Directorate of Performance Assurance

CORPORATE RECORDS MANAGEMENT POLICY

Reference:	DCP270
Version:	2.0
This version issued:	24/02/17
Result of last review:	Major changes
Date approved by owner (if applicable):	N/A
Date approved:	20/02/17
Approving body:	Trust Governance and Assurance Committee
Date for review:	December, 2019
Owner:	Wendy Booth, Director of Performance Assurance
Document type:	Policy
Number of pages:	24 (including front sheet)
Author / Contact:	Jeremy Daws, Head of Quality Assurance

Contents

1.0 Introduction / Purpose

1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to eventual disposal.

1.2 The previously cited Records Management: NHS Code of Practice has been superseded by the Records Management Code of Practice for Health and Social Care 2016 (referred to within this document as the 'Code') published by the Information Governance Alliance (IGA) for the Department of Health (DH).

1.3 The reissued Code merges together best practice guidance for corporate records management and clinical records together, therefore the reissued Trust policy is renamed to include within the scope wider records management, not limited to non-clinical records as before.

1.4 Due to the level of detail contained within this Code and comprehensive guidance with regard to the retention schedule for corporate documents, contained within this policy is a link to the code of practice. This policy will provide a preface to the guidance and outline how the Code will be implemented within the Trust.

1.5 The full Code can be found at the following link:
https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

1.6 The Code is based on current legal requirements and professional best practice. It is designed to help organisations implement the recommendations of the Mid Staffordshire NHS Foundation Trust Public Inquiry. It was drafted by a working group of representatives from the Information Governance Alliance, the Health and Social Care Information Centre, NHS England, the Department of Health, the National Archives and from a range of NHS and Social Care Organisations including Acute and integrated Mental Health Trusts, Clinical Commissioning Groups, GP practices and professional bodies (full details are found in Appendix 1 of the Code).

1.7 The Code is a key component of information governance arrangements for the NHS. Standards and practice covered by the Code will change over time so the source document that this NLAG policy is based will be reviewed regularly and updated as necessary, another reason for linking to the guidance within this policy.

1.8 The Public Records Act 1958 requires that all public bodies have effective management systems in place to deliver their functions. For health and social care, the primary reason for managing information and records is for the provision of high quality care. The Secretary of State for Health and all NHS organisations have a duty under this Act to make arrangements for the safe keeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

1.9 This Code concentrates on the management of records through their lifecycle, i.e. from creation to eventual archiving or destruction. This Code must be read in conjunction with the materials published by the Professional Records Standards Body (PRSB) for Health and Social Care standards.

1.10 Appropriate adherence to the Code during a records lifecycle ensures that the Trust is compliant with the General Data Protection Regulation (GDPR) which will supersede the Data Protection Act during 2018, and will cover in full manual structured filing systems or those were a set of personal data is accessible according to specific criteria. The GDPR does not cover or apply to unstructured filing systems.

1.11 Guidance laid out in the Code also includes reference to how organisations can be compliant with Government recommendations covering the use of public archives. Since January 2015, public sector organisations are now required to transfer records selected for permanent preservation under the Public Records Act to approved Places of Deposit 20 years after their creation, rather than 30 years.

1.12 The Trust Board has adopted this records management policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- compliance with legislation and standards
- better use of physical and server space
- better use of staff time
- improved control of valuable information resources
- reduced costs
- support the organisation achieving its overall strategy
- provide a framework for supporting standards, procedures and guidelines and regulatory requirements (such as CQC and the HSCIC hosted DH Information Governance Toolkit) by ensuring that necessary records are available for use in demonstrating current practice. This also provides a framework for enabling the Trust to respond to the records management requirements outlined in the Freedom of Information Act, the Data Protection Act and the Environmental Information Regulations 2004

1.13 The Trust also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

1.14 This policy, alongside the Code, sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

1.15 This policy document should be read in conjunction with the Trust's Information Lifecycle Management (ILM) and Corporate Records Strategy which sets out how this policy's requirements will be delivered.

1.16 The objective of the policy is to set out the approach taken within the Trust to provide a robust Records Management framework for the current and future management of information.

