NHS
Wigan Borough
Clinical Commissioning Group

Records Management Policy

DOCUMENT CONTROL PAGE	
Title	Records Management Policy 2021
Supersedes	Records Management Policy 2018
Minor Amendments	Updated to align with the Records Management Code of Practice 2021 (A guide to the management of health & social care records) published by NHSX in August 2021 following a public consultation undertaken in 2020.
Author	Chris Lawless (IG Manager)
Ratification	Information Governance Operational Group – September 2021 Governance & Audit Committee – December 2021.
Application	All Staff
Circulation	All Staff
Review	December 2023
Date Placed on the Intranet/SharePoint:	**EqIA Registration Number** **37/14**

Contents

Introduction

1. All NHS records are public records (apart from the relevant exemptions under the Data Protection Legislation) under the terms of the Public Records Act 1958. Each member of staff is responsible for the records they create and use.

2. 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 their eventual disposal.

3. Failure to comply with relevant legislation could result in reputational damage to the CCG and carries the risk of significant financial penalties being imposed by the Information Commissioner's Office (ICO).

4. The purpose of this document is to act as a guide to provide guidance and signpost to all CCG (henceforth referred to as "the CCG") staff on Records Management.

5. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority / honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

6. This document sets out a framework within which the staff responsible for managing the CCG'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

7. The CCG is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include improved commissioned care and services for the public, better use of the physical environment and electronic server space, better use of staff time, improved control of valuable assets and information and resources, compliance with legislation and standards and reduced costs for the CCG.

Key Legislation / Codes of Practice

8. The CCG has a statutory obligation to maintain accurate records of its activities which are public records under the terms of the:

    - **The Public Records Act 1958** - An Act of Parliament to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.

- **The Data Protection Act 2018** - An Act of Parliament which regulates the processing of personal data relating to living individuals, including the obtaining, holding, use or disclosure of such information. Access to the health records of living patients is governed by this Act.
- **The UK General Data Protection Regulation (GDPR)** regulates the processing of personal data. Article 30 of the GDPR requires that all organisations maintain records of processing activities. Transparency is key in data protection legislation it is imperative that we inform individuals about our data processing activities. It is therefore imperative that good records management is in place in the CCG. Staff must ensure that information relating to records management / retention schedules are completed in the CCG Information Asset and Data Flow Mapping Registers which are located on SharePoint.
- **The Freedom of Information Act 2000** - An Act of Parliament that makes provision for the disclosure of information held by public authorities or by persons providing services for them. The Lord Chancellor's Code of Practice on the management of records is issued under section 46 of this Act.
- **The Access to Health Records Act 1990** - An Act of Parliament that regulates access to the health records of a deceased person.
- **The Regulation of Investigatory Powers Act 2000** which permits the 'interception' of communications, such interception must be proportionate to the needs of the organisation, society and the users of the communication system.
- **Records Management Code of Practice 2021** (A guide to the management of health & social care records) was published by NHSx in August 2021. This acts as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice and sets out a schedule of minimum retention periods for many types of records. It includes a records retention schedule which is a formal control document. It sets out the classes of records which the CCG retain and the length of time these are retained before a final disposition action is taken i.e. destruction or transfer to a permanent place of deposit, such as the National Archives. All staff should follow and adhere to the retention schedule contained within the national RM Code of Practice.

9. This policy should only be used as a guide. The NHSX Records Management Code of Practice 2021 (located on SharePoint) should be consulted and followed on all matters related to records management as it contains the full and in depth detail required.

10. Information and information systems are important assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the CCG. This policy is a key component of the CCG's overall 'Data Security (IG)

Management Framework and should be considered alongside the other Data Security (Information Governance) related policies and procedures and other relevant CCG policies.

