Bolton Clinical Commissioning Group

Records Management Policy and Procedure

Policy Number	**IG005**
Target Audience	**CCG**
Approving Committee	**CCG Chief Officer**
Date Approved	**March 2020**
Last Review Date	**January 2020**
Next Review Date	**January 2022**
Policy Author	**IG Team**
Version Number	**V6.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Bolton Clinical Commissioning Group

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1.1	January 2015	A Hughes	Change of Overall Responsibility
2.0	January 2017	IG Team	Changes from CSU to GMSS. Addition of section 5. NHS Numbers. Reference to Records Management Code of Practice for Health and Social Care 2016.
2.0	February 2017	IM&T Ops Board	Approved.
3.0	January 2018	IG Team	Review to incorporate the GDPR legislation
4.0	January 2018	IM&T Ops Board	Approved.
5.0	February 2018	CCG Chief Officer	Approved.
5.1	December 2019	IG Team	Reviewed and updated
6.0	February 2020	IG Board	Approved
6.1	March 2020	CCG Chief Officer	Approved.

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1. Introduction and Aims

The purpose of this document is to provide guidance to all Bolton Clinical Commissioning Group (henceforth referred to as "the CCG") staff on the management of records.

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 or destruction.

Records are a valuable resource due to information they contain. High quality information underpins the delivery of high quality evidence based service and care. Furthermore this information has most value when it is accurate, up-to-date and accessible when it is needed.

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

All organisations need to keep records of its activities, patients, staff and the public would rightly expect that the CCG maintains records on its activities and decisions that affect their service and experience.

The CCG has adopted this Records Management Policy and Procedure document and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- 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.

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

This policy is a key component of the CCG's overall Information Governance framework and should be considered alongside the other Information Governance policies, and other relevant CCG policies such as the Data Quality Procedure.

The aims of this policy are to ensure:

- **Accountability** - records are adequate to account fully and transparently for all business actions and decisions, in particular to:

- protect legal and other rights of staff or those affected by those actions;
- facilitate audit or examination;
- provide credible and authoritative evidence.

- **Availability** - to ensure events or activities can be followed through and form a reconstruction as necessary;

- **Accessibility** – can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with their initial use, with the current version being identified where multiple versions exist;

- **Interpretation** - the context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and were appropriate, how the record is related to other records;

- **Quality** – records can be trustworthy - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;

- **Maintenance through time** - that the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

- **Security** – records are secure from unauthorised or inadvertent alteration or erasure, access and disclosure are properly controlled and there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required;

- **Retention and disposal** – records are retained and disposed (or destroyed) of appropriately, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value;

- **Staff are trained** – so that all staff are made aware of their responsibilities regarding records management.

The Records Management Code of Practice for Health and Social Care 2016 that was published by the Information Governance Alliance in July 2016 acts as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice and sets out a schedule of minimum retention periods for many types of record.

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 a permanent place of deposit, such as The National Archives.

2. Background

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

- Public Records Act 1958;
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act 2000;
- Records Management Code of Practice for Health and Social Care 2016;
- NHS Information Governance: Guidance on Legal and Professional Obligations;
- EU General Data Protection Regulation 2016 (GDPR).

a. The Public Records Act 1958 - an Act of Parliament to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.
b. The Data Protection Act 2018 - an Act of Parliament which regulates the processing of personal data relating to living individuals, including the obtaining, holding, use or disclosure of such information. Access to the health records of living patients is governed by this Act.
c. The Freedom of Information Act 2000 - an Act of Parliament that makes provision for the disclosure of information held by public authorities or by persons providing services for them. The Lord Chancellor's Code of Practice on the management of records is issued under section 46 of this Act.
d. The Access to Health Records Act 1990 - an Act of Parliament that regulates access to the health records of a deceased person.
e. The Regulation of Investigatory Powers Act 2000 which permits the 'interception' of communications, such interception must be proportionate to the needs of the organisation, society and the users of the communication system.
f. The Records Management Code of Practice for Health and Social Care 2016 was published by the Information Governance Alliance in July 2016. It is a best practice guide for 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.
g. 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.
h. The GDPR regulates the processing of personal data in all EU member states. It is implemented in the UK by the Data Protection Act 2018 (DPA) which complements the GDPR. The two pieces of legislation must be read together.

