NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG)

Records Management and Lifecycle Policy 2020 - 2022

Ratification Process

Lead Author:	Corporate Services Manager and Information Governance Lead
Reviewed by:	Information Governance, Business Intelligence and IM&T Steering Group
Approved by:	Information Governance, Business Intelligence and IM&T Steering Group – 15th October 2020
Ratified by:	Integrated Performance and Assurance Committee (IPAC)
Date ratified:	24th November 2020
Version:	2.1
Review date:	September 2022 (or earlier if significant change to local or national requirements)
Valid on:	24th November 2020

Document Control Sheet

Development and Consultation	Policy developed by the CCG IG Lead/DPO following GDPR/DPA 2018 in consultation with the IG, BI & IM&T Steering Group and endorsed by the Clinical Executive Committee (superseded by the Integrated Performance and Assurance Committee) and CCG Governing Body.
Dissemination	This Policy will be promoted to all staff via the weekly staff newsletter and uploaded to the CCG's website.
Implementation	The SIRO is responsible for monitoring the application of the policy by ensuring that: • The Policy is brought to the attention of all employees. • Managers are aware of their responsibilities for ensuring that staff under their control implement the Policy. • Appropriate training and guidance is provided to staff. • Corporate business processes support the implementation of the Policy.
Training	Training will be undertaken as part of the CCG's ongoing processes using eLearning for Healthcare modules and bespoke face to face training.
Audit	Implementation of the Policy will be monitored on a regular basis.
Review	This policy will be reviewed biennially or earlier if there are changes in procedures or legislation.
Links with other Guidance	The Policy should be read in conjunction with: • CCG Code of Conduct for Confidentiality • CCG Information Security for Staff Policy • CCG Safe Haven Policy • CCG IG Forensic Readiness Policy • CCG Freedom of Information Policy • CCG Disciplinary Policy and Procedure • CCG Ways of Working Policy • NEL CSU Registration Authority Policy & Procedure • Cambridgeshire and Peterborough Health and Social Care Information Sharing Framework (hosted by Cambridgeshire County Council) • The Good Practice Guidelines for GP electronic patient records (V4; 2011) • Records Management Code of Practice for Health and Social Care 2016
Equality and Diversity	The OD & HR Advisor (Equality and Diversity) has reviewed the Rapid Equality & Diversity Impact assessment and concluded that the Policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were identified.

Revisions

Version	Page / Para No	Description of Change(s)	Date approved
1.0	All	Development of new policy for GDPR / Data Protection legislation compliance	September 2018
2.0	All	Biennial review and update to align Policy with the CCG's new ways of working and include a section and appendix on the CCG's Incident Records Retention Strategy.	October 2020
2.1	Appendix 8 - Disposal of Unwanted Equipment and Information (Section on Destruction of Paper Waste).	Note added outlining the CCG's process for staff to retrieve documents erroneously placed in the blue confidential waste bins.	September 2021

Contents

1. Introduction

1.1 The purpose of this document is to provide guidance to all Cambridgeshire and Peterborough Clinical Commissioning Group (henceforth referred to as "the CCG") staff on Records Management. This policy was adopted from the NHS England Policy of the same name.

1.2 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal. The CCG has a statutory obligation to maintain accurate records of its activities and public records under the terms of the Public Records Acts 1958 and 1967.

1.3 Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care 2016 replaced the Records Management: NHS Code of Practice published by the Department of Health. This guide sets out 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.

1.4 The implementation of the General Data Protection Regulation Protection (GDPR) requires better records management. Organisations need to know what personal data they hold, to be able to tell individuals how long they will keep it for, to be able to access it when they need to, and to keep it securely. This Records Management Policy and Procedure document aids compliance with GDPR and UK Data Protection Act 2018.

"Data concerning health" is defined by the GDPR as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status." 2 Mar 2018.

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

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

1.7 The Policy will support continued development of a robust records management framework including a complete Information Asset Register.

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

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards;

- reduced costs.

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

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

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

2. Aims of a Records Management System

2.1 The aims of the Records Management System are to ensure that records are:

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

3. Scope

3.1 This policy and procedure 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.

3.2 This guidance relates to all clinical and non-clinical records held in any format by the CCG. A record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees, including:

- patient health records, including those concerning all specialties, but excluding GP medical records (Guidance for GPs set out in HSC 1998/217) and includes private patients seen on NHS premises;
- administrative records (including e.g. personnel, estates, financial and accounting records: litigation and records associated with complaints including notes associated with complaint-handling);
- any type of audio and videotapes, cassettes and CD-ROMs;
- computer databases, output, and disks, and all other electronic records;
- photographs, slides and other images
- scanned documents;
- any portable media containing information;
- material intended for short term or transitory use, including notes and "spare copies" of documents;
- meeting papers, agendas, formal and informal meetings including notes taken by individuals in note books and bullet points are all subject to the above; and emails and other electronic communications.

This list is not exhaustive and does not include copies of documents created by other organisations that are kept for reference and information only.

3.3 Limitations and Applications for CCG Staff - The introduction of the Health and Social Care Act 2012 removed some of the powers and rights of commissioning organisations to obtain, handle, use and share confidential and identifiable information from the CCG. In general, CCG staff are not entitled to use Personal Confidential Data (PCD). Whilst this policy and procedure references health records, this advice is only applicable to CCG staff who have a legal right to this information and it is not applicable to all staff.

3.4 A document becomes a record when it has been finalised and becomes part of the organisation's corporate information.

4. Definitions

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 of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving and disposal.

4.2 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.

4.3 In this policy, **records** are defined as “recorded information, in any form, created or received and maintained by the CCG in the transaction of its business or conduct of affairs and kept as evidence of such activity.”

4.4 **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.

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

4.5.1 Corporate records types may include;

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

These records will support the CCG with a number of key statutory requirements, including:

- Provision of an accurate account of the planning the delivery and evaluation of care;
- Clinical liability;
- Parliamentary accountability;
- Purchasing and contracting, or service agreement management;
- Financial accountability;
- Disputes or legal action;
- Support to Freedom of Information
- Demonstrating sound clinical, information and corporate governance.

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

4.7 All records created in the course of the business of the CCG are corporate records and are public records under the terms of the Public Records Acts 1958 and 1967. This includes email messages and other electronic records (whether business or private email address is used) and are subject to release for FOI and Subject Access / Access to Health Record requests. (See NHS Mail Data Retention and Information Management Policy January 2020).