Aim

11. The aim of this policy is to ensure:

- **Accountability** - Records are adequate to account fully and transparently for all business actions and decisions, in particular to:
    - protect legal and other rights of staff or those affected by those actions.
    - facilitate audit or examination.
    - provide credible and authoritative evidence.
- **Availability** - To ensure events or activities can be followed through and form a reconstruction as necessary.
- **Accessibility** – Can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with their initial use, with the current version being identified where multiple versions exist
- **Interpretation** - The context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and were appropriate, how the record is related to other records.
- **Quality** – Records can be trustworthy - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- **Maintenance through time** - That 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.
- **Security** – Records are secure from unauthorised or inadvertent alteration or erasure, access and disclosure are properly controlled and there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

12. The CCG records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision making, protect the interests of the CCG and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

13. The CCG 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.

Roles & Responsibilities

Managing Director / Accountable Officer

14. The Managing Director / Accountable Officer has ultimate responsibility for the implementation of the provisions of this policy. As the ‘Accountable Officer’ he / she is responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

Assistant Director, Governance

15. Overall responsibility for Records Management lies with the Assistant Director of Governance who delegates the responsibility for managing the development and implementation of procedural documents to the Information Asset Owners within the CCG.

Directors, Associate Directors, Senior Managers & Line Managers

16. Directors, Associate Directors and senior managers are personally accountable for the quality of records management within the CCG and 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, data security and protection.

Caldicott Guardian

17. The Caldicott Guardian is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential personal information are in place. This includes ensuring patient records, where processed by the CCG, adhere to the Caldicott principles.

Senior Information Risk Owner (SIRO)

18. The Chief Finance Officer is the designated Senior Information Risk Owner and the Information Governance Lead in the CCG. The SIRO will ensure that the procurement of new electronic systems that hold records are risk assessed for security and privacy at the early stage of the project and that current systems are risk assessed.

The Information Governance Manager

19. The IG Manager will ensure that guidance is readily available to staff on best practice in records management and will raise identified issues at the Information Governance Operational Group (IGOG) meetings.

All Staff

All CCG employees (including temporary and contract staff), whether clinical or administrative, who create, receive and use records in any form of media have records management responsibilities. In particular, all staff must ensure they keep appropriate records of their work in the CCG and manage those records in keeping with this policy and with any guidance. Furthermore, under the Public Records Act any record that any individual creates is a public record and may be subject to both legal and professional obligations, including compliance with relevant legislation including the Freedom of Information Act 2000, the UK GDPR and the Data Protection Act 2018.

20. It is the responsibility of all staff including those on temporary or honorary contracts, agency staff and students to comply with this policy. Staff will receive instruction and direction regarding the policy from a number of sources including from their line manager, team briefings and communications.

What is a record?

21. ISO 15489-1:2016 defines a record as: *'Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business'.*

22. Section 205 of the Data Protection Act 2018 defines a health record as a record which:

- Consists of data concerning health.
- Has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates

23. A record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees

- Administrative records (including e.g. personnel, estates, financial and accounting records: notes associated with complaint-handling);
- CDs and DVDs (if still used).
- Computer databases, output, and disks (if still used), and all other electronic records.
- Photographs, slides and other images;
- Scanned documents.
- Any portable media containing information.
- Material intended for short term or transitory use, including notes and “spare copies” of documents.
- Meeting papers, agendas, formal and informal meetings including notes taken by individuals in note books and bullet points.
- Emails.

24. A document becomes a record when it has been finalised (declared) and becomes part of the organisation’s corporate information.

Key Components of Records Management

25. Records management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record. The key components of records management are:

- Record creation.
- Record keeping.
- Record maintenance (including tracking of record movements).
- Access and disclosure.
- Closure and transfer.
- Appraisal.
- Archiving and disposal.

Records Management Process

26. The CCG follows a ‘Records Management’ process to ensure records all processed confidentially and securely via paper or electronic means on the CCG network ensuring that they are:

- Available when needed so that events or activities can be followed through and reconstructed as necessary.
- Accessible, located and displayed in a way consistent with their initial use, with the current version being identified where multiple versions exist.
- Able to be interpreted and set in context: who created or added to the record and when, during which business process, and how the record is related to other records.
- Trustworthy and hold integrity, reliably recording the information that was used in, or created by, the business process.
- Maintained over time, irrespective of any changes of format so that they are available, accessible, able to be interpreted and trustworthy.
- Secure from unauthorised or inadvertent alteration or erasure, with access and disclosure being properly controlled and audit trails tracking use and changes.
- Held in a robust format which remains readable for as long as records are required.
- Retained and disposed of appropriately using documented retention and disposal procedures, which include provision for reviewing and permanently preserving records with particular archival value.

