Southport and Formby
Clinical Commissioning Group

NHS Southport and Formby Clinical Commissioning Group

Corporate Records Management and Retention Policy 2014-2016

Title:		Document Number		
NHS Southport and Formby CCG Corporate Records Management and Retention Policy				
Next Revision Due: October 2016		**Author**	**Consultation and Communication**	**Approved by**
Department responsible for this document:	Cheshire and Merseyside Commissioning Support Unit (North West CSU)	Senior Governance Manager (Information Governance)	Corporate Governance Support Group	SFCCG Quality Committee
DESIGNATION	**NAME**	**SIGNATURE**		**DATE**
Chief Finance Officer	Martin McDowell			October 2014

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0	Corporate Governance Support Group	8th October 2014
	SFCCG Quality Committee	17th December 2014

Contents

Section **Page**

1. EXECUTIVE SUMMARY

1.1. The Corporate Records Management and Retention Policy for the Clinical Commissioning Group (CCG) sets out the requirements of all staff when managing the retention of records. The Policy is supported by substantial guidelines and procedures, which give further details of how to comply with the actual Policy.

1.2. Staff should treat this Policy as guidance based on best practice for managing corporate records. In general terms, this Policy covers all records (documents), which the CCG has produced.

1.3. The records management function is recognised as a specific corporate responsibility within the CCG. It provides a managerial focus for records of all types in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal. All confidential papers will be disposed of by shredding.

1.4. Clearly defined responsibilities and objectives are set out below, and the CCG is committed to ensure adequate resources to achieve them.

1.5. Archiving of corporate paper documents will be carried out in line with the CCG arrangements in place, which will be reviewed over time as the CCG develops.

2. INTRODUCTION

2.1. All CCG staff must ensure they are familiar with the contents of this policy, which describes the standards of practice we require in the management of our corporate records. It is based on current legal requirements and professional best practice.

2.2. All organisations need to keep some records, and patients and the public would rightly expect that the CCG maintains records on its activities and decisions that affect their health service in an exemplary way.

2.3. Records and Documents are different. Documents consist of information or data that can be structured or unstructured and accessed by people in the CCG. Records provide evidence of the activities of the CCG's functions and policies. Records have strict compliance requirements regarding their retention, access and destruction, and generally have to be kept unchanged. Conversely, all records are documents.

2.4. A record can be in various formats including email, paper, digital, social media, videos and telephone messages. Records are created to provide information about what happened, what was decided, and how to do things. Individuals cannot be expected or relied upon to remember or report on past policies, discussions, actions and decisions accurately all of the time. So, as part of their daily work they keep a record – by updating a register or database, writing a note of a meeting or telephone call, or filing a letter or email – which ensures that they and their successors have something to refer to in the future.

2.5. Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based healthcare. Information has most value when it is accurate, up-to-date and accessible when it is needed. An effective records management function ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required.

2.6. Records management is about controlling records within a framework made up of policies, standard operating procedures, systems, processes and behaviours. Together they ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the organisation benefits from effective management of one of its key assets, its records.

2.7. A records retention schedule is a control document. It sets out the classes of records which the CCG retains and the length of time these are retained before a final disposition action is taken (i.e. destruction or transfer to archives). It applies to information regardless of its format or the media in which it is created or might be held. All staff members should be familiar with this records retention schedule and apply retention periods to records.

2.8. A records management policy is a cornerstone of effective management of records in an organisation. It will help to ensure the CCG keeps the records it needs for business, regulatory, legal and accountability purposes.

2.9. The purpose of this policy is to establish a framework in which the CCG's records can be managed, and to provide staff members with a high-level overview of the legal obligations that apply to NHS records.

3. OBJECTIVES

3.1. The primary function of the Policy is to improve the management of all types of NHS records, with regard to their preservation, retention and destruction.

3.2. The CCG has a statutory duty to make arrangements for the safekeeping and eventual disposal of their records.

3.3. The suggested retention periods should be taken by NHS organisations to be a guide based on best practice, and therefore followed for all corporate (non-clinical) records.

3.4. Ensuring local application of this Policy and its supporting guidelines and procedures, is the responsibility of all staff.

