HEALTHIER PEOPLE,
BETTER FUTURE

NHS
Heywood, Middleton and Rochdale
Clinical Commissioning Group

Records Management Policy

Reference Number:	IG79
Version:	V5
Name/Department of originator/author:	Lisa Winstanley & Chris Lawless
Approval Committee	Information Governance Operational Group
Date Approved	May 2018
Ratified Body:	Corporate Governance Committee
Date ratified:	December 2018
Review date:	May 2020
Target audience:	All CCG employees, including Contractors, Agency workers and volunteers

DOCUMENT CONTROL

Policy Title:	Records Management Policy
Policy Area	Information Governance
This policy Supersedes	V4
Description of Amendment(s)	Updated to reflect new legislations (the GDPR and the Data Protection Act 2018)
This document should be read in conjunction with:	All other IG / Data Security related policies and guidance.
This document has been developed in consultation with:	GM Shared Services – People Services ☐ GM Staff Side ☐ Internal Auditors ☐ HMR CCG Staff ☐
Published by:	Heywood, Middleton and Rochdale Clinical Commissioning Group, Number One Riverside, Smith Street, Rochdale, OL16 1XU
Intended Audience:	All CCG employees, including Contractors, Agency workers and volunteers
Policy path location	SharePoint
Policy shared location	HMR CCG SharePoint

Document Approvals This document requires the following approvals:

Governance – Committee /Board/Other	Purpose	Outcome	Date
Information Governance Operational Group	Review and approval	Approved	16th May 2018
Corporate Governance Committee	Review and approval	Approved	12th December 2018

Policy review control information

Version	Date	Reviewer Name(s)	Comments
Draft V0.1	Dec 2013	GMSS IG Team	New policy
V1	Nov / Dec 2013	IGOG / FP & Risk	Approved
V2	Nov / Dec 2014	IGOG / FP & Risk	Approved
2.1 / V3	Oct / Dec 2015	IGOG (Oct) / FP & Risk (Dec)	Approved
V4	July / Aug 2017	IGOG July / CGC (Aug) approved via chairs actions.	Approved
V5	May 2018	IGOG	Approved

Contents

1. Introduction

1.1. The purpose of this document is to provide guidance to all NHS Heywood, Middleton and Rochdale CCG (henceforth referred to as "the CCG") staff on Records Management.

1.2 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. The CCG has a statutory obligation to maintain accurate records of its activities which are public records under the Public Records Acts 1958 & 1967.

1.3 The Records Management Code of Practice for Health and Social Care (published by the Information Governance Alliance in July 2016) is a guide for use in relation to the practice of managing 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. Please refer to: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

1.4 The implementation of the EU General Data Protection Regulation (GDPR) requires better records management. Organisations need to know what personal data they hold, be able to access it when they need to and ensure they keep it secure. Organisations must also show transparency and tell individuals what data they hold and who they share it with.

1.5 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 NHS 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.

1.6 For the purpose of this document CCG records refer to Corporate records (i.e. personnel files, minutes etc.) and clinical/health records (patient health records) where appropriate.

1.7 The CCG 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:

- Better use of physical and server space
- Better use of staff time

- Improved control of valuable information resources
- Compliance with legislation and standards
- Reduced costs.

1.8 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 corporate function.

1.9 The development of these procedures and practices will help the organisation meet the required standards ensuring that records are managed and controlled appropriately throughout their life cycle, in the most cost effective way, and in accordance with legal, operational and information needs.

1.10 It is the responsibility of all staff including those on temporary or honorary contracts, agency staff and students to comply with this policy.

1.11 The aims of this policy are to ensure that:

- **Records are available when needed** - from which the CCG 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 worthiness 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 are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

2. Purpose

2.1. The development of these procedures and practices will help the organisation meet the required standards ensuring that records are managed and controlled appropriately throughout their life cycle, in the most cost effective way, and in accordance with legal, operational and information needs.