5. NHS Number

5.1 The NHS Number is a unique number given to every baby born in England and patient registered with the NHS and is the prime patient identifier. This patient identifier enables clinical and administrative records to be exchanged more safely between both electronic and manual systems.

5.2 The CCG will ensure that NHS numbers are used on all clinical communications, clinical records and on all systems processing patient information.

5.3 And will further ensure the following principals are applied when processing patient information and will not procure any IT system that does not support these principals.

5.4 NHS Number Principles

5.4.1 Find It

- Find / Request the NHS Number on referral letters / forms received;
- Determine and verify the NHS Number before or at the start of an episode of care;
- If this is not possible then tracing should be performed as early as possible in the episode either at point of contact or as a back-office process.

Use It

- Use the NHS Number to search for an electronic record as the 'First Choice';
- Use the NHS Number to identify people presenting for care;
- Include the NHS Number on electronic records, wristbands, notes, forms, letters, document and reports which include patient information and are used for that person's care;
- Use the NHS Number as the key identifier for service users;
- Ensure systems can support the NHS Number;
- Use the Personal Demographics Service (PDS) or Demographics Batch Service (DBS) to trace NHS Numbers;

Share It

- Include in all communications, written, verbal and electronic, during telephone calls, on all letters, referrals, forms, documents;
- Internally within your organisation and with all other organisations you contact as part of the provision of care;
- Ensure the NHS Number is included when providing users with any letters or forms;
- Supply the NHS Number as the key identifier for any patient information that assess across systems and organisation boundaries.

6. Accountability, responsibilities and training

6.1 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 records management procedural documents and for working with the Corporate Services Information Governance (IG) Team who will provide some Records Management advice and guidance in line with their contractual obligations.

6.2 The **Caldicott Guardian** is the conscience of the organisation and is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential personal information are in place. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

6.3 The **SIRO** (Senior Information Risk Owner), under delegated authority from the Chief Officer will oversee compliance with the GDPR and Data Protection Act (DPA) and the development of appropriate policy and procedure. The SIRO will be advised by supported by the IG Team. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.

6.4 **Information Asset Owners (IAOs) / Administrators (IAAs)** under the responsibility of the SIRO will:

- be identified, provided with sufficient training material / guidance documentation to enable them to carry out the role 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 Subject Access Request;
- ensure that personal data held in the Information Asset register is maintained in line with the CCG's 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.

6.5 **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; identify training for staff and conduct internal audits. 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.).

6.6 **The Information Governance Manager** in liaison with the Governance Director is responsible for co- coordinating, publicising, implementing and monitoring the Records Management Policy and Procedure and reporting issues or concerns to the CCG's IG, BI and IM&T Steering Group when required.

6.7 **Directors and senior managers** are accountable for the quality of records management within the CCG and all line managers must ensure that their staff,

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

6.8 The CCG's **IG, BI and IM&T Steering Group** will be responsible for ensuring that this policy and procedure is implemented and that the records management system and processes are developed, co-ordinated and monitored.

6.9 **All CCG employees** (including temporary and contract staff), whether clinical or administrative, who create, receive and use records in any form of media have records management responsibilities. All staff must ensure they keep appropriate records of their work in the CCG and manage those records in keeping with this policy and with any guidance. Furthermore, any record that any individual creates is a public record and may be subject to both legal and professional obligations, including compliance with relevant legislation included the Freedom of Information Act, the Data Protection Act and GDPR. This responsibility is established at, and defined by, the law (Public Records Act 1958).

6.10 Staff will receive instruction and direction regarding the policy from several 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 the Data Security Awareness Programme modules via e-Learning for Health. Information Governance training is required to be undertaken on an annual basis.

In line with the Code of Conduct, it is the responsibility of all staff to ensure that they keep appropriate records of their work in the CCG and manage those records in keeping with this policy and any guidance subsequently produced. All employees must:

- Record any important and relevant information, making sure that it is complete;
- Ensure that if written it is legible so that it can easily be read and reproduced when required;
- Retain where it can be found when needed;
- Keep it up to date;
- Only use and share information where necessary;
- Suitably dispose of records as soon as possible (see Records Management Code of Practice for Health and Social Care 2016 for appropriate retention periods).

This applies to all staff including those on temporary or honorary contracts, agency staff and students.

CCG staff are advised about issues regarding confidentiality on commencement of their employment, through induction and it is referred to in job descriptions and contracts in line with all aspects of Information Governance. Failure to comply with any aspect of this policy may result in disciplinary action being taken in line with the CCG's Disciplinary Policy. (Section 28 outlines the possible penalties for CCG employees in breach of legislation and contractual requirements).

7. Inventory of Records held

7.1 The CCG will establish and maintain mechanisms through which Directorates and

other units can document the records they are maintaining. The inventory of record collections will facilitate:

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

7.2 The register will be reviewed annually with the support of the IG team.

8. Record Creation

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

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

8.3 All records should be complete and accurate:

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

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

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

- file reference;
- file title;
- if appropriate protective marking i.e. Customer Confidential/CCG Confidential;
- if possible an anticipated disposal date and what action to take;
- where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed;
- all filling systems to be documented and kept up to date.

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

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

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

8.9 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 can meet the CCG's legal obligations;
- organisations can preserve its corporate memory and track business decisions or transactions over time.

8.10 For checklist on how to create a Record refer to **Appendix 1** – Checklist: Creating a Record.

9. Record Quality

9.1 All CCG staff should be trained in record creation use and maintenance, consummate to their roles, including understanding what should be recorded and how it should be recorded and the reasons for recording it. Staff should know:

- how to validate the information with the patient or the carer or other records to ensure they are recording the correct data;
- why they are recording it;
- how to identify, report and correct errors;
- the use of the information and record;
- what records are used for and the importance of timeliness, accuracy and completeness;
- how to update and add information from other sources.

9.2 Full and accurate records must possess the following three essential characteristics:

- Content – the information it contains (text, data, symbols, numeric, images or sound);
- Structure – appearance and arrangement of the content (style, font, page and paragraph breaks, links and other editorial devices).
- Context – background information that enhances understanding of the business environment/s to which the records relate (e.g. metadata, software) and the origin (e.g. address title, function or activity, organisation, program or department).