2.0 Scope of the Policy

2.1 In the context of corporate information assurance, corporate information refers to information generated and received by an organisation other than clinical/care (or service user) information. The term refers to information generated by an organisation's business activities, and therefore will include records from the following (and other) areas of the organisation:

- The Office of the Chief Executive
- Trust Board business
- Trust Governors
- Directorate of Estates & Facilities
- Directorate of Finance
- Directorate of Strategy & Planning
- Directorate of People & Organisational Effectiveness
- Deputy Chief Executive's Office & Directorate of Operations
- Chief Nurse Directorate
- Medical Director's Office
- Directorate of Performance Assurance & Trust Secretary

2.2 Examples of corporate information from these areas would include:

- Policies and procedures
- Strategies and action plans
- Minutes and agendas
- Reports (e.g. annual, accounting, Board)
- Financial Standing Orders
- Public consultations
- Databases
- Contracts

2.3 When handling any type of record, it is important to make the distinction between a record and a document. In the context of the IG Toolkit requirement, a document becomes a record when it has been finalised and becomes part of an organisation's corporate information. At this point it should only be held in the corporate system, i.e. a network drive, shared folder and not on a local drive on a PC or laptop.

2.4 As previously defined, the revised Code now also includes reference to clinical records. Therefore to better understand the scope of this policies application (and the more detailed Code, referenced throughout), the following provide examples of records that should be managed using the guidelines set out within the Trust Policy/Code:

- Function:
  - Patient health records (electronic or paper based, including those concerning all specialties and GP records)
  - Records of private patients seen on NHS premises
  - Accident and emergency, birth and all other registers
  - Theatre registers and minor operations (and other related) registers
  - Administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint handling)
  - X-ray and imaging reports, outputs and images
  - Integrated health and social care records
  - Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions
- Format:
  - Photographs, slides and other images
  - Microform (i.e. microfiche/microfilm)
  - Audio and video tapes, cassettes, CD-ROM etc
  - Emails, websites and intranet sites that provide key information to patients and staff, text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype (which are considered to be corporate records)
  - Computerised records
  - Scanned records

2.5 Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format.

3.0 Aims of the Trust Records Management Policy – Key Points

3.1 The aims of the Trust Records Management System are to ensure that:

- **records are available when needed** – from which the Trust is able to form a reconstruction of activities or events that have taken place
- **records can be 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
- **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
- **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
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format
- **records are secure** – from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required
- **records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value

  and

- **staff have guidance to refer to** – so that all staff are made aware of their responsibilities for record-keeping and record management

3.2 This policy provides an overall policy statement on how it manages records, including electronic records.

4.0 Aims of the Records Management Code of Practice for Health & Social Care 2016

4.1 The Data Protection Act (DPA) sets out in law how personal and sensitive personal information may be processed. The DPA principles are:

- Personal information must be fairly and lawfully processed
- Personal information must be processed for limited purposes
- Personal information must be adequate, relevant and not excessive
- Personal information must be accurate and up to date
- Personal information must not be kept for longer than is necessary
- Personal information must be processed in line with the data subjects' rights
- Personal information must be secure
- Personal information must not be transferred to other countries without adequate protection

4.2 The Code is also designed to aid adherence to the Caldicott principles:

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

5.0 Duties and Responsibilities – Also See Appendix A

5.1 Chief Executive

5.1.1 The Chief Executive has overall responsibility for records management in the Trust. As the officer accountable, he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is the key to this as it will ensure appropriate, accurate information is available as required.

5.1.2 The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

5.2 Director of Performance Assurance & Trust Secretary

5.2.1 The Director of Performance Assurance & Trust Secretary will hold the day to day responsibility and lead role for the management of corporate records within the Trust.

5.2.2 The Director of Performance Assurance & Trust Secretary will be responsible for advising on queries/issues raised around any records containing person identifiable information.

5.3 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

5.4 Trust Lead for Information Governance / Information Governance Steering Group

5.4.1 The Trust Lead for Information Governance/Information Governance Steering Group is responsible for ensuring that this policy is implemented, through the Information Lifecycle Management (ILM) and Corporate Records Strategy and that the records management system and processes are developed, co-ordinated and monitored.