Record Creation

27. Each department should have a process for documenting its activities which takes into account this policy to advise staff what information needs to be retained as a record, in what format and where it should be stored.

28. Records must hold adequate ‘integrity’ so their evidential weight is legally admissible and can withstand scrutiny in the event of litigation or claim. True and accurate records protect the right of the individual or the CCG.

29. Records should be created and maintained in a manner that ensures that they are clearly identifiable, accessible, and retrievable in order to be available when required.

30. Each record should be given a unique name / number. Where possible the name should be meaningful and closely reflect the record content. Similarly structured names should be given to records which are linked. The following should be documented when a paper or electronic record is created:

- File reference.
- File title.
- If appropriate protective marking i.e. Official, Official – Sensitive.
- If possible an anticipated disposal date and what action to take.
- Where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed.
- All filling systems to be documented and kept up to date.

31. The CCG will ensure consistency is established in the way information is presented to target audiences, both internally and externally. When creating a record the CCG will need to achieve the following:

- Ensure information can be located promptly and time wasted on locating or recreating lost documents reduced.
- Appropriate disclosure of information to staff or the public who require and are authorised to access.
- Evidence of individual and corporate performance and activity.
- Physical and digital space is used effectively.
- Records created are able to meet the CCG’s legal obligations.
- Organisations can preserve its corporate memory and track business decisions or transactions over time.

32. Managers of departments should ensure staff are made aware of their responsibilities, are properly trained and that reviews and monitoring for compliance are undertaken.

Record Naming

33. Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the CCG to assist in good management of records. Staff should seek guidance from line / department manager before naming any documents, this is particular important where they are records that contain personal data.

34. Staff should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

Record Quality

35. Records must be complete and accurate in order to allow staff to undertake appropriate actions in the context of their responsibilities, the integrity of a record is vital.

36. Full accurate records must possess the following characteristics

- Complete (Captured in full).
- Accurate (exact).
- Relevant (meets current and potential user needs).
- Accessible (retrievable when required).
- Timely (recorded and available as soon after the event as possible).
- Content – The information it contains (text, data, symbols, numeric, images or sound).
- Structure – Appearance and arrangement of the content (style, font, page and paragraph breaks, links and other editorial devices).
- Context – Background information that enhances understanding of the business environment/s to which the records relate (e.g. metadata, software) and the origin (e.g. address title, function or activity, organisation, program or department).

37. The structure and context of each record will alter depending on the record being created. For example, policies will need to hold contextual information like author names, review date and ratification information; whereas agenda does not require that type of information but should include attendees, venue, date and time.

38. The CCG should establish quality checks which will minimise / eradicate errors. Dependent on the type of record the following checks should be undertaken:

- Ensure the correct retention period has been input onto the document which confirms the right retention / destruction will have been calculated;
- Ensure all names are spelt correctly and in the correct format;
- Ensure the unique identifiers are correct and in the right format;

- Check the barcode number is correct (if relevant);
- The inventory should be checked for all other possible errors.

Record Tracking, Storage and Maintenance

39. Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what format(s) they are made accessible, and their relationship to organisational functions. An information inventory or record audit is essential to meeting this requirement. The inventory will help to enhance control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.

40. The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions. Tracking mechanisms should record the following (minimum) information:

    - The item reference number of the record or other identifier.
    - A description of the item (e.g. file title).
    - The person, unit or department, or place to whom it is being sent.
    - The date of the transfer to them.
    - The date of the information returned (if applicable).

41. Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

42. Digital / electronic records must be saved to a CCG networked drive in the appropriate folder.

43. Records containing personal, special category or business sensitive data must be protected from unauthorised access, inadvertent alteration or erasure, at all times.

44. Equipment / facilities used to store records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allows maximum accessibility to the records commensurate with frequency of use.

45. For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to readable information.

46. When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure.

Archiving policies and procedures should be observed for both paper and electronic records.

47. Any duplicate documents (except where copy letters sent or received have had comments added by hand) should be culled and confidentially destroyed.