4. SCOPE OF THE POLICY

4.1. All staff (including Governing Body members, temporary staff, secondees, work placed students and contract staff) are within the scope of this policy

4.2. It also applies to anyone contracted to the CCG, who, in the course of their work is required to create and/or access corporate records normally restricted to directly employed staff.

5. GENERAL CONTEXT

5.1. The Records Management: NHS Code of Practice replaces previous guidance as listed below:

- HSC 1999/053 – *For the Record*.
- HSC 1998/217 – *Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients* (Replacement for FHSL (94)(30))
- HSC 1998/153 – *Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice.*

5.2. Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based healthcare, and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when it is needed. An effective records management service ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required. Information may be needed:

- to support patient care and continuity of care;
- to support day-to-day business which underpins the delivery of care;
- to support evidence-based clinical practice;
- to support sound administrative and managerial decision making, as part of the knowledge base for NHS services;
- to meet legal requirements, including requests under subject access provisions of the Data Protection Act or the Freedom of Information Act;
- to assist clinical and other types of audits;
- to support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research; or
- to support patient choice and control over treatment and services designed around patients.

5.3. The Code of Practice identifies the specific actions, managerial responsibilities, and minimum retention periods for the effective management of all types of NHS records (i.e. both corporate and health records) from creation, as well as day-to-day use of records, and storage, maintenance and ultimate disposal procedures.

6. LEGAL AND PROFESSIONAL OBLIGATIONS

6.1. The CCG will take actions as necessary to comply with the legal and professional obligations set out for records, and in particular:

- Public Records Act 1958
- Data Protection Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act 2000
- Records Management: NHS Codes of Practice (Part 1 and 2)
- NHS Information Governance: Guidance on Legal and Professional Obligations

The Public Records Act 1958 is 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 1998 is 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 Freedom of Information Act 2000 is 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 is an Act of Parliament that regulates access to the health records of a deceased person.

The Regulation of Investigatory Powers Act 2000 which permit the 'interception' of communications. Such interception must be proportionate to the needs of the organisation, society and the users of the communication system.

The Records Management: NHS Codes of Practice (Part 1 and 2) are 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. They are based on legal requirements and professional best practice.

NHS Information Governance: Guidance on Legal and Professional Obligations provides guidance on the range of legal and professional obligations that affect the management, use and disclosure of information.

6.2. Failure to comply with the regulations stated in paragraph 2.1.could result in reputational damage to the CCG and carries financial penalties of up to £500,000 imposed by the Information Commissioner. This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

7. CORPORATE LEVEL PROCEDURES

7.1. This Policy covers the management of both documents and records in the CCG. The policy sets in place the strategic governance arrangements for all documents and records produced and received by the CCG in accordance with agreed best practice, as well as the principles established in ISO 15489 (the International British Standard for Records Management).

7.2. This policy is mandatory and applies to all information in all formats. It covers all stages within the information lifecycle, including create/receive, maintain/use, document appraisal, declaration as a record, record appraisal, retention and disposition.

7.3. Staff members must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Freedom of Information Act 2000 or the Data Protection Act 1998.

7.4. Staff members are expected to manage records about individuals in accordance with this policy irrespective of their race, disability, gender, age, sexual orientation, religion or belief, or socio-economic status.

8. KEY PERFORMANCE INDICATORS

8.1. The following key performance indicators have been identified to measure the effectiveness of this document:

i. staff will know where to access the document;

ii. staff will know how to archive documents;

iii. policy to be reviewed by the review date.

9. ROLES AND RESPONSIBILITIES

i. Accountable Officer

The Accountable Officer through the Executive Management Team is accountable for Records Management within the CCG. Responsibilities include:

- Operational responsibility for the Records Management policy and the overall development and maintenance of the Records Management Framework.
- The application of this policy in respect of ensuring effective employee records management and for managing access requests for those records made under the Data Protection Act 1998.
- Ensuring this policy complies with legal and regulatory edicts.
- Providing learning and development with key learning points from this policy and for monitoring compliance with the policy to assess its overall effectiveness.
- Developing and supporting a culture of high quality records management practice across the CG to deliver associated organisational benefits.
- Knowing what records the CG holds and where they are, by conducting regular stock-takes of records.
- Ensuring that records created by the CCG are stored securely and that access to them is controlled.