5.4.2 The Trust Lead for Information Governance is responsible for freedom of information, data protection and other information governance work areas and works closely with the lead for records management (Director of Performance Assurance & Trust Secretary).

5.4.3 Responsibility for Corporate Records Management within functional specialities (e.g. Estates, Finance, Information Management & Technology, Human Resources, Purchasing/supplies, Governance and Performance Assurance etc) will be undertaken by individuals nominated within each directorate.

5.5 Health Records Manager

5.5.1 The Health Records Manager is responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

5.5.2 Additional Health Records policies should be referred to for specific guidance, i.e.:

- Health records library access
- Health records filing procedures
- Health records availability/unavailability procedures
- Creating and tracking of health records

5.5.3 Health Records Managers will have up to date knowledge of the laws and guidelines relating to confidentiality, data protection (including subject access requests), and freedom of information requests. However support and advice is available from the Lead for Records Management or the Lead for Information Governance.

5.6 Local Records Managers

The responsibility for local records management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units and business functions within the Trust have overall responsibility for implementing the policy and in particular the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policies.

5.7 All Staff

5.7.1 All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced. All staff will receive appropriate training to ensure knowledge of responsibilities, in particular those relating to the Common Law Duty of Confidence.

5.7.2 All staff, on induction should be aware and have this guidance made available to them.

5.8 Healthcare Professionals – Also See Appendix B

5.8.1 Healthcare professionals contributing to the clinical record need to ensure the quality of information recorded, pertaining to a patients care is accessible, interpretable and trustworthy. Healthcare professionals, as part of their professional duties, are therefore required to be aware of and be compliant with minimum standards of quality documentation. Most professional bodies and Royal Colleges have produced their own bespoke guidance on this subject, healthcare professionals should be working to ensure compliance with these minimum standards of best practice.

5.8.2 If no professional guidance or speciality specific guidance exists, healthcare professionals should familiarise themselves with the Academy of Medical Royal Colleges (AoMRC) generic medical record keeping standards (hosted by the Royal College of Physicians) prepared for use in the NHS. These standards, for ease of access, are cited in Appendix B of this policy.

6.0 Accountability

6.1 **All** Managers are personally accountable for the quality of records management within the Trust.

6.2 **All** Line Managers/Supervisors must ensure that their staff are adequately trained and work to appropriate guidelines.

6.3 Ownership and copyright in these records, as a rule, is with the Trust and not with any individual employee.

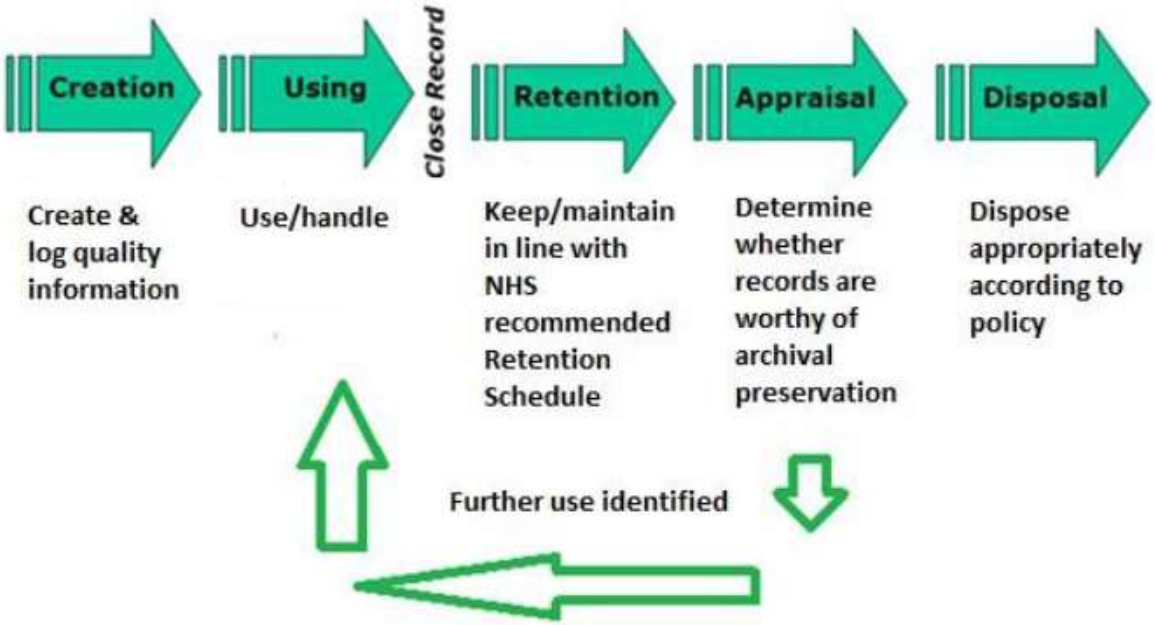
6.4 The Board is responsible for endorsing this policy statement via the approval mechanisms established and delegated authority to the Trust Governance & Assurance Committee (TGAC).