Failure to comply with the GDPR or DPA could result in reputational damage to the CCG and carries significant financial penalties imposed by the Information

Commissioner's Office (ICO). Furthermore, individuals can be prosecuted for knowingly or recklessly disclosing, procuring or obtaining personal data. This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

3. Scope

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

This policy applies to all records of the CCG held in any format (e.g. paper, electronic, audio visual). These include (but are not limited to) records relating to the administration of either CCG, personnel, finance, estates, complaints, legal, commissioning, continuing health care funding, individual funding.

This list is not exhaustive.

4. Definitions

Personal Data' is defined as: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (Article 4(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 (or destruction) of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record. The key components of records management are:

- creation / receipt;
- distribution;
- use (access and disclosure);
- maintenance (including tracking of record movements);
- appraisal and disposition.

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.

National Archives – The National Archives is a centre of expertise in creating, managing and preserving official information and is the UK government's official archive. They give detailed guidance to government departments and the public sector, including the NHS, on information management and advise others about the care of historical archives.

Appraisal – the process of evaluating which records should be kept, and for how long; to meet the needs of the CCG, the requirements of government accountability and the expectations of researchers and other users of records. This also includes consideration as to whether records have archival value.

A **document** is any piece of written or recorded information in any form, produced or received by an organisation or person. It may contain, for example, details of a business decision and will therefore need to become part of a formal record, or a document may be of very short- term value and will not need to be retained.

A **record** is anything that contains information (in any media or format) created or received and which forms permanent evidence of a business activity and which needs to be retained as evidence of such activity. A document becomes a record when it has been finalised and becomes part of the CCGs' corporate information. At this point, the record should not be amended without clearly indicating that changes have been made and creating an audit trail.

Corporate records - records other than health records that are of, or relating to, the CCGs' business activities covering all the functions processes, activities and transactions of the CCG.

Corporate records may be held in any format (e.g. paper or electronic) and includes any records stored on the CCG's networks or CCG issued or approved equipment/devices.

Examples of corporate records include (but are not limited to) meeting papers, reports of any description, tender documents, evaluation reports, ledgers, contracts, agreements, healthcare funding, strategies, policies and other administrative documents.

Corporate records may include service user information. Corporate records may include clinical or healthcare information which is used to support the funding or provision of care, but is not used directly for the primary care of the patient. (Records used directly for the primary care of the patient are classed as clinical records, and usually held by provider organisations.)

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.

Information is a corporate asset. The CCG records are important sources of administrative, evidential and historical information. They are vital to the CCG to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

5. Roles and Responsibilities

Chief Officer
Overall responsibility for the Records Management Policy and Procedure lies with the Chief Officer who has overall responsibility for managing the development and implementation of the records management within the CCG.

Caldicott Guardian
The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. They will support work to enable information sharing where it is appropriate to share, and advice on possible choices for meeting compliance when processing information.

Data Protection Officer (DPO)
The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits (these may be delegated to the Information Governance Manager). In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Senior Information Risk Owner (SIRO)
Take ownership of the organisation's Information Risk policy. Acts as advocate for information risk on the board. Drive culture change with regard to information risks in a realistic and effective manner. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.

Information Asset Owners (IAOs)
IAOs under the responsibility of the SIRO 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;
- ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
- be responsible for the Information Asset assigned to them;
- ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a Right to Access Request;
- ensure that personal data held in the Information Asset is maintained in line with the CCGs Record Management Policy and Procedure, 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.

Information Governance (IG) Manager
The Information Governance (IG) Manager will provide IG and record management advice and guidance in line with contractual obligations and support CCG management where applicable. In addition the IG Manager will investigate any personal data protection breach arising record management issues and report and seek guidance from the DPO.

Line Managers
Line managers must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is, they must have an up-to-date knowledge of the laws and guidelines concerning confidentiality and data protection.

All Staff
All staff, and those working on behalf of the organisation, are expected to follow this policy and its procedures. This relates to all staff who create and use / process records as part of the delivery of CCG business. This covers records in all formats (paper and electronic), both active and inactive.

