| **4.** | **Creation and Maintenance of Records Structures** | Local records management procedures should 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 |  |
| **5.** | **Creating, Accessing and Reviewing Records** | It must be ensured that access to records for any purpose whatsoever, must be strictly controlled on a need to know basis. The controls put in place will depend upon the media in which records are held and how records are stored. |  |
| **6.** | **Protective Marking Schema**. | This indicates of the confidential nature of each document or record and informs staff of the appropriate level of care and confidentiality with which the document or record should be treated. |  |
| **7.** | **Tracking and Tracing** | This facilitates a mechanism by which the location of records or copies of records can be known at all times***.*** |  |
| **8.** | **Transporting and Transferring Records** | The transportation of records, documents and all portable media containing records must be transported securely. |  |
| **9.** | **Records Retention and Review** | The Records Management Code of Practice sets out statutory retention periods for key corporate documentation which must be followed. |  |
| **10.** | **Secure Records Disposal** | All records must be disposed of in a secure manner to render the information illegible and non-retrievable. |  |
| **11.** | **Audit of Records Management Systems** | All departments must audit their records management systems annually firstly to ensure that they have all been recorded on the corporate Information Asset Register and secondly to review controls within the systems and ensure that they remain appropriate and adequate to protect the information held within the system. |  |