7.0 How to Manage Records

7.1 Records / Information Lifecycle – Best Practice

7.1.1 The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest. This best practice lifecycle is pictorially represented in the following diagram.

Figure 1 - The Records/Information Lifecycle



7.1.2 Using the above steps as a framework, the following headed sections provide the best practice and references to the Code for greater detail/guidance.

7.2 CREATION of Records

7.2.1 It is important that records are kept in their context and the best way to achieve this is to file or classify them. Records cannot be tracked or used efficiently if they are not classified or if they are classified inappropriately.

7.2.2 Records captured or filed in a corporate filing system (i.e. a shared accessible network drive like H Drive) will possess some of the necessary characteristics to be regarded as authentic and reliable. Good quality document standards are essential to provide accurate records of the trust's activities.

7.2.3 To support the filing within the corporate system, a common format for where new records are created, will ensure that those responsible for record retrieval are able to locate records more easily. Guidance on the common format to be used is sub-divided into 5 headings:

- **Referencing to be applied to new records:**

  - A referencing system should be used that meets the organisation's business needs, and can be easily understood by staff members that create documents and records. The most commonly used within the Trust is alphanumeric as it allows letters to be allocated to business activities and as such, within the Trust's corporate filing system on H Drive, each major business function has filing for shared access by teams within each of those areas

  - The index 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 and logical names to assist filing and retrieval of records

  - The Trust's corporate filing system should be used, specifically shared network drives enabling access for others. The Trust uses its H drive for this purpose. Filing on local drives or individual PCs/laptops should be actively discouraged

  - For paper corporate documents (where electronic versions do not exist) an index or register is needed to signpost to where paper corporate records are stored i.e. the relevant folder of file. However, it can be also a guide to the information contained in those records.

- **Version control standards to be followed:**

  - For paper records that are originally created electronically, version control is important as documents may undergo a lot of revision and redrafting. Version control is the management of multiple revisions to the same document and differentiates one version from another. It is particularly important that the final version is identified correctly for referencing in paper format and eventual archiving

  - Most documents will only need a simple version control techniques, such as the use of naming conventions. Use a unique version number to distinguish one version from another

  - Use this procedure for all documents where more than one version exists, or is likely to exist in the future. Use a version numbering system that uses version number with points to reflect major or minor changes, such as version 1.1 (first version with a minor change), version 2.0 (second version with a major change), version 2.2 (third version with minor change)

- Put the version number and date on the document itself. The version numbers must be on the document cover and in the footer of each text:
  - **Link to Code:** https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
  - Code page 16-18: best practice in determining classification
  - Code page 19: best practice in storage of records

- **Agreed naming conventions to be used:**
- The Trust follows advice issued by the National Archives:
  - Give a unique name to each record
  - Give a meaningful name which closely reflects the record 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

    and
  - Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version)
    - **Link to Code:** https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
    - Code page 15: best practice guidance on recording and naming conventions

- **Where original records should be filed:**
  - The Trust will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. The inventory of record collections will facilitate:
    - the classification of records into series
    - the recording of the responsibility of individuals creating records
    - The register will be reviewed regularly