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

9.4 Quality Checking

The CCG should establish quality checks which will minimise/eradicate errors. A different member of staff should quality check to the one that has input the information. Dependent on the type of record the following checks should be undertaken:

- ensure the correct retention period has been input onto the document which confirms the right retention/destruction will have been calculated;

- ensure all names are spelt correctly and in the correct format;
- ensure the unique identifiers are correct and in the right format;
- check the barcode number is correct (if relevant);
- the inventory should be checked for all other possible errors.

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

9.5 Data Set Change Notices and Advance Notification

A Data Set Change Notice (DSCN) and Advance Notification (AN) is the mechanism for introducing an information requirement or information standard to which the NHS, those with whom it commissions services and its IT system suppliers, must conform.

10. Record Keeping

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

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

10.3 All records must conform to these record keeping guidelines, legislation, NHS Resolution (NHSR), Department of Health, Information Governance requirements and professional guidelines.

11. Record Maintenance

11.1 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.

11.2 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.

11.3 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.

11.4 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.

11.5 When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account

of the need to preserve important information and keep it confidential and secure. Archiving policies and procedures should be observed for both paper and electronic records.

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

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

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

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

11.10 A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation. 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. An annual risk assessment shall be carried out by the Information Asset Owner to identify the security weaknesses or business continuity risk. Information Asset registers should be included in the directorate business continuity plan.

12. Tracking of Records

12.1 Accurate recording and knowledge of the whereabouts of all clinical and non-clinical records is essential if the information they contain is to be located quickly and efficiently. Records must not be taken out of the office unless this has been agreed by the Line Manager and a tracking mechanism is in place. The tracking system could be manual or electronic and linked to a department's IT system.

12.2 Tracking mechanisms should record the following (minimum) information:

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

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

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

12.4 Electronically operated tracking systems include:

- a computer database, excel spread sheet in place of paper/card index;
- bar code labels and readers linked to computers;
- work flow software to electronically track documents.

12.5 The minimum data which needs to be recorded includes:

- service user's name;
- NHS number;
- date the records were removed;
- destination and name of intended recipient;
- name of the person releasing the records.

12.6 A well thought out, manual or electronic system should:

- provide an up-to-date easily accessible movement history and audit trail;
- be routinely checked and updated;
- be recorded i.e. all movements of a record even if the record is exchanged between teams / staff members within the same building;
- provide a return receipt and it made clear to whom the records should be returned;
- ensure information recorded on the tracking system must be correct and applicable to ensure the system remains effective;
- take into consideration any filing that comes in whilst the records are traced out and must be filed according to local documented procedures until such time as the records are returned;
- ensure that any records are returned safely to their correct home and absent records are chased on a frequent basis;
- maintain a log of all records received into the department including the date received, service user name and NHS number.

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

13. Record Transportation (applies to physical records)

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

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

13.2 NHS organisations are required to map their information flows in accordance with the requirements of NHS Digital's Data Security and Protection Toolkit. The objective of this is to demonstrate that an organisation, in this case the CCG, clearly identifies and has addressed the risks associated with the transfer of identifiable information. This mapping requires all organisations to have an up to date register of information transfers (i.e. audit or mapping the flows of information in and out across the organisation). The CCG maintains an Information Sharing Register for the documenting of all uses and flows of personal information in accordance with GDPR Article 30 and DPA 18 Schedule 1 Part 4).

13.3 Offsite movement of records or other confidential/sensitive information. *(See Appendix 7 – Archiving Guide and CCG Safe Haven Policy – Appendix 3 – Guidance for Transporting Person Identifiable Information).*

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

- Records should not be removed for administrative purposes i.e. writing reports. A trace should be kept at the base from which records have been removed and staff are aware of the location of the record;
- Records should not be left unattended in cars;
- Records kept in any staff possession should remain safe and secure at all times i.e. out of sight and locked away when not in use;
- Records should only be taken off site with the approval of the Line Manager;
- Any vehicle used for the transportation of records must be insured for business use. If the staff member is involved in a road traffic accident which necessitates the car being left on the roadside or taken to a garage, records should be removed.
- If this is not possible the matter should be reported to the Line Manager and an incident form completed.
- Where external courier services are used to transfer patient health records between health organisations, a formal contract/ service level agreement needs to be put in place, which should include a confidentiality clause. A sealed package should be presented to the courier for signature, which should then be signed for by the organisation receiving the records.
- Employees must only send and ask for medical records to be transferred by recorded delivery / courier in an emergency.
- Health or social care records or other confidential information for transportation between CCG sites/departments must be enclosed in sealed bags/envelopes and labelled appropriately i.e. Confidential or Safe Haven. For specific situations of extreme sensitivity i.e. child protection, a further statement should be added stating 'to be opened by addressee only'.
- If paper health records are held that require transportation between CCG sites/departments, they must be carried by authorised staff only. Authorised staff may include:
  - Appropriate member of staff;
  - Internal transport systems;
  - Authorised courier service;
  - Off-site records storage supplier;
  - Special delivery service by Royal Mail.
- Transfer of information slips / records or an equivalent electronic process should

be used to track movement of records.

- The records should not be left unattended in transit at any time. When carried in a car they must be out of sight, i.e. locked in the boot.
- Only in exceptional circumstances may records be taken home by a member of staff to work on. Staff who do so will be responsible for the security and confidentiality of the records as set out in the Safe Haven Policy guidelines on receipt and transporting of items. Please also refer to the Ways of Working Policy for more detail.

13.4 A record must be kept for any transportation of records from one place, organisation or department to another.

13.5 For information and procedures on posting records/sensitive information refer to **Appendix 4**.

14. Lost / Missing Records

14.1 A lost/missing record is a record either that cannot be found following a search in the office environment or is unavailable.

14.2 The loss of records constitutes a reportable incident and should be reported on the CCG's Datix Incident Reporting System in accordance with the CCG's Incident Reporting Procedure. The line manager will be responsible for tracing the record, informing the IAO and IAA, and reporting the incident.

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

15. Scanning

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

- the initial costs of the scanning and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;
- the need to consult in advance with the local Place of Deposit or The National Archives regarding records which may have archival value, as the value may include the format in which it was created; and
- the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

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

16. Disclosure and Transfer of Records

16.1 There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that

require or permit disclosure. Guidance should be sought from the CCG's IG Team prior to any disclosure. If the request for access to information is made under the Freedom of Information Act 2000, then the request should immediately be forwarded to the Freedom of Information mailbox CAPCCG.freedomofinformation1@nhs.net in order to comply with the deadlines specified in the Act.