ii. CCG Managers

CCG Managers are responsible for:

- Ensuring that the Policy is implemented within their area of responsibility.
- Ensuring that the Policy is built into local processes and that there is on-going compliance.
- Ensuring that any breaches of the Policy are reported, investigated and acted upon.

iii. All Staff

- All staff (including Governing Body members, temporary staff, secondees, work placed students and contract staff) are subject to this Policy.
- All staff are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they adhere to the Policy on a day to day basis.

iv. Information Asset Owners

- Information Asset Owners are responsible for ensuring that for each asset that they ‘own’ is managed in accordance with this policy, and also for maintaining adequate records within the context, both legal and regulatory, of the business area the asset operates.
- Set Owners within each CCG area will champion records management from a local level supporting their team in records management matters. Roles and responsibilities are outlined in Appendix A.

- All staff are responsible for keeping a record of any significant business transaction conducted as part of their duties for the CCG. The record should be saved appropriately, a retention period assigned and access controls applied if necessary.

v. Information Governance Senior Manager (from the CSU)

The Information Governance Senior Manager will:

- Maintain the currency of this Policy.
- Provide advice on request to any member of staff on the issues covered within it.

10. MONITORING RECORDS MANAGEMENT PERFORMANCE

10.1. A number of bodies monitor NHS performance in respect of records management. The Audit Commission regularly conducts studies into records management and related information quality issues. The Department of Health collects performance details as part of the annual Information Governance Toolkit assessment. The NHS Litigation Authority also undertakes a risk assessment survey as an integral part of the Clinical Negligence Scheme for Trusts (CNST).

10.2. Other bodies likely to comment on records management performance include the Information Commissioner when investigating alleged breaches of Data Protection or Freedom of Information legislation, or in promoting the Lord Chancellor's Code of Practice on Records Management under section 46 of the Freedom of Information Act.

11. RECORDS MANGEMENT OBLIGATIONS

11.1. All individuals who work for an NHS organisation are responsible for any records which they create or use in the performance of their duties. Furthermore, any record that an individual creates is a public record.

11.2. The key statutory requirement for compliance with records management principles is the Data Protection Act 1998, where personal information is held. It provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer. It applies to personal information generally, not just to health records. Therefore the same principles apply to records of employees and contract

workers held by employers, for example in finance, personnel and occupational health departments.

12. RECORDS INVOLVED IN INVESTIGATIONS, LITIGATION AND LEGAL HOLDS

12.1. A Legal Hold, also known 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 or investigation. Organisations have a duty to preserve relevant information when a lawsuit or investigation is reasonably anticipated. Staff must immediately notify the Senior Information Risk Owner (SIRO) if they have been notified of a Litigation or Investigation or have reasonable foresight of a future Litigation or Investigation as this could result in records being held beyond their identified retention period.

12.2. The SIRO will use this information and log details of the records which have been placed on hold.

12.3. The Legal Hold decision will be determined by Senior Management.

12.4. 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.

13. RECORD ACCESS

13.1. There are a range of statutory provisions that give individuals the right of access to information created or held by the CCG such as a data Subject Access Request (SAR), or a Freedom of Information request. The Data Protection Act 1998 allows individuals to find out what personal data is held about them. The Freedom of Information Act 2000 gives the public the right of access to corporate information held by public authorities.

14. RECORDS SECURITY: WORK BASE, HOME WORKING, AGILE WORKING

14.1. All person identifiable data or commercially sensitive data must be saved with appropriate security measures. A secure drive has been created to hold such CCG data.

14.2. Staff should not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of the CCG.

14.3. Removable Media must be CCG owned and encrypted by the ICT service. Ideally, person sensitive data should not be stored on any removable media, however if there is no other option ensure this data is stored on a corporate encrypted device and deleted once transferred to identified secure area folder.

14.4. When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.

14.5. The CCG follows *Safe Haven* procedures to ensure staff are aware how to receive personal information in a secure manner at a protected point.

14.6. Each department should have at least one designated safe haven contact point. Ideally, all information transmitted to the organisation should pass to these contact points. The CCG will operate safe haven procedures for all flows of person identifiable information.