- The Trust will maintain by department, a list of record categories, which are important enough to warrant formal registration. This is for the most part a function supported by the Trust Document Control System, ensuring that key corporate information to guide staff in their practice is reviewed regularly and accessible via the Trust's Hub

- Registration will reflect the Trust's statutory and legal obligations as well as its own business and information needs

- The Trust will have in place means of locating the whereabouts of all registered records. Wherever practical and appropriate this will be an electronic tracking system

    - **Link to Code:** https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

    - Code page 15: best practice guidance on recording and naming conventions

    - Code page 16: best practice in determining records that need to be kept

- **When to apply a protective mark:**

    - When corporate records are entered into the Document Control System these records are protected from editing and access to the original editable document is monitored by the Trust Document Controller. This is to preserve the timeliness and trustworthiness of the information stored within the Document Control System. This process is administered by the Trust Document Controller

    - This process ensures that there is an audit trail

7.3 USING Records

7.3.1 Records Maintenance:

- Paper contained within the records should be arranged in a logical structure and be ordered chronologically. Duplicate papers should be removed and where a file becomes too large, a second volume should be created

- **Specific guidance to medical records:** Paper contained within the records should be arranged by speciality and all relevant information placed behind the appropriate speciality divider and ordered in date order, most recent date directly behind the divider (for further information relating to this process please refer to the Health Records Filing Procedures). Where a file becomes too large a second volume should be created, for further details relating to the administration of this process within Health Records please refer to the Health Records Filing Procedures and the Health Records Splitting Procedures

- Where records are transferred from one location to another location, the person transferring the records should update the Clinical Record Tracking System (CRT) accordingly. CRT should be updated for every movement of a clinical record (for further guidance please refer to the Creating and Tracking Health Records Electronically Process). Health Records should be transported securely at all times (for further guidance please refer to the Transportation and Conveyance of Health Records Process)

- Services and departments should devise a file plan to keep track of all the records they hold to assist with records auditing. The file plan should be reflected in the physical storage of the files. The information held in paper records may be required to respond to a request under the Freedom of Information Act 2000. Such requests must be processed within a specific timescale which require records to be readily accessible to authorised staff

- All records within the Trust will be stored securely in accordance with the Data Protection Act 1998 and Caldicott Principles

- The Trust will maintain registration with the Information Commissioner's Office

- The process of registration, storage and retrieval will be subject to audit review

- Healthcare professionals making entries into the clinical record should be familiar with and adhere to a minimum standard expected in relation to record keeping/documentation standards – see Appendix B for list of the Academy of Medical Royal Colleges (AoMRC) generic medical record keeping standards (hosted by the Royal College of Physicians) prepared for use in the NHS.

7.3.2 Disclosure:

- Only the specific information required should be disclosed to authorised parties and always in accordance and with strict adherence to, the Data Protection Act and the Freedom of Information Act.

- The Trust's Caldicott Guardian's support staff should be involved in any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality – NHS Code of Practice.

7.3.3 Transfer

- The mechanisms for transferring information from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The Directorate of Performance Assurance can advise on appropriate safeguards. Guidance can also be found within the Information Governance Toolkit on the CFH website: http://systems.hscic.gov.uk/infogov

7.4 RETENTION of Records

7.4.1 It is a fundamental requirement that all of the Trust's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the Trust's business functions.

7.4.2 The Trust has adopted the retention periods set out in the Records Management: Code of Practice for Health and Social Care 2016. The retention schedule will be reviewed periodically by the Information Governance Alliance and this policy/document will be reviewed at least every 2 years.

7.4.3 The recommended minimum retention periods will be applied to both paper and electronic records. The deletion of e-mails should at all times reflect the context and content of the message.