16.2 The CCG Information Governance Team should be made aware of any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice.

16.3 The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The Information Governance Team can advise on appropriate safeguards.

17. Retention, Archiving and Disposal of Records

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

17.2 The purpose of the 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.

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

17.4 Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility. See **Appendix 8.**

18. Retention of Incident Records

18.1 In any incident, it is important that a comprehensive record is kept of all events, decisions, reasoning behind key decisions and actions taken. Each organisation is required to maintain its own records and those involved in the incident should retain all their records. For those who make decisions, it is very important to have a comprehensive and accurate log of what you have done during the incident as this represents a permanent record that could be used for internal or external inquiry at any time; often several years after the event or incident. See Appendix 9 CCG Incident Records Retention Strategy.

19. Record Closure

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

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

20. Retention Schedules and Record Disposal

19.1 It is a fundamental requirement that all 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.

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

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

19.4 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.

19.5 The Public Records Act requires certain public bodies to transfer records of historical value for permanent preservation to local archive services appointed as 'places of deposit' (PoD). The point of transfer was by the time the records reached 30 years old. Changes in legislation mean that since 1 January 2015 specified local public sector organisations (magistrates' courts, prisons, coroners' courts, NHS bodies and some arms-length bodies including the Environment Agency) must now transfer records selected for permanent preservation to a place of deposit at 20 years after their creation, rather than the previous 30 years. Transferred records should be in good condition and appropriately packed, listed and reviewed for any FOIA exemptions. More detailed guidance on the selection for records for transfer under

the Public Records Act 1958 can be found on The National Archives website: http://www.nationalarchives.gov.uk/archives-sector/our-archives-sector-role/legislation/20-year-rule-and-records-of-local-interest/

The relevant PoD will provide additional local guidance on how the schedules should be implemented. As a general rule, national public sector organisations will deposit with The National Archives while local organisations will deposit with a local PoD. http://www.nationalarchives.gov.uk/information-management/manage-information/places-of-deposit/

19.6 Records over 30 years old and selected for permanent preservation must be transferred to the Public Record Office or kept in a 'relevant place of deposit' for public records. In most cases, such records will be stored in the nearest Local Authority Record Office.

19.7 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.

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

19.9 A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the CCG.

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

19.11 It must be remembered that the destruction of records is an irreversible act.

19.12 Please see **Appendix 5** for Retention Schedules for Corporate Records. Link included to full national retention schedules (Appendix 3) of the Records Management Code of Practice for Health and Social Care.

21. Freedom of Information

21.1 When classifying NHS documents regard should be paid to the requirements of the Freedom of Information Act 2000.

21.2 Consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to inappropriate decisions not to disclose information that would later be embarrassing to the CCG.

21.3 Protective markings should wherever possible be restricted to information that would be exempt from disclosure, including temporary exemptions, such as the drafts of documents that are intended for publication.

21.4 A note of the exemptions that might be relevant to the protective markings is included in **Appendix 6**.

21.5 On receipt of Freedom of Information requests staff should forward onto the CCG FOI mailbox for management of response.
CAPCCG.freedomofinformation1@nhs.net

22. Training Requirements

22.1 An assessment of training needs will be undertaken with staff affected by this document.

22.2 Based on the findings of that assessment appropriate awareness training will be provided to staff as necessary.

23. Access to Health Records and Subject Access Requests

23.1 A Subject Access Request, commonly referred to as a SAR, is a request from a data subject to see a copy of personal information that is held about them by an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by the CCG, both in electronic and paper files. See Right of Access Information Commissioner's Office (ICO).

23.2 Any individual is entitled to:

- Know what information is held about them and why;
- Gain access to it regardless of the media which it is held;
- Have their information kept up to date;
- In some situations, require the CCG to rectify/block, erase or destroy inaccurate information;
- Not have confidential information processed about them likely to cause damage or distress;
- Not have confidential information processed about them for the purposes of direct marketing.

23.3 In certain cases, the CCG will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent may be needed. It may be a condition of patients, and employment of staff, that they have been made aware and agree to the CCG processing specific classes of personal information.

23.4 The CCG may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety, or to comply with the requirements of other legislation.

23.5 The Access to Health Records Act 1990 provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

23.6 For further guidance and information please see the CCG's Access to Records Policy which incorporates Subject Access Requests.

24. Information Risk Management

24.1 Where required the information risk management process will take place using the NHS "5x5 Risk Matrix" as detailed in the NPSA's "Risk Matrix for Risk Managers". The Risk Management Policy contains guidance on how to interpret the scores that will be

attributed to risks and provide the basis for information risk reporting to the CCG's IG, BI and IM&T Steering Group and Integrated Performance and Assurance Committee (IPAC).

25. Records Management and System Audit

25.1 The process for monitoring and evaluating the effectiveness of this policy, including obtaining evidence of compliance will be part of the CCG's Data Security and Protection Toolkit annual self-assessment.

The CCG will audit its records management practices for compliance with the framework to:

- identify areas of operation that are covered by the CCG policies and identify which procedures and/or guidance should comply to the policy;
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance: and
- highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment related procedures.

25.2 The results of audits will be reported to the IG, BI and IM&T Steering Group and exceptions escalated to the Integrated Performance and Assurance Committee.

26. IG Training and Awareness

26.1 CCG staff are mandated to undertake Information Governance training (in the form of Data Security Awareness e-Learning module) annually. Good Record Keeping features within this training. All CCG Staff will be made aware of their responsibilities for record-keeping and record management.

26.2 Where staff may take on a specific Information Governance role within the CCG e.g. Records Management, dealing with Access to Records, Data Protection Impact Assessments or Information Asset Ownership, additional Information Governance training may be required.

26.3 The Information Governance Training (Data Security Awareness e-Learning module) will be utilised, and uptake will be monitored. Where required for specific teams the CCG will deliver annual face to face training sessions that include Records Management.

26.4 The CCGs IG, BI and IM&T Steering Group will be responsible for ensuring that this policy and supporting procedures are implemented, and that the records management system and processes are developed, co-ordinated and monitored.

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

26.6 To maintain high staff awareness, the CCG will direct staff to several sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training courses;
- other communication methods, for example, team meetings; and staff extranet.