14.7. When transferring data either directly or via a third party, ensure security measures and precautions have been actioned by the sender and receiver. A robust contract should be in place detailing responsibilities.

14.8. Never leave your computer logged on when unattended.

15. INFORMATION LIFECYCLE MANAGEMENT

15.1. Information Lifecycle Management is included within this Corporate Records Management and Retention Policy.

15.2. All NHS records produced are subject to a range of legislation, including the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

15.3. It is important that employees recognise information security issues arising from the storage of person identifiable data (PID) and that they continue to

use information in accordance with the Data Protection and Freedom of Information Acts, and the NHS Records Management Code of Practice.

15.4. The Caldicott Guardian continues to be responsible for protecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring that patient identifiable information is shared in a secure and responsible manner.

15.5. The Senior Information Risk Owner (SIRO) continues to be responsible for ensuring that identified information threats are followed up and risks managed.

15.6. Records and Information Management plays an integral role within The CCG as it underpins effective information sharing within our organisation and externally to patients and suppliers. The law requires certain records to be kept for a defined retention period; however records are used on a daily basis for internal purposes to help make decisions, provide evidence, etc. There are 5 stages in the Records Life Cycle:

Stage 1: Creation and Receipt

This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. It can be created by internal employees or received from an external source.

Stage 2: Distribution

Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are distributed when photocopied, printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used.

Stage 3: Use

This stage takes place after information is distributed. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other CCG operations. It is also considered the *Active Phase*.

Stage 4: Maintenance

Maintenance is when records are not used on a day to day basis and are stored in the Records Management system. Even though they are not used on a day to day basis, they will be kept for organisational, legal or financial reasons until they have met their retention period.

The maintenance phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in

a business decision. Records should not be removed from a Records Management system; the information should be copied and tracked to ensure no amendments were made.

Stage 5: Disposition

Disposition is when a record is less frequently accessed, has no more value to the CCG or has met its assigned retention period. It is then reviewed and if necessary destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value to the CCG will be kept and sent to the National Archives, where it will be kept for the future of the organisation and may never be destroyed. This is the final phase of a records lifecycle.

16. RECORD NAMING AND GOOD PRACTICE

16.1. 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 aid in the management of records.

16.2. Staff members 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.

16.3. The CCG standard naming convention must be used for the filename of all electronic documents created by CCG staff members from the implementation date of this policy. New documents must follow the standard naming convention.

16.4. Version Control is the management of multiple revisions to the same document. Version control enables us to tell one version of a document from another.

16.5. Where records contain person identifiable data or corporate sensitive information it is a legal requirement that such data is stored securely. You must ensure such data is stored within the secure drive and have the correct protective marker applied.

16.6. Key electronic records must be held within shared drives rather than individuals' drives. This ensures that the record is easily accessible even in the document owner's absence.

16.7. Good record keeping should prevent record duplication. Staff members should ensure team members have not previously created a record prior to initiating a new document.

16.8. Staff members should ensure their handwriting is legible when making entries on paper records.

16.9. Staff members should ensure records are relevant including their opinions about individuals, as they have the right to be provided with a copy of their records.

16.10. Be aware when redacting Microsoft Word documents electronically by using the black highlight text tool as this process is reversible. A Microsoft Word file converted into PDF can be easily read merely by copying if from PDF back into Word. Best methods of redaction include cover up tape, specific blacking pen or scalpel.

17. RECORD KEEPING

17.1. 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.

17.2. 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.

17.3. 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.

17.4. 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.

17.5. 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. There should be archiving procedures in place for both paper and electronic records.

17.6. 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 CCG. Key expertise in relation to environmental hazards, assessment of risk, business continuity and other considerations is likely to rest with information security staff and their advice should be sought on these matters.

18. RECORD MAINTENANCE

18.1. At present there is no external data storage organisation for paper records. To keep costs low, and in accordance with our aim to move to become a largely paperless organisation, staff are encouraged to save in electronic format wherever applicable. Records which need to remain in paper format are 'Sealed' records which are usually identified by an embossed stamp and are executive level.