7.4.4 The '20-year rule' – Public Records Act and transfer to Places of Deposit:

- Guidance laid out in the Code also includes reference to how organisations can be compliant with Government recommendations covering the use of public archives. Since January 2015, public sector organisations are now required to transfer records selected for permanent preservation under the Public Records Act to approved Places of Deposit 20 years after their creation, rather than 30 years. Compliance with this guidance is assessed annually by the National Archives undertaking a survey establishing the extent of public records that have been preserved in places of deposit

- Public records requiring consideration as to permanent preservation at a place of deposit are defined as "information that has been 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). Your records provide evidence of your organisation's activities." Examples of such records include minutes, registers, correspondence files and plans. Adherence to the Public Records Act covers non-digital records only and should not be confused with the separate process for retention of certain records to use in ongoing business activities

  - The Trust will seek to ensure that electronic data is managed to prevent any corruption or deterioration:

    - **Link to Code:** https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

    - Code pages 41-80: best practice guidance on retention schedules

    - Deletion must conform to retention and destruction criteria as laid out in the Code (https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care, pages 41-80)

    - Code page 21: best practice guidance on digital media

    - Code pages 23-25: best practice guidance on digital media continuity, preservation and forensic readiness

7.4.5 Scanning of Records:

- Specific and comprehensive guidance on scanning from paper format to digital format is contained within the Code, at the following location:
  - **Link to Code:**

    https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
  - Code pages 39-40: Scanned records

7.5 APPRAISAL of Records

7.5.1 Destruction will be normally actioned after the minimum retention period specified, unless the appropriate Executive Director advises the Trust Board that a record be retained for an extended period.

7.5.2 The Trust will calculate the recommended minimum retention periods from the end of the calendar or accounting year following the last entry:

- **Link to Code:**
  https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
- Code page 22: best practice guidance on review for continued retention

7.6 DISPOSAL of Records

7.6.1 Most NHS records, even administrative ones, contain sensitive and/or confidential information.

7.6.2 Destruction management will ensure that confidentiality is safeguarded at every stage.

7.6.3 Destruction will ensure complete illegibility and will either be by shredding, pulping, incineration or in the case of electronically held data, by purging the magnetic media.

7.6.4 Contractors used to undertake the destruction process will be certified to do this work, and a certificate of destruction will be issued and held within Northern Lincolnshire & Goole NHS Foundation Trust for each destruction request.

7.6.5 It is particularly important under the Freedom of Information legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies which have been formally adopted by the organisation and which are enforced by properly trained and authorised staff. Therefore it is necessary that all records should be disposed of appropriately using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of information with archival value:

- **Link to Code:** https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
- Code pages 20-21: best practice guidance on destruction options

8.0 Further Guidance: How to Deal with Specific Types of Records

8.1 The Information Governance Alliance have written this section to deal with a number of issues raised by health and social care records managers to TNA, the HSCIC and the DH between 2009 and the end of 2015 since the previous Code was issued in 2006.

8.2 These issues relate to the following health and social care records:

- General Practitioner Records
- Records at Contract Change
- Prison Health Records
- Youth Offending Service Records
- Secure Units for patients detained under the Mental Health Act 1983
- Family Records
- Child School Health Records
- Integrated Records
- Integrated Viewing Technology and Record Keeping
- Complaints Records
- Specimens and Samples
- Continuing Care Decisions Records
- Records of Funding
- Ambulance Service Records
- Adopted Persons Health Records

- Health Records of Transgender Persons
- Witness Protection Health Records
- Controlled Drugs Regime
- Asylum Seeker Records
- Occupational Health Records
- Public Health Records
- Records of non-NHS funded patients treated on NHS premises
- Patient/Client Held Records
- Records dealt with under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000
- Staff Records
- Email and Record Keeping Implications
- Records Created via Social Media
- Records Created Through Bring Your Own Device (BYOD)
- Cloud Based Records
- Website as a Business Record
- Scanned Records
- Duplicate Records
- Edisclosure/Ediscovery and Records Implications

8.3 Information:

- **Link to Code:** https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care
- Code pages 26-40: best practice guidance on destruction options

9.0 Legal and Professional Obligations

9.1 All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Code, in particular:

- The Public Records Act 1958
- The Public Records Act 1958, revised guidance from 01 January 2015, reduces the time frame from 30 to 20 years
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The Records Management Code of Practice for Health and Social Care 2016

9.2 Additionally any new legislation affecting records management as it arises.

10.0 Monitoring Compliance and Effectiveness

10.1 Audit

10.1.1 The Trust will survey or audit corporate records. This will not mean that every single record has to be recorded in a central index but it will involve knowing what series of records are held by which business areas and that there are named information asset owners managing all records appropriately.