27. Monitoring and Review

27.1 This policy and procedure will be monitored through staff awareness whilst assessing supporting evidence for the NHS DSP Toolkit.

27.2 This policy and procedure will be reviewed every two years, or as required by the following:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

27.3 Where there are no significant alterations required, this Policy and Procedure shall remain for a period of two years from the ratification date.

28. Legislation

28.1 All NHS records are public records under the Public Records Acts 1958. The CCG will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice for Health & Social Care 2016, additionally:

- The Public Records Act 1958 and 1967;
- The Data Protection Act 2018 / General Data Protection Regulation (GDPR);
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice; and
- National Archive - http://www.nationalarchives.gov.uk/

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

28.3 Under the Freedom of Information Act 2000, once a record has been requested, it cannot be destroyed. It is a criminal offence to amend, erase or destroy information once a request is received.

Legislation (Requirement)	What it covers	Personal responsibilities	Penalties for breaches
Data Protection Act 2018 / GDPR	Person identifiable information about living individuals – manual and automated records (e.g. on computer, video tape, digital images).	Keep all person identifiable information secure and confidential – see Code of Conduct for specific details.	Unauthorised disclosure of personal identifiable information could lead to court action and a criminal conviction and/or the payment of compensation to a claimant.
Human Rights Act 1998 (Article 8)	An individual's right to privacy for themselves and their family members	As above	As above
Computer Misuse Act 1990	Unauthorised access to computer held programs and information/data	Do not use any other person's access rights (e.g. user id and password) to access a computer database	A criminal record and a prison sentence of up to 5 years.
Common Law Duty of Confidentiality	An individual's right to confidentiality of their information when alive and once they have died	Keep all information secure and confidential. Also covers wishes of deceased persons – if it is recorded they do not want details of their treatment disclosed when they die.	Disciplinary action and possible dismissal.
Caldicott (National Data Guardian for Health and Care)	Security and confidentiality of personal health and social care information for patients and service users	See CCG Code of Conduct or Caldicott Guardian or Data Protection Officer.	Disciplinary action and possible dismissal.
Contract of Employment	Employee responsibilities incl. security and confidentiality of	Comply with contract and Code of Conduct.	Disciplinary action and possible dismissal.

Legislation (Requirement)	What it covers	Personal responsibilities	Penalties for breaches
	any information accessed during the course of work		

29. Other relevant CCG Policies

- Information Governance Framework
- Information Governance Policy
- Data Protection Policy
- Code of Conduct for Confidentiality Policy
- Cyber Security Policy
- IT Security for Staff Policy
- Risk Management Policy
- Access to Records Policy
- Safe Haven Policy
- FOI Act Policy and Publication Scheme
- IG Forensic Readiness Policy
- Data Quality Policy

Note: 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 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 event 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.

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, factual, consistent and accurate
- Legible, clear and unambiguous
- Contemporaneous, i.e. written as soon as possible
- Consecutive and dated (and timed if appropriate)
- If appropriate, signed by the data subject/individual according to the service specific policies
- Only in exceptional circumstances, should entries to records be delayed
- Not include abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements
- Be written clearly and in such a manner that the text cannot be erased.

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 - 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 reported on the Datix Incident Reporting System to alert the Information Governance Team;
- 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

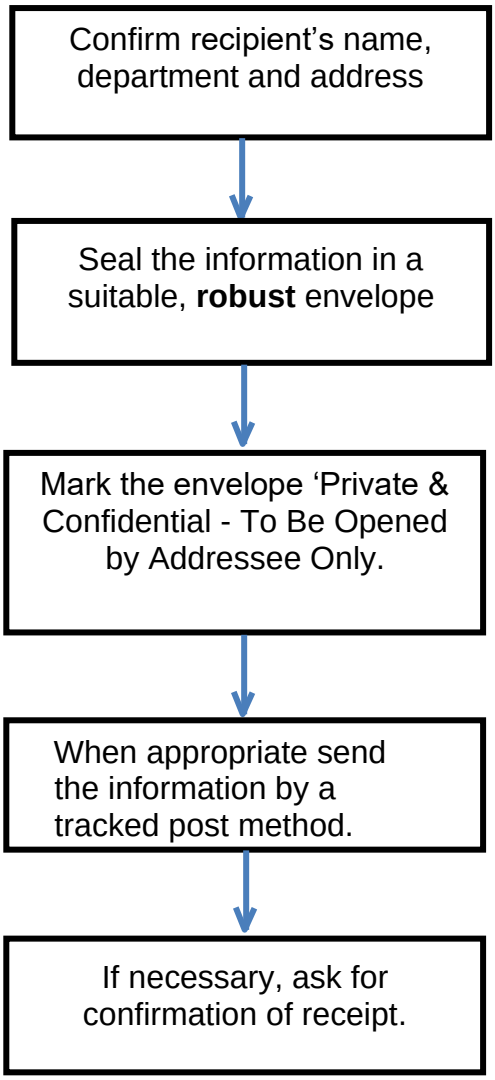
- A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment;
- Any unavailable/missing records must be reported on the Datix Incident Reporting System to alert the Information Governance Team;
- A temporary record should be created, as described 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 reported.

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 4 - Sending Information via Postal Service

Guidance for sharing Personal, Confidential or Sensitive information by POST



Appendix 5 - Retention Schedule for Corporate Records

Full Guidance and retention schedules can be found in Appendix 3 of the Records Management Code of Practice for Health and Social Care at: https://digital.nhs.uk/codes-of-practice-handling-information

Record Type	Retention start	Retention period	Action at end of retention period	Notes
9. Corporate Governance				
Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
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.
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.
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	
Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings

Record Type	Retention start	Retention period	Action at end of retention period	Notes
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 Act. 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.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
10. Communications				
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
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

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
11. Staff Records & Occupational Health Although pension information is routinely retained until 100**th** birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75**th** birthday.				
Duty Roster	Close of financial year	6 years		Review and if no longer needed destroy
Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner		Review and if no longer needed destroy
Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday		Review and if no longer needed destroy
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

Record Type	Retention start	Retention period	Action at end of retention period	Notes
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 Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see the good practice box Staff Record Summary used by an organisation.
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	

Appendix 6 - Freedom of Information Act Exemptions
(that may be relevant to the use of protective markings)

Category	Possible Exemption [sections(s) of the FOI Act]
Appointments	S 40 Personal information (may be subject to a public interest test)
Barred	S 44 Legal prohibitions on disclosure
Commercial	S 43 Commercial interests (subject to a public interest test)
Contracts	S 43 Commercial interests (public interest test)
For Publication	S 22 For future publication (public interest test)
Management	S 38 Endanger health and safety (public interest test)
Personal	S 40 Personal information (may be subject to public interest test)
Policy	S 22 For future publication (public interest test)
Proceedings	S 30 Investigations and proceedings S 31 Law enforcement

Appendix 7 - Archiving Guide

Archiving Process - Standard Operating Procedure

1. Background

Standard Operating Procedures (SOPs) are both a set of written instructions and a written record of procedure. SOPs aim to ensure that regularly performed tasks are completed consistently and uniformly across the CCG and can be an effective measure to improve performance and results.