18.2. The movement and location of paper records should be controlled to ensure that a record can be easily retrieved at any time. This will enable the original record to be traced and located if required and must be held in a shared location.

18.3. Paper file storage must also be safe from unauthorised access and meet fire regulations.

18.4. Information Asset Owners should ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of the CCG.

18.5. Records held in electronic format and saved on shared drives have regular back-up copies scheduled and undertaken on a daily basis.

19. INFORMATION QUALITY ASSURANCE AND AUDIT

19.1. It is important that all NHS organisations train staff appropriately and provide regular update training. In the context of records management and information quality, organisations need to ensure that their staff are fully trained in record creation, use and maintenance, including having an understanding of:

- what they are recording and how it should be recorded;
- why they are recording it;
- how to validate information against other records – to ensure that staff are recording the correct data;

- how to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them;

- the use of information – so staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important); and

- how to update information and add in information from other sources.

19.2. 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 (for example finance, IT, HR). A Department information survey or record audit is essential to meeting this requirement. This survey will also help to enhance control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.

19.3. Paper and electronic record keeping systems should conform to the Corporate House Style and 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.

19.4. The record keeping system should either adhere to the Corporate House Style or should include a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information when it is needed and to maintain security and confidentiality.

20. RECORD DISCLOSURE

20.1. 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.

20.2. Only certain staff members have the authority, which is dictated by their role, to disclose records. Staff members with this authority should make a record of any copies of records they have disclosed, and to whom.

21. RECORD TRANSFER

21.1. Records selected for archival preservation and no longer in regular use by The CCG should be transferred to an archival institution, for example a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities.

21.2. Following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, non-active records are required to be transferred no later than 20 years from the creation date of the record, as required by the Public Records Act 1958.

21.3. The SIRO will identify the CCG's Place of Deposit and assist in the transfer of those records identified.

22. RETENTION ARRANGEMENTS

22.1. Detailed guidance on retention periods for a full range of NHS personal health and different types of business and corporate records is provided in Annex D of the Code.

22.2. It is particularly important under 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 CCG and which are enforced by properly trained and authorised staff.

22.3. Archiving of corporate paper documents will be carried out in line with the CCG arrangements in place.

23. APPRAISAL OF RECORDS

23.1. Appraisal refers to the process of determining whether records are worthy of permanent archival preservation. This should be undertaken in consultation with the CCG Managers who have 'records management' responsibilities.

23.2. The retention schedules in Annex D of the Code outline the recommended minimum retention periods for all types of NHS records. The purpose of this 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.

23.3. Appraisal refers to the process of determining whether records are worthy of permanent archival preservation, as certain records created by the CCG may be of historical interest to The National Archives.

23.4. The purpose of the appraisal process is to ensure 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.

23.5. Appraisal should only be undertaken after consultation with the SIRO.

23.6. It is the responsibility of the staff member who is leaving their current post or the organisation, and their Line Manager, to identify as part of the exit procedure specific records that should be retained in line with the Record Retention Schedules. These records should then be transferred securely to the requisite drive and any non-work related records disposed of.

24. RECORD CLOSURE

24.1. 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.

24.2. 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.

24.3. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

24.4. Records should be closed, for example, made inactive and transferred to secondary storage as soon as they have ceased to be in active use other than for reference purposes.

24.5. The CCG has a Records Retention Schedule, which will help staff apply timescales to their records to ensure records are not kept longer than necessary.

25. RECORD DISPOSAL

25.1. The CCG retention/disposal schedule is taken from the retention schedules contained in the Code. The CCG schedule covers all records held by the CCG, including electronic records.

25.2. In the event of any records selected for archival preservation and no longer in regular use by the CCG, these will be transferred as soon as possible to an archival institution (for example a Place of Deposit – see Annex E of the Code) that has adequate storage and public access facilities.

25.3. It is the responsibility of the CCG to ensure that the methods used throughout the destruction process provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Most NHS records are confidential records. All confidential papers will be disposed of by shredding.

25.4. A record of the destruction of records, showing their reference, description and date of destruction will be maintained and preserved by the nominated Records Manager, so that the CCG is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules will constitute the basis of such a record.