10.1.2 It may be possible to link this process to information asset management. To do this, it must identify where the records are being held and that they are being held under the correct security conditions and in the case of clinical records, remain confidential. The process can be used as an opportunity for asset owners to identify how long their records need to be held. The process will also identify business critical assets and ensure that there are adequate business continuity measures in place to assure access.

10.1.3 The results of audits will be reported to the Information Governance Steering Group.

10.2 Review

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced). It will be reviewed and updated in conjunction with the Trust's Information Lifecycle Management (ILM) and Corporate Records Strategy (2017-2019).

11.0 Associated Documents

11.1 Destruction and Retention – Clinical Health Records Policy.

11.2 Information Lifecycle Management (ILM) and Corporate Records Strategy Corporate Records Management Strategy.

11.3 Health Records Filing Procedures.

11.4 Health Records Splitting Procedures.

11.5 Creating and Tracking Health Records Electronically Process.

11.6 Transportation and Conveyance of Health Records Process.

11.7 Health Records Management Policy & Strategy.

12.0 References

12.1 Records Management: Code of Practice for Health and Social Care 2016 (Information Governance Alliance, 2016).

12.2 The Public Records Act 1958 (amended by the Freedom of Information Act 2000).

12.3 International Standard ISO, 15489, Records Management.

12.4 Model Action Plan for Developing Records Management Compliant with the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000 [National Archives].

12.5 Lord Chancellor's Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000 November 2002.

12.6 NHS Digital – Information Governance Toolkit requirements for the management of organisational/corporate records in Acute Trusts, Requirement No: 14-601.

12.7 The National Archives annual survey and guidance on the '20-year rule', February 2017 [http://www.nationalarchives.gov.uk/about/our-role/plans-policies-performance-and-projects/our-projects/20-year-rule]

13.0 Definitions

None.

14.0 Consultation

14.1 Information Governance Steering Group.

14.2 Trust Governance & Assurance Committee for Approval.

15.0 Dissemination

Dissemination will be via the Trust Intranet.

16.0 Implementation

For implementation details, see the Information Lifecycle Management (ILM) and Corporate Records Strategy (2017-2019).