Staff will receive instruction and direction regarding the policy from a number of sources:

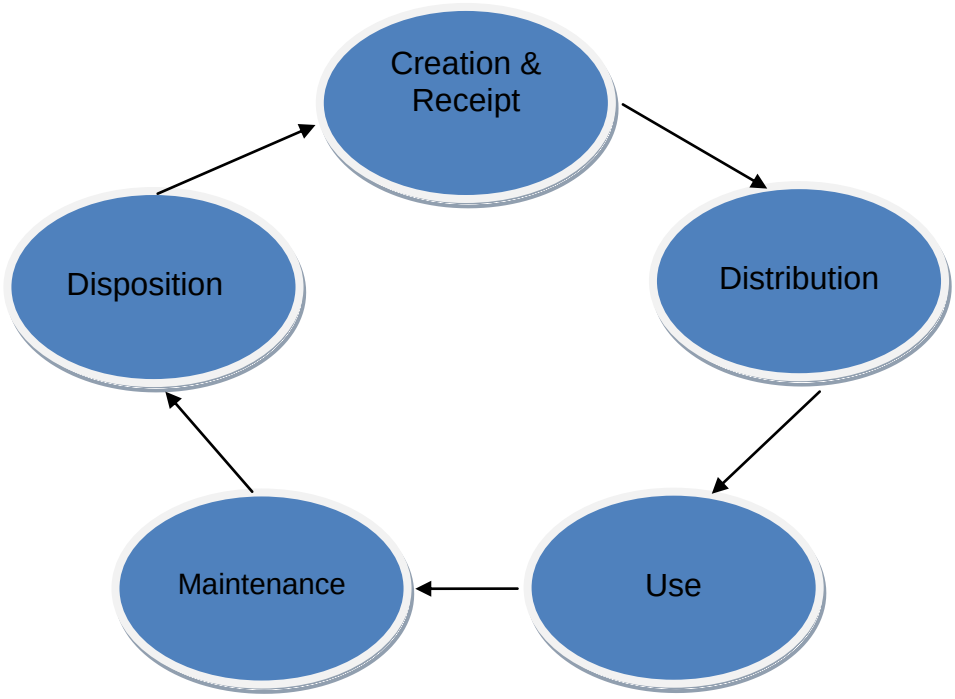
- policy/strategy and procedure manuals;
- line manager;
- other communication methods (e.g. team brief/team meetings); and
- staff Intranet.

All staff are mandated to undertake mandatory Information Governance training. The training is required to be undertaken on an annual basis in accordance with the Data Security and Protection Toolkit.

Information Governance (IG) Board
The CCG's IG Board will be responsible for ensuring that this policy and procedure is implemented, through the Records Management Policy and Procedure, and that the records management system and processes are developed, co-ordinated and monitored.

6. Records and Information Life Cycle Management

Records and Information Management plays an integral role within the CCG as it underpins effective information sharing within the organisation and externally to patients, staff, the public 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. The diagram shows 5 key steps in the Records Life Cycle.



Stage 1: Creation and Receipt
This part of the life cycle is the start, when pen is put to paper, an entry is made 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 and it is complete and accurate.

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 for. Records are distributed when photocopied, printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used / processed.

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 being stored. Even though they are not used on a day to day basis, they will be kept for 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 retained for 20 years and sent to The National Archives, where they will be kept for the future of both organisations and may never be destroyed. This is the final phase of a records lifecycle.

7. Register of Records

The CCG will use the Information Asset Register to monitor and understand the collections of records and information the CCG holds.

The register will include:

- the type of records currently held;
- the format in which the records are held;
- the record keeping systems currently in use;
- the retention period in accordance with the retention schedule published by the Information Governance Alliance, Records Management Code of Practice for Health and Social Care 2016.

Each department will be responsible for the integrity of the information provided within the register and will review the register annually with the support of the IG Manager. Who, along with the IAO and / or department manager will assess how effective the record keeping system is and identify and implement any improvements which need to be made.

8. Record Creation

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

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.

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.

Each record should be given a unique name / number. Where possible the name should be meaningful and closely reflect the record content. Similarly structured names should be given to records which are linked.

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

- file reference;
- file title;
- if appropriate protective marking i.e. Official, Official - Sensitive;
- if possible an anticipated disposal date and what action to take;
- where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed;

- all filling systems to be documented and kept up to date.

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.

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

For checklist on how to create a Record refer to Appendix 1, Checklist; Creating a Record.

9. Record Naming

Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the CCG to assist in good management of records.

Staff should seek guidance from line / department manager before naming any documents, this is particular important where they are records that contain personal data.

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

10. Record Quality

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

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).

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.

Quality Checking

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

- ensure the correct retention period has been input onto the document which confirms the right retention / destruction will have been calculated;
- ensure all names are spelt correctly and in the correct format;
- ensure the unique identifiers are correct and in the right format;
- check the barcode number is correct (if relevant);
- the inventory should be checked for all other possible errors.