48. In order to identify when records were last active or the service user was last in contact with the service, it is advisable that year labels are used on the front cover.

49. If there are separate sets of records relating to the same service user which is a consequence of historic practice, these should all be stored together upon discharge and kept together when archived.

50. A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation.

Record Transportation

51. All staff have a legal duty to keep information safe and secure. Security and confidentiality of records should be paramount at all times. This is particularly important, in high security risk situations such as the transportation of records between sites. Records should not be taken off site without the authorisation of the relevant line manager. To reduce the risk of loss of records and the risk of breaches of confidentiality, staff are advised to observe the following minimum precautions:

- Records must only be taken off–site / removed from site when absolutely necessary and with the written permission of the 'Information Asset Owner'.
- To ensure staff are aware of the location of the record a log of what information is being moved and why, and when applicable, details of where and to whom it is being taken, by whom and how, should also be recorded.
- Records should not be left unattended. In the event that they are left unattended, every precaution must be taken to keep them secure an inaccessible to unauthorised persons.
- Records being transported should always be kept out of sight.
- Records should not be left unattended in cars.
- Records which need to be dispatched externally must be sent by secure post or approved Courier. An up to date list of courier companies which have signed up to the national agreement for public sector bodies can be viewed on the Crown Commercial services website (http://ccsagreements.cabinetoffice.gov.uk).Where secure post is required – A tracked and trace service should be used, for example Royal Mail Special Delivery. Recorded Delivery does not meet Department of Health standards as the post is not tracked throughout the whole journey.

Lost / Missing Records

52. A lost / missing record is a record either that cannot be found following a search or is unavailable.

53. In the event of a missing record, a thorough search must be undertaken. This will include initiating a search at the base (this may include facilitating / requesting searches at non-CCG locations if appropriate in addition to reviewing the tracking history of the record).

54. The loss of records constitutes a reportable incident and should be reported immediately in accordance with the CCG's Data Security (IG) Incident Reporting Procedure and an investigation will commence.

55. It is important that records can be retrieved at any time during the retention period, whether for management or legal purposes.

Paper Records to Electronic (Scanning)

56. For reasons of business efficiency and in order to free storage space, the CCG may consider the option of scanning into electronic format which exist in paper format.

57. Where this is proposed the 'Information Asset Owner' must first complete a 'Data Protection Impact Assessment (DPIA)' which must be reviewed and approved by the Information Governance Operational Group (IGOG) before scanning has commenced.

58. When looking to scan records the following should be considered:

- That the scanned image can perform equally as well as the original paper record.
- That scanned images can be challenged in court (just as paper can).
- There must ability to demonstrate authenticity of the scanned image.

59. Examples of common mistakes when scanning records are:

- Only scanning one side and not both sides, including blank pages - to preserve authenticity, both sides of the paper record, even if they are both blank, must be scanned (this ensures the scanned record is an exact replica of the paper original).
- Scanning a copy of a copy - leading to a degraded image.
- Not using a method that can show that the scanned record has not been altered after it has been scanned – questions could be raised regarding process and authenticity.
- No long-term plan to enable the digitised records to be stored or accessed over the period of their retention.

60. Once scanned records have been digitised and the appropriate quality checks completed and the scanned record is deemed to be legally admissible it will then be possible to destroy the paper original, unless the format of the original has historical value, in which case consideration should be given to keeping it with a view to permanent transfer.

61. Please note: No paper record should be destroyed without the prior approval of (IGOG).

62. In the event that scanned records do not meet the British Standard (10008) for "Legal Admissibility of Electronic Records", the original paper records must be retained in accordance with normal retention and disposal schedules.

For more information in relation to scanned records please refer to page 112 and 113 of the NHSX Records Management Code of Practice 2021.

Evidence required for courts

63. In UK Law, the civil procedure rules allow evidence to be prepared for court and, as part of this, the parties in litigation can agree what documents they will disclose to the other party and, if required, dispute authenticity. The disclosure of digital records is referred to as E-Disclosure or E-Discovery. The relevant part for disclosure and admissibility of evidence is given in the Ministry of Justice's Civil Procedure Rules - Part 3. If records are arranged in an organised filing system, such as a business classification scheme, or all the relevant information is placed on the patient or client file, providing records as evidence will be much easier. Further advice on electronic records and evidential weighting can be found in BIP10008: Evidential Weight and Admissibility of Electronic Information.