17.0 Equality Act (2010)

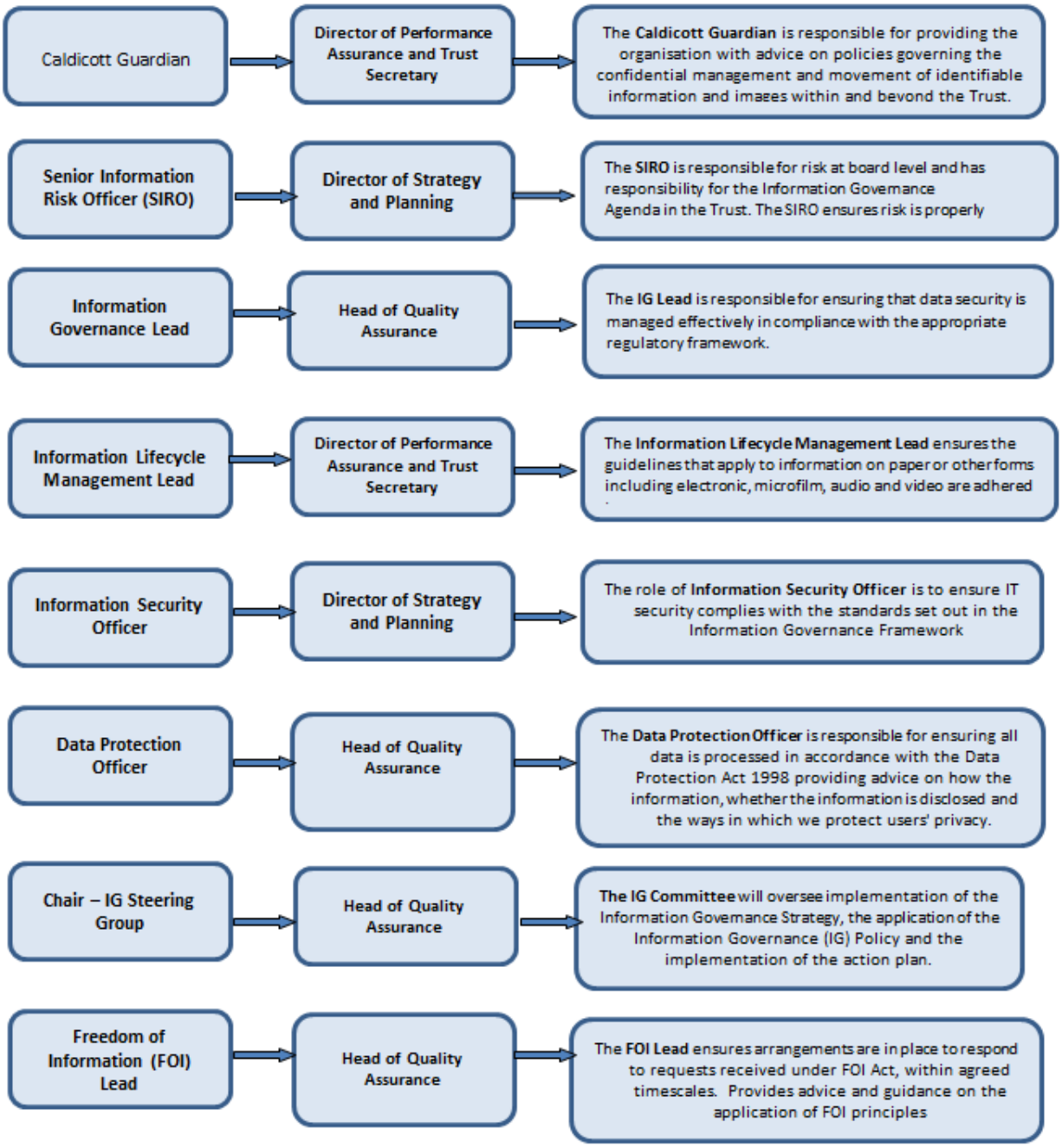
17.1 In accordance with the Equality Act (2010), the Trust will make reasonable adjustments to the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Trust will endeavour to develop an environment within which individuals feel able to disclose any disability or condition which may have a long term and substantial effect on their ability to carry out their normal day to day activities.

17.2 The Trust will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Trust's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010).

The electronic master copy of this document is held by Document Control, Directorate of Performance Assurance, NL&G NHS Foundation Trust.

Appendix A

Information Governance Roles and Responsibilities



Appendix B

Table 1 - AoMRC medical record keeping standards

Standard Number	Description
1	The patient's complete medical record should be available at all times during their stay in hospital
2	Every page in the medical record should include the patient's name, identification number (must include NHS number, may include local ID) and location in the hospital
3	The contents of the medical record should have a standardised structure and layout
4	Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order
5	Data recorded or communicated on admission, handover and discharge should be recorded using a standardised proforma
6	Every entry in the medical record should be dated, timed (24 hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned, dated and timed[27]
7	Entries to the medical record should be made as soon as possible after the event to be documented (for example change in clinical state, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded
8	Every entry in a medical record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made
9	On each occasion a transfer of care occurs, the consultant responsible for the patient's care will change the name of the responsible consultant and the date and time of the agreed transfer of care
10	An entry should be made in the medical record whenever a patient is seen by a doctor. When there is no entry in the hospital record for more than four (4) days for acute medical care or seven (7) days for long-stay continuing care, the next entry should explain why
11	The discharge record/discharge summary should be commenced at the time a patient is admitted to hospital
12	Advanced Decisions to Refuse Treatment, Consent, and Cardiopulmonary Resuscitation decisions must be clearly recorded in the medical record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney

Further information about professional standards for records can be obtained from your relevant professional body. The main standard setting bodies in Health and Social Care in England are noted in Appendix Two of the full code: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care)