The CCG have implemented a Data Quality Procedure which provides further detail and should be used alongside this policy.

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

11. Record Tracking, Storage and Maintenance

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.

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

Tracking mechanisms should record the following (minimum) information:

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

- the date of the information returned (if applicable).

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.

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

Records containing confidential or personal data must be protected from unauthorised access, inadvertent alteration or erasure, at all times.

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

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.

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.

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

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.

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.

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.

12. Record Transportation

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

- records must only be taken off–site / removed from a department when absolutely necessary. To ensure staff are aware of the

location of the record a log of what information is being moved and why, and when applicable, details of where and to whom it is being taken, by whom and how, should also be recorded;

- records should not be left unattended. In the event that they are left unattended, every precaution must be taken to keep them secure an inaccessible to unauthorised persons;
- records being transported should always be kept out of sight;
- records should not be left unattended in cars;
- records 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 which need to be dispatched externally must be sent by secure post or approved Courier –
    - when using an internal courier services, confidential records must be transported in a sealed container / envelope / transit bag and labelled appropriately (refer to section 20). The recipient's details in full must be clearly visible. A return address should be visible;
    - courier services for records must only be obtained from an organisation that has signed up to the national agreement for public sector bodies, or that has provided adequate security assurances set out in a written contract with the CCG;
    - an up to date list of courier companies which have signed up to the national agreement for public sector bodies can be viewed on the Crown Commercial services website (http://ccsagreements.cabinetoffice.gov.uk).
- where secure post is required –
    - a tracked and trace service should be used, for example Royal Mail Special Delivery. Recorded Delivery does not meet Department of Health standards as the post is not tracked throughout the whole journey;
    - a plain, robust envelope or packet must be used and must not be overfilled;
    - if re-using envelopes ensure that the recipient's and senders details are clear and the content is not visible.
- where hand carried by staff, records must be contained in a robust folder, wallet, or envelope, to safeguard against such things being accidentally viewed by unauthorised persons, accidental dropping or dispersing of documents;
- when appropriate, ensure that records are returned back on site as soon as possible and record that the information has been returned.

Appendix 3 – Transportation of information log sheet. This should be used when transporting any records from one place / organisation / department to another.

Follow the process on Appendix 5 to ensure confidential records are posted securely.

13. Lost / Missing Records

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

unavailable.

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

The loss of records constitutes a reportable incident and should be reported in accordance with the CCG's Data Security & Protection Breaches / Incident Reporting Policy where an investigation will commence.

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

More information can be found at Appendix 4.

14. Paper Records to Electronic (Scanning)

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

Where this is proposed, the evidential value of the record must be protected in accordance with British Standards 1008 to protect legal admissibility of scanned paper records. In some cases it might be desirable to hold original ink signed records. This is permissible, although scanning such documents is preferable so long as the scanned version is legally admissible.

In the event that scanned records do not meet the British Standard (10008) for "Legal Admissibility of Electronic Records", the original paper records must be retained in accordance with normal retention and disposal schedules, as outlined in section 17 of this policy.

Where documents have been scanned and are no longer in active use, consideration should be given to storing the original documents in the CCGs' offsite records storage and archiving system. See sections 16 and 17 of this policy.

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. Record Disclosure

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 IG Manager.

If required the Caldicott Guardian and DPO will be consulted where there is any proposed disclosure of confidential patient information, particularly where this disclosure does not fall under any provision.

16. Records no longer required for current business use

Appraisal refers to the process of determining whether records are worthy of additional retention or permanent archival preservation. This should occur when records (paper or electronic) are not required for current business use.

The appraisal process will indicate:

- how long they should be retained for, in accordance with the retention schedule detailed in the Records Management Code of Practice for Health and Social Care 2016;
- the destruction due date will also be calculated - in accordance with this retention schedule;
- whether the records should be destroyed when they reach their minimum retention period and destruction due date;
- whether the records need to be retained for a longer period (see Section 18);
- whether they are worthy of archival preservation.

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.

When paper records are no longer required for current business and they have been appraised as above, but they have not reached the minimum retention period, they should be archived – either to an on-site storage area or to the CCGs' offsite records storage facility.

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.

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.

17. Retention Schedules, Record Disposal and Record Destruction

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 CCG's business functions.

The appraisal process must be followed, as per section 16, before any records are disposed of.