Records involved in Investigations, Inquiries, Litigation and Legal Holds

64. A Legal Hold, which may also be referred as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation or inquiry for e.g. The Infected Blood Enquiry.

65. The CCG has a duty to preserve relevant information when a lawsuit, investigation or inquiry is reasonably anticipated.

66. Staff who have been notified of a Litigation, Investigation or Inquiry or have reasonable foresight of a future Litigation, Investigation or Inquiry must notify their line manager and 'Information Asset Owner' immediately who will seek guidance from the IG Manager if required. This may result in records being held beyond their identified retention period.

67. The Department Manager along with the IG Manager will ensure there is a log of the request, detailing the records that have been placed on hold.

68. When a Legal Hold is terminated, records previously covered by the Legal Hold should be retained in accordance with the applicable retention period under this policy without regard to the Legal Hold, and retained non-records or records not previously subject to retention may be destroyed (after appraisal has taken place).

Email and Record Keeping

69. Email is widely accepted as the primary communication tool used every day by all levels of staff in organisations. They often contain business (or in some cases clinical) information that is not captured elsewhere and so need to be managed just like other records. The National Archives has produced guidance on managing emails.

70. Email has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record. However, a common problem with email is that it is rarely saved in the business context.

71. The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates.

72. Where email is declared as a record or as a component of a record, the entire email must be kept, including attachments so the record remains integral - for example, an email approving a business case must be saved with the business case file. For more detail regarding Emails please see The Acceptable Use of IT Policy located on SharePoint.

Record Retention / Destruction

73. The Data Protection Act 2018 stipulates that personal data should not be kept for longer than is necessary. The CCG will conform to this principle by applying minimum record retention periods. The CCG recognises that records must be retained for a minimum period of time for legal, operational, research and safety reasons.

74. The CCG will establish record retention periods in accordance with the type of record and its importance to the CCG business function by fully adopting the retention periods set out in the NHSX Records Management Code of Practice 2021 which is available on the CCG SharePoint site.

75. The retention periods given in the NHSX RM COP are the minimum periods for which records must be retained for health and care purposes. In most cases, it will

be appropriate to dispose of records once this period has expired, unless the records have been selected for permanent preservation.

76. The CCG recognises that the destruction of records is an irreversible act that must be clearly documented. All records identified for disposal will be destroyed under confidential conditions.

77. A decision for destruction of records must be made by the relevant Information Asset owner who has knowledge of the relevant business area to which the records relate, in conjunction with the IG Manager and the Information Governance Operational Group.

The following are examples of when information cannot be destroyed or disposed of:

- If it is subject to a form of access request, for example, Right of Access Request (SAR) or an FOIA request.
- If it is required for notified legal proceedings, for example, a court order, or where there is reasonable prospect of legal proceedings commencing (an impending court case). This information will possibly be required for the exercising or defending of a legal right or claim.
- If it is required for a coroner's inquest.
- If it is of interest to a public inquiry, for example, who will issue guidance to organisations on what kind of records they may require as part of the inquiry. Once notified, organisations can re-commence disposal, taking into account what records are required by the inquiry. If in doubt, check with the Inquiry Team.

78. A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the CCG, thus making the CCG aware of any destroyed records. Destruction of records must not take place without recorded agreement from the Information Governance Operational Group.

79. Local records managers (Heads of Service) will ensure that records that are no longer required for business purposes are closed, the appropriate destruction date recorded and archived in the CCG secure storage facility.

80. It is important not to get disposal and destruction confused.

81. Disposal does not necessarily mean destruction, though it is one method of disposal. Disposal is the removal of the CCG's responsibility for the record, this could be through appropriate destruction of the records, or transferral of the records to an approved Place of Deposit. This is likely to be 'The National Archives' and is only appropriate for records of historical or continuing value.