2.2. This guidance relates to all clinical and non-clinical records held in any format by the CCG, or any on behalf of the CCG. 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, including:

- Administrative records including e.g. personnel, estates, financial and accounting records: notes associated with complaint-handling
- Audio and videotapes, cassettes and CD-ROMs
- Computer databases, output, and disks, and all other electronic records
- Material intended for short term or transitory use, including notes and “spare copies” of documents
- Meeting papers, agendas, formal and meetings including notes taken by individuals in note books and bullet points are all subject to the above
- Emails and other electronic communications.

2.3. Please note the above list is not exhaustive and where the policy refers to health records please note this advice refers to CCG staff who have legal justification to access health records.

2.4 A document becomes a record when it has been finalised and becomes part of the organisations corporate information. For further information on any of the above please refer to the CCG Information Governance Staff Handbook.

3. Definitions

3.1. 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 organisations 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.

3.2. In this policy, Records are defined as 'recorded information, in any form, created or received and maintained by the organisations in the transaction of its business or conduct of affairs and kept as evidence of such activity.

3.3. The term Records Life Cycle describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

3.4. Corporate/business records are defined as anything that contains information in any media, which has been created or gathered as evidence of undertaking of work activities in the conduct of business. Corporate records may also be generated through supporting patient care and can also be generated through agency/casual staff, consultants and external contractors.

3.5. Corporate records types include;

- Administrative records (including personnel, estates, financial and accounting, contract records , litigation and records associated with complaints- handling)
- Registers and rotas
- Office /appointment diaries
- Photographs, slides, plans or other graphic work (not clinical in nature)
- Micro film a (i.e. fiche/film)
- Audio and video tapes
- Records in all electronic formats including emails.

3.6. A health record is defined as being any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of the individual.

4. Roles and Responsibilities

4.1. Chief Officer

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

4.2 Caldicott Guardian

The CCG Caldicott Guardian is the conscience of the organisation and are responsible for ensuring that national and local guidelines on the handling of confidential personal information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.3 Senior Information Risk Owner (SIRO)

The SIRO, under delegated authority from the CO will oversee compliance with the DPA / GDPR and the development of appropriate policy and procedure. The SIRO will be advised by the nominated Data Protection Officer and supported by the CCG Information Governance Officers. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.

4.4 Data Protection Officer (DPO)

The DPO will facilitate 'accountability' and demonstrate the CCG's compliance with the GDPR and the Data Protection Act. Principal tasks are to advise the CCG and its staff on compliance obligations /provide advice on Data Protection Impact Assessments (DPIA) / monitor compliance with the GDPR and organisational policies including staff awareness and provisions for training. The DPO is the first point of contact with the ICO and data subjects for all data protection matters.

4.5. Information Asset Owners (IAO's) / Administrators IAA's)

Under the responsibility of the SIRO:

- Information Asset Owners (IAOs) will be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area
- Will ensure the integrity of the information within their area and restrict the use to only authorised users who require the access
- Will be responsible for the Information Asset assigned to them;
- Will ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a SAR;
- Will ensure that personal data held in the Information Asset is maintained in line with the CCGs Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy

Overall responsibility for the Records Management Policy and implementation lies with the CCG Information Governance Lead who has delegated responsibility for managing the development and implementation of records management procedural documents and for working with the GMSS Information Governance Team.

. The CCG Information Governance Lead is responsible for co-ordinating, publicising, implementing and monitoring the records management processes and reporting issues or concerns to the Information Governance Operational Group.

4.6. **Directors / Senior Managers / Information Asset Owners**

Directors, senior managers and Information Asset Owners are responsible 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 and data protection.

4.7. **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, 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 EU General Data Protection Regulations and the Data Protection Act 2018.

4.8. This responsibility is established at, and defined by, the law (Public Records Acts 1958 & 1967). Furthermore, as an employee of the NHS, any records created by an employee are public records.

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

5. NHS Number

5.1. The Health and Social Care Act 2015 came into force on the 1st October 2015 this mandates Health and Adult Social Care organisations to use a consistent identifier (the NHS Number) for data sharing associated with facilitating care for an individual. The use of the NHS number as the main identifier will help to reduce the risk of errors being made when identifying a record.