The CCG has adopted the retention periods set out in the Records Management Code of Practice for Health and Social Care 2016. These retention schedules outline the recommended minimum retention period for records held by Health and Social Care organisations. The destruction advice contained within this document should also be adhered to.

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

The destruction of records is an irreversible act and must be clearly documented. All records identified for disposal will be destroyed under confidential conditions. A decision for destruction of records must be made by a senior manager who has knowledge of the relevant business area to which the records relate, in conjunction with the IG Manager. Destruction of records must not take place without recorded agreement from the CCG's IG Board.

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.

Where there are record types held by the CCG that are not listed in the detailed retention schedules advice should be sought from the IG Manager. Attention will be paid to other similar types of records.

The decision regarding retention and disposal of record types not listed in the Retention and Disposal Schedules will be made by the CCG's IG Board. A Retention and Disposal Schedule log of such local approvals will be maintained by the IG Manager.

In the event that records need to be kept for longer than the minimum retention period due to ongoing administrative need, this should be referred to the IG Manager in the first instance and then to the IG Board. If it is approved that the records should be retained for a period longer than the minimum (provided that this does not total a period of 30 years or more from creation), an internal retention schedule will be developed accordingly. (Records may not be retained for more than 30 years without the approval of the National Archives).

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

A log of all record disposals / destructions should be retained within the Department.

Please see Appendix 7 - Retention Schedule for Bolton CCG for further details.

18. Records involved in Investigations, Inquiries, Litigation and Legal Holds

A Legal Hold, which may also be referred as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation or inquiry. The CCG has a duty to preserve relevant information when a lawsuit, investigation or inquiry is reasonably anticipated. Staff who have been notified of a Litigation, Investigation or Inquiry or have reasonable foresight of a future Litigation, Investigation or Inquiry must notify their line manager / department head immediately who will seek guidance from the IG Manager if required.

This may result in records being held beyond their identified retention period.

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

The Legal Hold decision will be determined by the Senior Management, in this case the CCG's Executive Team.

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.

19. Record Closure

Before records are classed as 'closed' i.e. made inactive and transferred to secondary storage, ceased to be in active use other than for reference purposes they should be appraised. See section 14.

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

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

20. Classification of NHS Information within the CCG

The aim of the Classification Marking of NHS Information is to demonstrate 'good practice' in marking the records for which the CCG are responsible.

The CCG holds a wide range of information and has a responsibility to manage all information in its care such that risk is minimised; to ensure business continuity and to protect the rights of individuals.

As the CCG is a public body and as such, classification must follow that laid down by Government. ALL information the CCG collects, stores, processes, generates or shares to deliver services and conduct business has fundamental value and requires an appropriate degree of protection.

EVERYONE who works at the CCG has a duty of confidentiality and a responsibility to safeguard any NHS information or data that they access, irrespective of whether it is marked or not. Government Security Classifications (updated May 2018) have been implemented to assist organisations in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect. The levels are:

> OFFICIAL - This is the default classification for all NHS documentation. Most organisations operate almost exclusively at this level. ALL routine public sector business, operations and services should be treated as OFFICIAL. There are subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable
>
> OFFICIAL – SENSITIVE: COMMERCIAL Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the organisation or a commercial partner if improperly accessed.
> Or
> OFFICIAL – SENSITIVE: PERSONAL Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Such documents / records should be marked with the caveat 'OFFICIAL-SENSITIVE: COMMERICAL or PERSONAL' in capitals at the top and bottom of the page. In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

NHS Confidential
The CCG is working to existing IG guidance and where necessary marking documents as either CONFIDENTIAL or COMMERCIALLY SENSITIVE. The CCG will be working to implement the NHS England Protective Marking Scheme. However, information received from an NHS organisation using the NHS England Protective Marking Scheme may be marked as OFFICIAL – SENSITIVE (depending on its type) which should then be treated as CONFIDENTIAL (or COMMERCIALLY SENSITIVE).

How to handle and store OFFICIAL / CONFIDENTIAL information;
EVERYONE is responsible to handle OFFICIAL / CONFIDENTIAL information with care by:

- Applying clear desk policy
- Information sharing with the right people

- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses
- Locking your screen before leaving the computer
- Using discretion when discussing information out of the office

Please refer to Appendix 8 for further information on the marking of documents and the Government Security Classifications.

21. Requests for Access to Information

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 Right of Access request, Freedom of Information request and correspondence on how a decision was made. The Data Protection Act 2018 allows individuals to find out what personal data is held about them, known as a Right of Access Request. The Freedom of Information Act 2000 gives the public the right of access to information held by public authorities.