2. Purpose

This document describes the process to archive files for the Cambridgeshire & Peterborough Clinical Commissioning Group (CCG) with the contractor responsible for archiving Restore Records Management.

3. Persons Affected

All staff within the CCG.

4. Definition

To archive appropriate documentation in a professional manner that can be retrieved quickly from the contracted archiving provider, Restore Records Management .

5. Responsibility

5.1 The Corporate Services and Resilience Manager is responsible for updating this document and ensuring Corporate Business Continuity Plans are supplied with up-to-date information.

5.2 The Corporate Services and Resilience Manager will be responsible for training new Corporate administration staff to use the archiving process to provide business continuity in the event of an emergency.

5.3 It is the responsibility of all Managers throughout the CCG to ensure their directorate staff are able to use the archiving process correctly and in the event of an emergency, for business continuity purposes.

6. Review

This process should be reviewed every two years or whenever the archiving process is changed.

7. Procedure for Box Preparation to Archive

- Each Archive box should have the Box Label on the front of the box. This label should be fully completed so that Restore Records Management are able to see where each box originated.

- One barcode per box – this needs to be placed in the designated area on the front of the box. Boxes and barcodes are available by contacting the Corporate Services and Resilience Manager at capccg.officemanager@nhs.net
- The 'date of destroy' – this should be written in the designated box under the barcode label. There should be one date of destroy per box – the contents of the box will need to reflect this. Guidance on retention periods can be found: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016
- All records should be placed into the archive box in envelopes or brown paper – one record per envelope.
- You will need to enclose in the box a completed Contents Page. The contents page should detail all items within the box.
- A record of the contents of each box and a copy of the contents page is to be kept by the team only and not by the Office Manager.
- Tape the boxes with parcel tape and mark private and confidential.
- Archiving is box indexed and not file/document indexed, if you require retrieval of a file from archiving in the future, the full box will be retrieved via the barcode. You will not be able to request an individual document/file.
- Complete the form for box collection. Only include the box barcode and collection address on the form, DO NOT include any confidential or patient information.
- When boxes are ready, please contact the Office Manager at (CAPCCG.officemanager@nhs.net) who will arrange for them to be collected. Ensure the boxes are available in the reception area at the CCG base.

9. Procedure for Collection to Archive

- The Corporate Services and Resilience Manager is set up as an approved contact and authoriser with Restore Records Management and is the only staff member who can request collection of boxes to go to archive for the CCG.
- On receipt of the completed form via email to the Corporate Services and Resilience Manager (CAPCCG.officemanager@nhs.net).
- The form is to be checked to ensure it only contains barcode number and collection address and no confidential information. Date the form and send to: Archive.Services.GB@tnt.co.uk Attach the completed form and ask that collection for archive is arranged under our standard Service Level Agreement (SLA).
- Confirmation email from Restore Records Management will be received and a date for confirmed collection. Inform reception staff of expected Restore Records Management collection date.

10. Procedure for Retrieval from Archive

- The Corporate Services and Resilience Manager is set up as approved contact and authoriser with Restore Records Management and can only request boxes to be retrieved from archive for the CCG.
- Complete the form for box retrieval. Only include the box barcode and address the box is to be delivered to on the form, DO NOT include confidential or patient information.

- Send the completed form via email to the Corporate Services and Resilience Manager (CAPCCG.officemanager@nhs.net). The form is to be checked to ensure it only contains barcode number and delivery address and no confidential information. Date the form and send to: Archive.Services.GB@tnt.co.uk Attach the completed form and ask that retrieval from archive is arranged under our standard SLA. You can ask for urgent retrieval if required, but this may be at an additional cost.
- Confirmation email from Restore Records Management will be received and a date for delivery. Inform reception staff and the requester of expected Restore Records Management delivery date.

Note: *All forms referred to within Appendix 7 are included in the CCG's Archive Process Standard Operating Procedure v2 March 2018*

Appendix 8 - Disposal of Unwanted Equipment and Information

Introduction

It is vital that confidentiality is safeguarded at disposal. Therefore, it is all employees' responsibility to ensure that the chosen method used to destroy records is fully effective and secures their complete illegibility. Methods may include: Shredding, Pulping, Incineration.

All information about people and the organisation should be disposed of in a secure manner when no longer required regardless of the media on which it may be held.

Prior to disposing of any information, employees should consult Cambridgeshire and Peterborough CCG's Records Management and Lifecycle Policy in conjunction with the Records Management Code of Practice for Health and Social Care 2016, to ensure that it is legal to dispose of the information. These policies outline the retention periods for information, and covers employee records, administrative records, estates records, reports, investigations and complaints etc. All relevant policies are available on the CCG's website.

All employees will be informed of the correct methods of disposal of waste/ unwanted information through staff training, induction and/or making them aware of policies and guidance available on the website.

Destruction of paper waste

It is important that all paper type business waste material is disposed of in a secure manner, to maintain confidentiality and comply with legal requirements.

All waste/unwanted paper will be disposed of by placing in the paper recycling bins or locked confidential blue bins located in Gemini House (on ground and first floors).

Unwanted paper may include draft documents, unwanted agendas and minutes of meetings, any papers in files the CCG no longer needs to retain, bad photocopies or handwritten notes etc. Any papers put into the cardboard recycle bins or general rubbish bins can be extracted by anyone who wishes to see and/or use the information. Care must be taken to ensure that confidential material is identified and removed so that only general papers are disposed of in these types of bins.