5.2. The NHS Number is a unique 10-digit number given to every baby born in England or patient registered with the NHS. This patient identifier enables clinical and administrative records to be exchanged more safely between electronic and manual system.

5.3 The CCG are required to demonstrate that they follow a consistent and comprehensive approach in using the NHS Number as the main identifier; however it must be noted that this is only in the case of **"Direct Patient Care".**

5.4. The **NHS number** is in the majority of cases widely used within health and social care organisations and should be present on all patient and service user records, both paper and electronic, as early in the care pathway as possible. It must be used alongside other demographic information to link together the correct records for a particular patient or service user. As a reminder the general principles of the NHS number standards are:

- **Find It** - find the NHS number for a person as soon as possible in the care pathway, ideally on initial contact with the service.
- **Will Use It** - use the NHS number to link a person to their care record; use the NHS number to search for an electronic record; use the NHS number on wristbands, documents and reports used for the care of the person.
- **Share It** - share the NHS number with other organisations so they can use it; include the NHS number on all correspondence and electronic messages.

5.5. It is important to remember the only legal gateway for the NHS number to be used is in the case of direct patient care and all such uses should be clearly identified on the CCG's Information Asset Register, Data Flow Mapping Register and Risk Assessments.

5.6. The outcomes of these reviews will be reported to the CCG's Information Governance Operational Group (IGOG), Senior Information Risk Owner (SIRO), Caldicott Guardian and the relevant Head of Service.

5.7. The CCG will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. The Information Asset Register will facilitate:

- The classification of records into series
- The recording of the responsibility of the individuals creating records.

6. Record Lifecycle

6.1. The term Records Lifecycle describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

7. Record Creation

7.1. The CCG should have a process for documenting its activities, taking into account the legislative and regulatory environment in which it operates.

7.2. 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.

7.3. All records should be complete and accurate:

- To allow staff to undertake appropriate actions in the context of their responsibilities;
- To protect legal and other rights of the organisation, patients, staff and other people affected
- To show proof of validity and authenticity.

7.4. 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. All records should have a unique number or filling system, which will be applicable only to that record. For example, a patient's medical record will be identifiable by the NHS number and an employee's personal file held in personnel number. Records must have clear and precise formats and must be structured in the same way that files of the same description are structured with an easy to follow standard index, either numerical, by date or alphabetically.

7.5. The following should be documented when a paper or electronic record is created:

- File reference;
- File title;
- If appropriate protective marking i.e. NHS Protect or NHS Confidential;
- 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.

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

7.7. All major decisions or key actions which may result from discussions or meetings should be recorded as this provides key evidence of business of business decision making activity

7.8. 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:

- Hold the necessary records to enable staff to perform their duties;
- 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.

A checklist on how to create a record is available on Appendix 1, Checklist; Creating a Record.

8. Record Quality

8.1. All CCG staff should be fully trained in record creation use and maintenance, consummate 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 record
- What records are used for and the importance of timeliness, accuracy and completeness
- How to update and add information from other sources

8.2. Full and accurate records must possess the following three essential characteristics

- 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).

8.3. 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.

8.4. Quality Checking - The CCG should establish quality checks which will minimise / eradicate errors. A different member of staff should quality check to the one that has input the information. 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.

For further information on how to check the quality of a record refer to Appendix 2 – Quality of Record entries.

9. Record Keeping

9.1. 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.

9.2. Paper and electronic keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.

9.3. All records must conform to these record keeping guidelines, legislation, NHSLA, DoH, Information Governance requirements and professional guidelines.

10. Record Maintenance

10.1. 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.

10.2. 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.

10.3. 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.

10.4. Equipment used to store current 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 allow maximum accessibility of the information commensurate with its frequency of use.

10.5 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.

10.6. All individual files should be weeded on a regular basis, to ensure the key documentation is readily identifiable and accessible. Bulky files should contain no more than 4 years' worth of records. Any file older than this should be culled and removed to an inactive file. The front cover of each such volume must clearly indicate that other volumes exist.

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

10.8. 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.

10.9. 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.

10.10 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.