Right of Access Request
Individuals have the right under Article 15 of the GDPR to request to see or be provided a copy of information that an organisation holds about them. The CCG has a Right of Access / Subject Access Requests Procedure which explains the process that data subjects should follow if they wish to obtain this information.

Freedom of Information Act 2000
Any information that belongs to the CCG may be subject to disclosure under the Freedom of Information Act 2000. From the 1 January 2005, the Freedom of Information Act 2000 allows anyone, anywhere to ask for information held by the CCG to be disclosed (subject to limited exemptions). Further information is available in the Freedom of Information Act 2000 Policy.

22. Training Requirements

All staff who create or use / process records, must receive local induction training in the records management system being used in the work area.

Local induction will provide staff with an understanding of;

- what should be included in records and how it should be recorded;
- how to identify and correct errors;
- how records will be used – so that will understand why timeliness, accuracy and completeness are so important).

Information Governance training must be undertaken on an annual basis. CCG staff are mandated to undertake the mandatory Information Governance annually. Records management features in this training. All CCG Staff will be made aware of their responsibilities for record-keeping and record management.

Where staff may take on a specific Information Governance roles within the CCG e.g. Records Manager, additional Information Governance training will be required. For further guidance refer to the CCG's IG Training Needs and Analysis (TNA) Document.

Where necessary the CCG can request ad-hoc face to face training sessions relating to Records Management this will be co-ordinated by the IG Manager.

23. Awareness

The CCGs IG Board will be responsible for ensuring that this policy is implemented, and that the records management system and processes are developed, co-ordinated and monitored.

This policy and procedure will be placed on the CCG's website for all staff to access.

A notice will be sent to all staff notifying them of the release of this document.

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, team meetings; and staff Intranet.

24. Monitoring and Review

The effectiveness of this policy will be monitored by analysis of incident reports and annual department reviews.

In compliance with Data Security and Protection Toolkit requirements, this policy will be reviewed biennially 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;

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

25. Legislation

- Public Records Act 1958
- Data Protection Act 2018
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act 2000

- Records Management Code of Practice for Health and Social Care 2016
- NHS Information Governance: Guidance on Legal and Professional Obligations
- EU General Data Protection Regulation 2016 (GDPR)

The CCG will also take action to comply with any new legislation affecting records management as it arises.

26. Other relevant Procedural Documents

- Information Governance Framework
- Information Governance Policy
- Data Protection & Confidentiality Policy
- Confidentiality Audit Policy
- Data Security & Protection Breaches / Incident Reporting Policy and Procedure
- Secure Transfer of Information Policy
- Acceptable Use Policy
- Information Risk Policy
- Information Security Policy
- Right of Access Procedure
- Data Quality Procedure

This list is not exhaustive.

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;
- 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.

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

Examples of good record keeping below:

- 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

Appendix 3 – Transportation of information log sheet

Address for Reply
Direct Telephone Number:
Direct Fax Number:
E-Mail Address:

Description of information to be transported / list of records, folders or disc titles:
……
……
……
……
……

Number of records / folders / discs / items:
……

To be transported by:
Name (Print):
……

Organisation and Designation:
……

Contact Number:
……

To be received by:
Name (Print):
……

Designation:
……

Organisation name and Address:
……

(including postcode)
……

Method of transportation:
……

Estimated duration of transit:
……

Goods received by Courier/Organisation/Department:

Date: …… Time: …….....

Print Name: ……..

Signature: .....

Name of CCG employee handing over the information:
…….....

Designation:
……

Contact Number:
……

Signature: Time and Date:
……

Goods received by: Date: ……..... Time:..……

Print Name: …….Signature:..……

The receiver (courier/organisation/department etc.) will immediately contact the CCG using the above contact details to confirm that the information has been successfully delivered. A copy of this form may be provided to the receiver on request.