25.5. If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act 2000 have been exhausted or the legal process completed.

25.6. Disposal is the implementation of appraisal and review decisions and the term should not be confused with destruction. A review decision may result in the destruction of records but may also result in the transfer of custody of records, or movement of records from one system to another.

25.7. Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records consumes time, space and equipment use, therefore disposal will aid efficiency. Staff members must regularly refer to The CCG's Record Retention Schedule saved within the Information Governance section of the Intranet.

25.8. Unnecessary retention may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Act 1998. If The CCG continues to hold information which we do not have a need to keep, we would be liable to disclose it upon request. The Data Protection Act 1998 also advises that we should not retain personal data longer than is necessary.

25.9. The accounts (mailbox and personal folder) of staff members who have left employment with The CCG will be deleted immediately unless there are extenuating circumstances, for example, an Employment Tribunal claim or litigation case. This will ensure best utilisation of server space, as well as to ensure that records are not held in excess of their retention period. It is the

Line Manager's responsibility to notify the ICT Service Desk of accounts that should not be deleted.

25.10. Staff members must seek specialist advice from the Information Governance team when considering destruction of the organisation's records through a commercial third party.

25.11. Staff members must seek specialist advice from the SIRO when considering off-site storage of the organisation's records with a commercial third party.

25.12. Short-lived documents such as telephone messages, notes on pads, post-its, e-mail messages, etc do not need to be kept as records. If they are business critical they should be transferred to a more formal document which should be saved as a record.

26. MONITORING

26.1 Compliance with this Policy will be monitored via the CCG SIRO, CCG Caldicott Guardian, the Information Governance Senior Manager (CSU), together with independent reviews by both Internal and External Audit on a periodic basis.

26.2 The Information Governance Senior Manager is responsible for the monitoring, revision and updating of this Policy on a 2 yearly basis or sooner if the need arises.

27. EQUALITY IMPACT ASSESSMENT

27.1 This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

27.2 As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

28. ASSOCIATED DOCUMENTS

The following documents will provide additional information:

- Information Governance Strategy
- Information Governance Policy
- Confidentiality and Data Security Policy
- Freedom of Information Policy
- The suite of ICT security policies

Appendix A - Records Retention Schedule

Records Management: NHS Code of Practice is available at:

https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

The Records Management: NHS Code of Practice *Annex D2: Business and Corporate (Non-Health) Records Retention Schedule* (pages 70 to 105) is available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf

These retention schedule details a minimum retention period for each type of non-health record. Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years.

The following types of record are covered by the retention schedules (regardless of the media on which they are held, including paper, electronic, images and sound):

- administrative records (including personnel, estates, financial and accounting
- records, and notes associated with complaint handling)
- photographs, slides and other images (non-clinical)
- microform (i.e. microfiche/microfilm)
- audio and video tapes, cassettes, CD-ROMs, etc
- e-mails
- computerised records; and
- scanned documents

The schedule is split into the following types of records:

- Administrative (corporate and organisation)
- Biomedical Engineering
- Estates/engineering
- Financial

- IM & T
- Other
- Personnel/human resources
- Purchasing/supplies

Record Retention

Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the Data Protection Act 1998 (DPA) and/or the Freedom of Information Act 2000. Moreover, compliance with these acts means that, for example, personal data must not be kept longer than is necessary for the purposes for which it was collected (Principle 5 of the DPA).

Records should only be destroyed as per the CCG's Policy. It can be a personal criminal offence to destroy requested information under either the Data Protection Act (Section 61) or the Freedom of Information Act (Section 77). Therefore, the CCG needs to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures.

The Code of Practice on Records Management, issued under Section 46 of the Freedom of Information Act 2000, requires that records disposal 'is undertaken in accordance with clearly established policies that have been formally adopted'. The Records Retention Schedule is a key component of the CCG's information compliance and allows it to standardise its approach to retention and disposal.

The recommended retention periods shown on the Records Retention Schedule apply to the official or master copy of the records. Any duplicates or local copies made for working purposes should be kept for as short a period of time as possible. Duplication should be avoided unless absolutely necessary. It should be clear who is responsible for retaining the master version of a record and copies should be clearly marked as such to avoid confusion.