11. Tracking of Records

11.1 For Accurate recording and knowledge of the whereabouts of all clinical and non-clinical records is essential if the information they contain is to be located quickly and

efficiently. Records must not be taken out of the office unless this has been agreed by the Line Manager and a tracking mechanism is in place. The tracking system could be manual or electronic and linked to a department's IT system.

11.2. 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).

11.3. Manually operated tracking systems are common methods for manually tracking the movements of active records and include the use of:

- A paper register – a book, diary, or index card to record transfers, item reference number of the record or other identifier;
- File "on loan" (library type) cards for each absent file, held in alphabetical or numeric order;
- File "absence" or "tracer" cards put in place of absent files.

11.4. Electronically operated tracking systems include:

- A computer database, excel spreadsheet in place of paper/card index;
- Bar code labels and readers linked to computers;
- Workflow software to electronically track documents.

11.5. The minimum data which needs to be recorded includes:

- Service user's name;
- NHS number;
- Date the records were removed,;
- Destination and name of intended recipient;
- Name of the person releasing the records.

11.6. A well thought out, manual or electronic system should:

- Provide an up-to-date easily accessible movement history and audit trail;
- Be routinely checked and updated;
- Be recorded i.e. all movements of a record even if the record is exchanged between teams/staff members within the same building;
- Provide a return receipt and it made clear to whom the records should be returned ;
- Ensure information recorded on the tracking system must be correct and applicable to ensure the system remains effective;

- Take into consideration any filing that comes in whilst the records are traced out and must be filed according to local documented procedures until such time as the records are returned;
- Ensure that any records are returned safely to their correct home and absent records are chased on a frequent basis;
- Maintain a log of all records received into the department including the date received, service user name and NHS number.

11.7. Managers should ensure that training and procedures are in place for manual and electronic tracking systems and that they are being adhered to.

12. Record Transportation

12.1 CCG employees and contractors 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 should be tracked out of the respective department so that other staff are aware of the location of the record;
- Records should never be left unattended where it would be possible for an unauthorised person to have access to them;
- Records being transported should always be kept out of sight;
- If records are taken home, they must be stored securely in accordance with the staff members Professional Code of Conduct.

12.2. NHS organisations are required to map their information flows in accordance with the guidance in the Information Mapping Tool. The objective of this is to demonstrate that an organisation, in this case the CCG, clearly identifies and has addressed the risks associated with the transfer of identifiable information. This mapping requires all organisations to have an up to date register of information transfers (i.e. audit or map the flows of information in and out across the organisation).

12.3. Offsite movement of records or other confidential/sensitive information

12.4. Security requirements also apply when staff records are transported. It is recognised that staff may find it necessary to remove records from their base, to ensure business continuity. To reduce the risk of loss of such records and to reduce the risk of breaches of confidentiality there are various considerations to be made, based on best practice:

- Records should not be removed for administrative purposes i.e. writing reports. A trace should be kept at the base from which records have been removed and staff are aware of the location of the record;
- Records should not be left unattended in cars;
- Records kept in any staff possession should remain safe and secure at all times i.e. out of sight and locked away when not in use;
- Records should only be taken off site with the approval of the Line Manager. If a record is taken off site, it must be stored securely in accordance with the Confidentiality Code of Conduct – Guidelines for Staff;
- Any vehicle used for the transportation of records must be insured for business use. If the staff member is involved in a road traffic accident which necessitates the car being left on the roadside or taken to a garage, records should be removed. If this is not possible the matter should be reported to the Line Manager and an incident form completed.

For further information please refer to the CCG Secure Transfers of Data Procedure. This Procedure should be used when transporting any records from one location / organisation / or department to another.

13. Lost or Missing Records

13.1. A missing record is a record either that cannot be found following a search using tracking methods, including initiating a search at the base where the record should be kept.

13.2. The loss of records constitutes a reportable incident and should be reported in accordance with the CCGs Information Governance & Cyber Security Incident Reporting Procedure.