Appendix 4 – Procedure for handling Missing / Lost Records

Lost records

- The member of staff should report the missing record to his/her supervisor/ manager as soon as possible
- The supervisor/manager should ensure that a thorough search takes place, using tracking methods, including initiating a search at the base where the record should be kept
- The event must be entered in the Missing Record Log and in addition an Incident Form completed
- A temporary record should be created, clearly marked as a temporary record, populated with all relevant information available for that data subject/individual. A temporary record should be set up and tracked on the relevant systems for the Department
- When original records are located the missing record log should be updated with details of where/how the original was located, and the two folders should be merged

Unavailable / Missing records

- A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment
- An entry should be made in the Missing Records Log
- A temporary record should be created, as described in the above section
- If an appointment is deferred (i.e. individual has a meeting/appointment with HR) as the record is not available this should also be recorded in the Missing Record Log

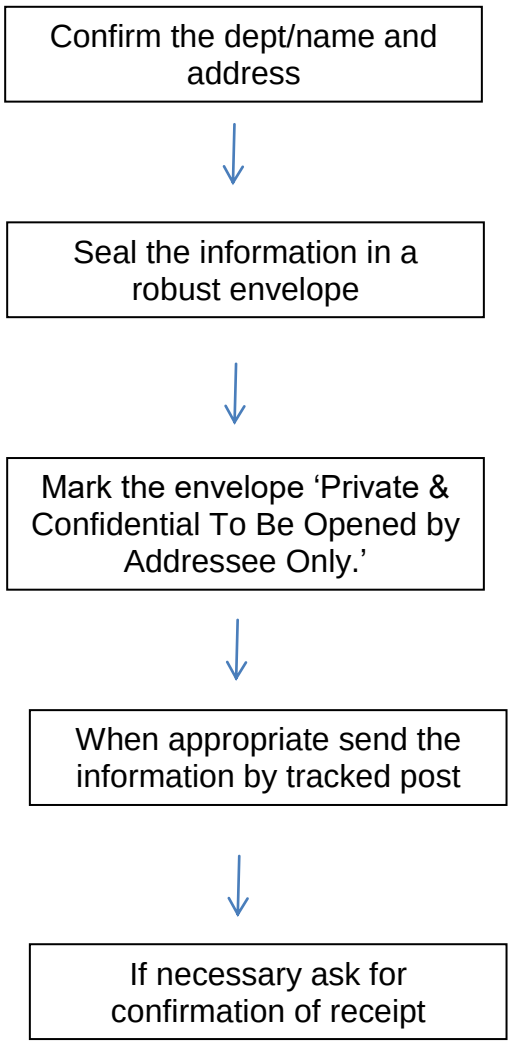
Reasons for records being unavailable may include:

- Record needed for another appointment/meeting
- Record with another Team/ Department
- Record not tracked
- Misfiled
- Wrong record/volume/temp record(s) sent

Appendix 5 – Sending Information via Postal Service

A reminder that a tracked and trace service should be used, for example Royal Mail Special Delivery. Recorded Delivery does not meet Department of Health standards as the post is not tracked throughout the whole journey.

Guidance for sharing Personal and / or Confidential information by POST



Appendix 6 – Full Guidance on Retention Schedules

Full Guidance and retention schedules can be found here:

https://digital.nhs.uk/codes-of-practice-handling-information

Appendix 7 – Retention Schedule for Bolton CCG

The following record types that are applicable to the CCG have been extracted from the Records Management Code of Practice for Health and Social Care 2016 (Appendix 3).

Staff should consult the IG Manager if the records they process do not appear in the list below.

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
Care Records with standard retention periods	Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Care Records with standard retention periods	Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Care Records with Non-Standard Retention Periods	Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care. The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.
Event & Transaction Records	Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	http://www.hscic.gov.uk/media/15729/DARS-Data-Sharing-Agreement/pdf/Data_Sharing_Agreement_2015v2%28restricted_editing%29.pdf

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
Event & Transaction Records	Equipment maintenance logs	Decommissioning of the equipment	11 years	Review and consider transfer to a Place of Deposit	
Event & Transaction Records	Requests for funding for care not accepted	Date of rejection	2 years as an ephemeral record	Review and if no longer needed destroy	
Corporate Governance	Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Corporate Governance	Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Corporate Governance	Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Committees/ Groups / Sub-committees not listed in the scheme of	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
	delegation				
Corporate Governance	Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Public Records Act 1958. If records are not excluded by such an instrument they must either be transferred to a place of deposit as a public record or destroyed 20 years after the record has been closed.
Corporate Governance	Incidents (serious)	Date of Incident	20 Years	Review and consider transfer to a Place of Deposit	
Corporate Governance	Incidents (not serious)	Date of Incident	10 Years	Review and if no longer needed destroy	
Corporate Governance	Non-Clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed destroy	
Corporate Governance	Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	
Corporate Governance	Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to a Place of Deposit	