Any papers that identify staff or patients or contain business sensitive information, financial information, complaints, Serious Untoward Incidents, and/or any information that may identify a patient **MUST** be put into the locked blue containers for confidential disposal.
Note: If a document needs to be retrieved from the confidential waste, the keys are securely stored at Reception and a Facilities Co-ordinator will accompany you whilst you retrieve the item and ensure that the bin lid is secured afterwards.

If the information is deemed to be highly sensitive or confidential it may be necessary to shred or tear into very small pieces prior to being placed in the confidential bin.

Once the bins are full, a designated authorised contractor will collect them. The contractor will dispose of the papers in a secure confidential manner as stipulated in the

contractual agreement between Cambridgeshire and Peterborough CCG and current provider, DataShred.

Staff are reminded that they have a personal duty to ensure papers containing sensitive detail are not to be put into the ordinary waste-paper bins, as doing so will constitute a confidentiality breach.

Media	How to dispose
PAPER (non-confidential)	Put into recycling bins located in each department. The bins will be collected/emptied when full by the authorised contractor and taken away in a secure manner for pulping/re-cycling.
PAPER (confidential)	If the information is sensitive the paper must be put into one of the blue confidential waste containers at Gemini House. There is a 'post box' size opening for papers to be 'posted'. These confidential waste bins are routinely collected by the data shredder contractor who will then shred the paper securely. **Note:** If a document needs to be retrieved from the confidential waste, the keys are securely stored at Reception and a Facilities Co-ordinator will accompany you whilst you retrieve the item and ensure that the bin lid is secured afterwards.

Computer media
Computer media will include all the items listed in the table below. This is not an exhaustive list of all possible media as technology will evolve and new media will become available as time progresses.

Below are the most common types of media in use at the time this policy was produced. This Policy will be updated regularly and therefore take account of new media throughout the review period.

Media	How to dispose
FLOPPY DISKS / DVDs/ CDs	The CCG do not routinely create Floppy disks, DVD, CDs but prior to disposal they must be re-initialised / reformatted and destroyed, or if defective, be physically destroyed, ideally by shredding or incineration. Once information has been removed from the disc it can be reused (only if encrypted) or, if no longer required, should be destroyed. The CCG have an agreement via an Egton supported service for the secure destruction of such items. If a staff member has such a device for destruction, please contact the Senior ICT Service Development Manager for advice. Prior to destruction this material should be physically locked away.
MAGNETIC TAPES	Must be re-initialised / degaussing and destroyed by incineration and/or shredding, or, if defective, will be physically destroyed by incineration. The CCG has an agreement via an Egton supported service for the secure destruction of such items. If a staff member has such a device for destruction, please contact the Senior ICT Service Development Manager for advice. Prior to destruction this material should be

Media	How to dispose
	physically locked away.
PCs	Hard disc will be wiped clean (erased) and then disposed of by an Egton supported service in a secure manner as agreed with the CCG.
TERMINALS / PCs	Will be disposed of by an Egton supported service in the agreed manner. NHS Cambridgeshire and Peterborough CCG employees will need to contact the Senior ICT Service Development Manager for this process to be initiated.
LAPTOPS	Will be returned to ICT department / line manager when an employee leaves or no longer requires a laptop. The asset register must be updated to reflect change of ownership. Any information not removed by the last user will be erased prior to being re-allocated to another user. When the laptop no longer works and is beyond repair, if possible, all software and data will be removed prior to being sent to an Egton supported service for safe destruction/disposal to comply with EU requirements. This disposal is coordinated through the CCG ICT team.
LARGER HARDWARE	Will be disposed of securely and safely by an Egton supported service as detailed in the Service Level Agreement.
SOFTWARE	Will be disposed of in a secure manner when no longer required. Most software is either downloaded or if uploaded from a CD and the CDs will be disposed of as stated above.
MEMORY STICKS/ FLASH CARDS	NHS Cambridgeshire and Peterborough CCG staff should only use CCG supplied encrypted memory sticks. When the information is no longer required, the user should delete it from the memory stick. When an employee leaves or no longer requires a memory stick it should be returned to the Senior ICT Service Development Manager and not passed to another member of staff without prior agreement. However, at times other organisations may supply such devices which will need to be disposed of. Disposal can be arranged via the Senior ICT Service Development Manager and the device must be kept securely until disposal is arranged.
MOBILE PHONES/ SMART PHONES	Will be returned to line manager before sending to CCG ICT Team (supported by 360com), where the phone will be re-set to the factory settings and it will be re-issued. If the phone is faulty it will be disposed of securely.
SIM CARDS/ MEMORY STICKS	If the SIM and/or memory card is faulty it will be cut into pieces and disposed of in a secure manner.
MULTI-FUNCTIONAL DEVICE / PRINTER HARDDRIVES	When a multi-functional device (MFD) / printer that contains a hard drive is removed, the hard drive should be destroyed on site or securely wiped. The company providing these devices will do so if they are informed of the requirement before they arrive to move or replace the MFD or printer. Further advice is available from the Senior ICT Service Development Manager.

Appendix 9 – CCG Incident Records Retention Strategy
Ensuring our CCG is able to respond to any future inquiries and keeping our CCG safe.

Roles and Responsibilities
Accountable Officer - is personally accountable for records management and retention within the CCG and has a duty to make arrangements for the safekeeping of those records.

Accountable Emergency Officer - The Accountable Emergency Officer (Director of Governance) is accountable to delivery of the CCG's Incident Response Plan which provides the framework for overall management of incidents, and retention of records in line with the NHSE EPRR Framework and Civil Contingencies Act 2004.

Senior Information Risk Owner (SIRO) - takes ownership of information risk policy.

Caldicott Guardian - oversees the confidentiality of patient information according to the seven Caldicott Principles.

Principles
In any incident, it is important that a comprehensive record is kept of all events, decisions, reasoning behind key decisions and actions taken. Each organisation is required to maintain its own records and those involved in the incident should retain all their records. For those who make decisions, it is very important to have a comprehensive and accurate log of what you have done during the incident as this represents a permanent record that could be used for internal or external inquiry at any time; often several years after the event or incident.

What will we do?
- ✓ Follow national guidance
- ✓ Comply with the Civil Contingencies Act
- ✓ Comply with the **Records Management Code of Practice for Health & Social Care**. Appendix 3 of the Code contains the **detailed retention schedules**, and the CCG Records Management & Lifecycle Policy
- ✓ Aligned with Incident Response Plan
- ✓ Retain any paperwork and data for 20 years (in line with Corporate Governance retention period for serious incidents)
- ✓ Ensure capture of key decisions including who made them and when.
- ✓ Ensure we have the ability to respond to any potential legal or public inquiry.
- ✓ Include any mitigations of risk for what is retained and how.
- ✓ Phased retention process to capture data throughout incident.