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

14. Scanning

14.1. All For reasons of business efficiency and in order to alleviate storage space/issues, the CCG can scan into electronic format inactive records which exist in paper format. The following factors should be taken into account:

- The costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;

- The need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created; and
- The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

14.2. In order to fully realise the benefits of reduced storage requirements and business efficiency, the CCG will securely dispose of the paper records that have been copied into electronic format and stored in accordance with appropriate standards.

15. Disclosure and Transfer of Records

15.1. There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. Guidance should be sought from the GMSS Information Governance Team prior to any disclosure. If the request for access to information is made under the Freedom of Information Act 2000, then the request should immediately be forwarded to the Patient Services Department within GMSS in order to comply with the deadlines specified in the Act.

15.2. The Caldicott Guardian should be made aware of any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice.

15.3. The mechanisms for transferring records 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 Information Governance Lead / GMSS IG Team can advise on appropriate safeguards.

16. Retention, Archiving and Disposal of Records

16.1. Appraisal refers to the process of determining whether records are worthy of additional retention or permanent archival preservation. If the latter, this should be undertaken in consultation with the National Archives, or with an approved Place of Deposit where there is an existing relationship.

16.2. The purpose of the appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

16.3. The procedure for recording the disposal decisions made following appraisal must be followed. The CCG will determine the most appropriate person(s) to carry out the appraisal in accordance with the retention schedule. This should be a senior manager with appropriate training and experience who has an understanding of the operational area to which the record relates.

16.4. Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility.

Please refer to the Records Management Code of Practice for Health and Social Care for guidance regarding retention schedules. If the information you require is nit contained within please contact the IG team for further guidance: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

17. Disclosure and Transfer of Records

17.1. Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. Each year a list of records coming to the end of their retention period should be reviewed. An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

17.2. Records / information contain personal confidential information and it is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and complete illegibility is secured. Destruction of all records, regardless of the media in which they are held should be conducted in a secure manner ensuring safeguards are in place against accidental loss or disclosure.

18. Retention Schedules and Record Disposal

18.1. It is a fundamental requirement that all of the CCG'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 CCG's business functions.

18.2. The CCG has adopted the retention periods set out in the NHS Records Management Code of Practice for Health & Social Care 2016. These retention schedules outline the recommended minimum retention period for NHS records:

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

18.3. Senior Managers will be responsible for ensuring disposal schedules are implemented as part of a rolling programme. Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry to the document. I.e. a file's first entry is in February 2001 and the last December 2006, the minimum retention period is eight years, it should therefore be kept in its entirety at least until 31st December 2014. If a member of staff feels that a particular record needs to be kept for longer than the recommended minimum period or there is a specific purpose further advice and approval should be sought from the Service Senior Manager / Director.

18.4. Where there are records held by the organisation that do not have a retention period advice should be sought from the Information Governance Operational Group where approval and inclusion of the retention period will be granted.

18.5. Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution that has adequate storage and access facilities. Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act.

18.6. Records not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear.

18.7. The methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Contractors, if used, are required to sign confidentiality undertakings and to produce written certification as proof of destruction.

18.8. 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.

18.9. If a record due for 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 Information Governance Lead.

18.10. It must be remembered at all times that the destruction of records is an irreversible act.

19. Records Management and System Audit

19.1. The process for monitoring and evaluating the effectiveness of this policy, including obtaining evidence of compliance will be part of the Data Security & Protection Toolkit (audit process). The CCG will regularly audit its records management practices for compliance with the framework.

19.2. The audit will:

- Identify areas of operation that are covered by the CCG'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 related procedures.

19.3. The results of audits will be reported to the relevant quality and standards groups within the CCG under designated authority from the CCG Governing Body.

20. Training and Awareness

20.1 Information Governance training is required to be undertaken on an annual basis. All CCG Staff will be made aware of their responsibilities for record-keeping and record management.

20.2. Where staff may take on a specific Information Governance roles within the CCG i.e. Records Manager, additional Information Governance training will be required. For further guidance please refer to the CCG Data Security Training Needs Analysis (TNA) Document located on SharePoint.

20.3. The CCG Information Governance Operational Group (IGOG) will be responsible for ensuring that this policy is implemented, and that the records management system and

processes are developed, co-ordinated and monitored.