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
Communications	Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Communications	Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Communications	Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Communications	Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Communications	Website	Creation	6 years	Review and consider transfer to a Place of Deposit	
Staff Records & Occupational Health	Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves	Review and if no longer needed destroy	

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
			whichever is sooner		
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file.	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Records & Occupational Health	Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see page 36 for an example of a Staff Record Summary used by an organisation.
Staff Records & Occupational Health	Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
Staff Records & Occupational Health	Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer 2 Statutory and mandatory training records - to be kept for ten years after training completed 3Other training records - keep for six years after training completed.
Procurement	Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Procurement	Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
Estates	Equipment monitoring and testing and maintenance work where asbestos is a factor	Completion of monitoring or test	40 years	Review and if no longer needed destroy	
Estates	Leases	Termination of lease	12 years	Review and if no longer needed destroy	
Finance	Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Finance	Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	
Finance	Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Expenses	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred	Should be transferred to a place of deposit as soon as practically possible

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
				with the board papers	
Finance	Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Finance	Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Finance	Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Finance	Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Legal, Complaints & information Rights	Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Freedom of Information (FOI) requests and responses and any associated	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
	correspondence				
Legal, Complaints & information Rights	FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Industrial relations including tribunal case records	Close of financial year	10 Years	Review and consider transfer to a Place of Deposit	Some organisations may record these as part of the staff record but in most cases they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Legal, Complaints & information Rights	Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit	
Legal, Complaints & information Rights	Patents / trademarks / copyright / intellectual property-	End of lifetime of patent or termination of licence/action	Lifetime of patent or 6 years from end of licence /action	Review and consider transfer to Place of Deposit	
Legal, Complaints & information Rights	Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Subject Access Requests (SAR) and disclosure correspondence	Closure of SAR	3 Years	Review and if no longer needed destroy	

Broad Descriptor	Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
Legal, Complaints & information Rights	Subject access requests where there has been a subsequent appeal	Closure of appeal	6 Years	Review and if no longer needed destroy	

Appendix 8 – Classification of NHS Information – Marking Guidance for the CCG

The Government Security Classifications are:

OFFICIAL
Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. There are subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

SECRET
Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well-resourced and determined threat actors and highly serious organised crime groups.

TOP SECRET
Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

This simplified procedure is intended to make it easier and more efficient for information to be handled and protected. The new procedure places greater emphasis on individuals taking personal responsibility for data they handle.

Things to remember about OFFICIAL information:

1. Ordinarily OFFICIAL information does not need to be marked for non-confidential information.
2. A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but should have additional measures applied in the form of OFFICIAL-SENSITIVE.
3. This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic records.
4. In additional to the marking of OFFICIAL-SENSITIVE further detail is required due to the content of the document or record, i.e.:

   OFFICIAL – SENSITIVE: COMMERCIAL
   Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the organisation or a commercial partner if improperly accessed.

   Or

   OFFICIAL – SENSITIVE: PERSONAL
   Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.
   Such documents/records should be marked with the caveat ‘OFFICIAL-SENSITIVE: COMMERICAL or PERSONAL’ in capitals at the top and bottom

of the page. In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

Table 1 – Descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL		
Category	Definition	Marking
Appointments	Concerning actual or potential appointments not yet announced	OFFICIAL SENSITIVE: COMMERCIAL
Barred	Where • there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or • disclosure would constitute a contempt of Court (information the subject of a court order)	OFFICIAL SENSITIVE: COMMERCIAL
Board	Documents for consideration by an organisation's Board of Directors, initially, in private (Note: This category is not appropriate to a document that could be categorised in some other way	OFFICIAL SENSITIVE: COMMERCIAL
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs	OFFICIAL SENSITIVE: COMMERCIAL
Contracts	Concerning tenders under consideration and the terms of tenders accepted	OFFICIAL SENSITIVE: COMMERCIAL
For Publication	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date	OFFICIAL SENSITIVE: COMMERCIAL
Management	Concerning policy and planning affecting the interests of groups of staff (Note: Likely to be exempt only in respect of some health and safety issues)	OFFICIAL SENSITIVE: COMMERCIAL
Patient Information	Concerning identifiable information about patients	OFFICIAL SENSITIVE: PERSONAL
Personal	Concerning matters personal to the sender and/or recipient	OFFICIAL SENSITIVE: PERSONAL
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published)	OFFICIAL SENSITIVE: COMMERCIAL

Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.	OFFICIAL SENSITIVE: COMMERCIAL
Staff	Concerning identifiable information about staff	OFFICIAL SENSITIVE: PERSONAL