Consideration One – Electronic Data

What will we do?
- ✓ Retention of emails of all key decision makers (Accountable Officer and Deputy Accountable Officer, Chief Officer Team members, Tactical Operational Cell (TOC) leads, Information Governance, Information Technology and Accountable Emergency Officer, Care Home Lead).
- ✓ Data Capture and retention of TOC folders on Microsoft Teams / SharePoint.
- ✓ Retention of electronic decision logs.
- ✓ Shared email accounts to be considered on a case by case basis due to the availability of this data being held elsewhere and already retained.
- ✓ Ensure communication to relevant decision makers and other staff regarding the

process relevant to them.

Consideration Two – Hard Copy Physical Data

What will we do?

- ✓ Retention of all formal log-books, pertinent to the incident.
- ✓ Ensure retention of flip charts and papers used in ICC prior to virtual working being implemented.
- ✓ Notebooks, post it notes, hard copy paper documents to be indexed and retained in "red box" relating to the incident.
- ✓ Archive all appropriately and retain availability for up to 20years.
- ✓ Provide clear communications to staff regarding process and point of contact.

Consideration Three – Lessons Learns

What have we learnt?

- ✓ Difficulty in the format of storing emails and ensuring availability in access to these in the future.
- ✓ Difficulty in the format providing an ability to "search and interrogate" the data in the future.
- ✓ Potential non-compliance with the request not to remove files from the TOC team structure during the data transfer.
- ✓ Capture all Incident Lessons Learnt and feed this into future planning.
- ✓ Lack of data retention confirmation from CCG leavers during the process.

Consideration four – Implementations into Phase 4 and Beyond

What will we do?

- ✓ Request all SRO and senior decision makers use a formal incident log book to ensure capture and the ability to more readily store and retain this information for the future
- ✓ Request all SROs for Recovery Workstreams use the Teams sites to save all files and work relevant to recovery within the areas to ensure smoother capture of data for Phase 2, if and when required.
- ✓ Review requirements for the above when the NHS Major Incident Level 4 has been reduced.
- ✓ Update Incident Response Plan, Business Continuity Plan, EPPR Framework and Outbreak Plans as appropriate, using CCG Lessons Learnt and Regional Input
- ✓ Inclusion of process for CCG leavers and consideration to whether we have the information required from previous leavers.

Annex A – Equality Impact Assessment Form

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Equality Impact Assessment Form

Name of Proposal (policy/strategy/function/service being assessed)	CCG Records Management and Lifecycle Policy
Those involved in assessment:	Information Governance, Business Intelligence and IM&T Steering Group
Is this a new proposal?	No - Biennial Review
Date of Initial Screening:	4 September 2018

What are the aims, objectives?	To provide guidance to all Cambridgeshire and Peterborough Clinical Commissioning Group (CG) staff on Records Management. This policy is adopted from the NHS England Policy of the same name.
Who will benefit?	The CCG, staff, patients and members of the public and the media.
Who are the main stakeholders?	The CCG Information Governance, Business Intelligence, IM&T Steering Group, staff, patients and members of the public, service providers and other partners who work in partnership with the CCG.
What are the desired outcomes?	To ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.
What factors could detract from the desired outcomes?	Lack of awareness of the existence of the Policy; Failure to follow the Policy/procedure and lack of training.
What factors could contribute to the desired outcomes?	Knowledge of the Policy, access of the policy and proper training
Who is responsible?	Everybody involved in handling and managing data on behalf of the CCG
Have you consulted on the proposal? If so with whom? If not why not?	IG, BI & IM&T Steering Group and endorsed endorsed by the Integrated Performance and Assurance Committee and CCG Governing Body.

Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick)		Yes	No
Age	Consider: Elderly, or young people		x
Disability	Consider: Physical, visual, aural impairment Mental or learning difficulties		x
Gender Reassignment	Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned		x
Marriage and Civil Partnership	Consider: Impact relevant to employment and /or training		x
Pregnancy and maternity	Consider: Pregnancy related matter/illness or maternity leave related mater		x
Race	Consider: Language and cultural factors, include Gypsy and Travellers group		x
Religion and Belief	Consider: Practices of worship, religious or cultural observance, include non-belief		x
Sex /Gender	Consider: Male and Female		x
Sexual Orientation	Consider: Know or perceived orientation		x

What information and evidence do you have about the groups that you have selected above?

This policy is designed to protect everyone's data regardless of their characteristics and therefore should have no adverse impact on any of the protected characteristics listed above.

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

How might your proposal impact on the groups identified? For example, you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People.

Examples of impact re given below:

a) Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc

b) Planning to extend access to contraceptive services in primary care without considering how their services may be accessed by lesbian, gay, bi-sexual and transgender people.

c) Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.

Please list the positive and negative impacts you have identified in the summary table on the following page.

Summary	
Positive impacts (note the groups affected) N/A	Negative impacts (note the groups affected) N/A

Summarise the negative impacts for each group:

Negative impacts will only occur if there is a lack of knowledge of the policy and lack of guidance and training.

What consultation has taken place or is planned with each of the identified groups?

N/A

What was the outcome of the consultation undertaken?

N/A

What changes or actions do you propose to make or take as a result of research and/or consultation?

Briefly describe the actions then please insert actions to be taken on to the given Improvement Plan template provided. Policy has been written in light of the new data protection legislation and other national requirements, with a view to improve data management and safeguard data subjects efficiently and effectively.

Will the planned changes to the proposal:	Please State Yes or No
Lower the negative impact?	Yes
Ensure that the negative impact is legal under anti-discriminatory law?	Yes
Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact?	Yes

Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits.

To mitigate any risks associated with this policy the CCG will regularly audit its records management practices for compliance with the framework and identify any gaps in the implementation of the policy.

What monitoring/evaluation/review systems have been put in place?

Complaints and training records.

When will it be reviewed?

September 2022

Date completed:	8th October 2020
Signature:	Lynn Carter, Information Governance Manager
Approved by:	Soomitra Kawal, E&D Advisor
Date approved:	14th October 2020