20.4. This policy will be placed on SharePoint for all staff to access.

20.5. To maintain high staff awareness the CCG will direct staff to a number of sources:

- Policy/strategy and procedure manuals;
- Line manager
- Specific training courses
- Other communication methods, for example, staff/team meetings; network locations and CCG newsletters.

21. Equality Statement

21.1 In applying this policy, the CCG aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

21.2 It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all.

21.3 This policy has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. In carrying out its functions, HMR CCG must have due regard to the different needs of different protected equality groups in their area.

21.4 This applies to all the activities for which HMR CCG is responsible, including policy development and review.

21.5 **Due Regard**

21.6 The CCG's commitment to equality means that this policy has been screened in relation to paying due regard to the Public Sector Equality Duty as set out in the Equality Act 2010 to eliminate unlawful discrimination, harassment, victimisation; advance equality of opportunity and foster good relations.

22. Monitoring and Review

22.1 This policy will be reviewed every 2 years, and in accordance with the following as and when required:

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

22.2. Where there are no significant alterations required, this Policy shall remain for a period of no longer than two years of the ratification date.

23. Legislation and Related Documents

23.1. All NHS records are classed as public records under the Public Records Acts. The CCG will take actions as necessary to comply with the legal and professional obligations set out in the Records Management Code of Practice 2016, in particular:

- The Public Records Act 1958
- The EU General Data Protection Regulation (GDPR) 2018
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice

23.2. This Policy should be read in conjunction with the following CCG Policies (please note this list is not exhaustive):

- Data Security, Protection and Confidentiality Policy
- Data Quality Procedure
- Information Security Policy
- Secure Transfers of Information
- Information Risk Policy.

Appendix 1 Checklist: Creating a Record

- Check you know how to create adequate records and what information they should contain
- Follow relevant CCG policies and guidelines to ensure creating full and accurate records
- Establish and document local procedures on creating business critical records to the department, or if using a corporate or local proforma; and ensure procedures are followed
- Use corporate templates wherever available so it clearly identifies the nature of the information and type of document
- Include fundamental elements like author, date, title, department, contact details, and it holds the approved corporate identity
- Ensure documents hold the relevant information specifically required for that type of record, like in the case of policies or forms. In the example of a policy this would include: executive signature, approval route, review date, EIA if applicable
- Capture decision-making in minutes or when creating records or emails, and that you maintain a record of any transactions. For example, agreements or discussions that impact on your work or with other teams/organisations
- Always ensure that the information you are recording is accurate and objective
- Use standard terms to describe documents and be consistent with use of acronyms
- Identify the creator and use their job title, plus other people who may have contributed to the document
- Explain within the text of the document, any codes or abbreviations used, as their meaning may become less clear over time
- Do not use logos, icons or catchphrases on documents that have been formally approved; include the CCG logo in all appropriate records
- Remember that your records, or local record keeping practises may be required for performance checks or in the invent of a claim or litigation.

Appendix 2 – Quality of Record Entries

Good record keeping is a mark of skilled and safe practice, whilst careless or incomplete record keeping often highlights wider problems with individual practice.

Structure and Content of Records

Where possible there must be one set of records for each data subject/individual.

Unique Identifier

A unique identifier must be used to ensure that records can be retrieved when archived or stored.

Record entries should be:

- Complete
- Legible
- Contemporaneous, i.e. written as soon as possible
- Consecutive
- If appropriate, signed by the data subject/individual according to the service specific policies
- Only in exceptional circumstances, should entries to records be delayed

Abbreviations

Abbreviations must not be used routinely.

Alterations

Contemporaneous alterations to records are acceptable when an entry has been made in error. When this occurs, the author must take the following actions:

- Make an entry stating “written in error” near the incorrect entry
- Sign, date and record the time of the annotation making the change
- Strike through the original entry with a single line leaving it discernible
- Make the correct entry, signing it and dating it.

It is unacceptable to:

- Delete or erase notes, such that the entry is no longer legible
- Use correction fluids of any part of a clinical record
- Change original entries, other than as specified above
- Change entries made by another person.