82. In the event that records need to be kept for longer than the minimum retention period due to ongoing administrative need, this should be referred to the IG Manager in the first instance and then to IGOG. If there is approval that the records should be retained for a period longer than the minimum (provided that this does not total a

period of 30 years or more from creation) an internal retention schedule will be developed accordingly. (Records may not be retained for more than 30 years without the approval of the National Archives).

83. If a record due for disposal / destruction is the subject of a statutory request for information or potential legal action, destruction should be delayed until disclosure has taken place or the legal process complete. Advice should be obtained from the IG Manager.

Please see the ‘Retention Schedule’ contained within the NHSX Records Management Code of Practice 2021 for further details.

Record Closure

84. Before records are classed as ‘closed’ i.e. made inactive and transferred to secondary storage, ceased to be in active use other than for reference purposes they should be appraised.

85. Records should be checked on a regular basis to assess whether they are coming to the end of their retention period.

86. When paper records or electronic records have been closed, a log detailing who has appraised and approved should be kept, along with the date of closure and whether it was disposed or destroyed, and the method.

Records Management Audits

87. It is the responsibility of Information Asset Owners to carry out regular validation processes and data checks / audits are on data being recorded within their area to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include, checking for duplicate or missing data, checking for deceased patients, validating lists and ensuring that national definitions and coding standards are adopted.

88. The results of the audits should be reported to the Information Governance Operational Group.

Equality and Diversity Statement

89. Promotion of equality, valuing diversity and upholding human rights are fundamental to providing good quality healthcare, addressing health inequalities and promoting wellbeing.

90. The CCG is committed to promoting Equality and Diversity through its Equality and Diversity Strategy 2013-2016.

91. To enable the CCG to meet its legislative duties and regulatory guidance, all new and revised procedural documents, services and functions are to undertake an impact assessment to ensure that everyone has equality of access, opportunity and outcomes regarding the activities. Contact the Governance Team for support to complete an initial assessment. Upon completion of the assessment, Governance will assign a unique EqIA Registration Number. The CCG undertakes Equality Impact Assessments to ensure that its activities do not discriminate on the grounds of:

- Age
- Disability
- Gender reassignment
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation

92. Before any committee, group or forum validate a strategy, policy or procedural document an EqIA Registration Number will be required.

93. This policy has been impact assessed for equality through the CCG's approved procedure. It has been assigned the EqIA number 37/14.

Consultation & Approval

94. Approval of this policy is through the Information Governance Operational Group (IGOG) and the Governance & Audit Committee.

95. Once approved the document will be placed on SharePoint.

96. The Assistant Director of Governance & Information Governance Manager will be responsible for monitoring compliance with this policy. It will also be monitored through staff awareness and as supporting evidence for the CCG Data Security & Protection Toolkit annual submission.

97. This policy will be reviewed on a two yearly basis and in accordance with the following as and when required:

- Legislative changes.
- Good practice guidance.
- Case law.
- Significant incidents reported; new vulnerabilities.
- Changes to organisational infrastructure.

Dissemination and Implementation

98. Dissemination: Following approval of strategies, policies and procedural documents it is imperative that all employees and other stakeholders who will be affected by the documents are proactively informed and made aware of any changes in practice that will result. All approved documents will be posted on SharePoint and the CCG's website where appropriate.

99. Implementation: Awareness will be raised regarding the changes to or introduction of this policy via the Governing Body, Committee and Team meetings.

Standards and Key Performance Indicators

100. This policy will be reviewed every two years or when there are significant changes in the policy.

101. This policy will be monitored for effectiveness by self-assessment against any external accreditation that is applicable and may be subject to review by internal audit.

References and Bibliography

- NHSX Records Management Code of Practice 2021
- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Regulation of Inventory Powers Act 2000 The National Archives: http://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide1.pdf
- The NHS Care Record Guarantee for England
- The Caldicott Guardian Manual 2017: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
- https://digital.nhs.uk/codes-of-practice-handling-information
- Data Security and Protection Toolkit (DSPT)
- ICO Guidance : https://ico.org.uk/

Associated CCG Documents

- Data Security, Protection and Confidentiality Policy.
- Data Security (IG) Handbook.
- Data Security and Confidentiality Audit Procedure.
- Secure Transfers of Data.
- Data Security (IG) Incident Reporting Procedure.