East Coast Community Healthcare Records Management Policy and Associated Procedures

Version No 9: October 2025

First Issued: May 2012
Review date: October 2028

Contents

*(For quick access to a specific heading - **press CTRL and click your mouse** to follow the link for the below options)*

1. INTRODUCTION

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any media and format type, from their creation, all the way through their life cycle to their eventual disposal.

The Information Governance Alliance Records Management Codes of Practice has published NHS Digital as a guide to the required standards of practice in the management of records for those who work within or under contract to the NHS organisations in England. It is based on current legal requirements and professional best practice.

East Coast Community Healthcare (ECCH) 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 ECCH 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.

ECCH has adopted this records management policy and is committed to ongoing improvements of its records management functions as it believes it will gain a number of organisational benefits from doing so. 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.

ECCH 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.

This document sets out a framework within which the staff responsible for managing ECCH 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.

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 ECCH 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
- Disposal

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.

In this policy, *Records* are defined as 'recorded information, in any form, created or received and maintained by ECCH in the transaction of its business or conduct of affairs and kept as evidence of such activity'. A *health record* consists of: '*any information relating to the physical or mental health or condition of the individual and has been made by or on behalf of a health professional in connection with the care of that individual."* (Data Protection Act)

Information is a corporate asset. ECCH's records are important sources administrative, evidential, and historical information. They are vital to NHS Gt Yarmouth & Waveney 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. *Recorded Information:* in this policy records are defined as recorded information in any form, created or received and maintained by ECCH in the transaction of its business or conduct of affairs and kept as evidence of such activity.

2. PURPOSE

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

- Records are available when needed – from which ECCH is able to form a reconstruction of activities or events that have taken place.

- Records can be accessed – records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.

- Records can be interpreted – the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records.

- Records can be trusted – record reliability represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

- Records be maintained through time – the qualities of availability, accessibility, interpretation, and trustworthiness can be maintained as long as the format is needed, perhaps permanently, despite changes of format.

- Records are secure – from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled, and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required

- Records are retained and disposed of appropriately – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent reservation of records with archival value

- Staff are trained – so that everyone is made aware of their responsibilities for record-keeping and record management

3. SCOPE

This policy applies to all East Coast Community Healthcare staff members, whether permanent, temporary, or contracted in (either as an individual or through a third party supplier).

This policy relates to all clinical and non-clinical operational records held in any format by ECCH. These include:

- All administrative records (e.g., personnel, estates, financial and accounting records, notes associated with complaints)
- All patient health records (for al specialties and including private patients, including x-ray and imaging reports, registers etc.)

4. DEFINITIONS

The following definitions are intended to provide a brief explanation of the various terms used within this policy.

Term	Definition
Records Management	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 ECCH and preserving an appropriate historical record.
Records Life Cycle	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.
Records	Recorded information, in any form, created or received and maintained by ECCH in the transaction of its business or conduct of affairs and kept as evidence of such activity'
Health Record	"Any information relating to the physical or mental health or condition of the individual and has been made by or on behalf of a health professional in connection with the care of that individual." (Data Protection Act)

5. RESPONSIBILITIES

ECCH Employees – All ECCH staff, whether clinical or administrative, who create, receive, and use records have records management responsibilities including adherence to this Policy. In particular all staff must ensure that they keep appropriate records of their work in ECCH and manage those records in keeping with this policy and with any guidance subsequently produced.

This task will include:
- implementing physical and or technical controls;
- administering access to information;
- ensuring the availability of information by implementing appropriate recovery options based on the business criticality of the information in their possession, as per the disaster

Chief Executive of ECCH – The Chief Executive has overall responsibility for records management in ECCH. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required. ECCH has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements. Information Governance principles require the appointment of a Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Caldicott Guardian.

ECCH Managers – The responsibility for local management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units, and business functions within ECCH have overall responsibility for the implementation of this Policy and the management of records generated by their activities, i.e., for ensuring that records controlled within their unit are managed in a way which meets the aims of ECCH records management policy in accordance with the requirements specified by the relevant Information Asset Owner.

Caldicott Guardian – ECCH's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Caldicott & Information Governance Group - ECCH's Caldicott & Information Governance Group is responsible for ensuring that this policy is ratified and that the records management system and processes are developed, co-ordinated and monitored.

Information Custodian - Information Asset Owners are those individuals who control information systems regardless of physical or logical location, storage medium, technology used, or the purpose(s) they serve.

6. POLICY STATEMENT

ECCH's Records Management policy defines the scope of Records Management, the processes it entails and how the organisation ensures that good practice is maintained for all Records Management.

7. PROCEDURE

Key Procedural Elements of the Policy

The Records Management Procedures comprise the following key objectives:

Responsibility and Accountability
To provide a clear system of accountability responsibility for record keeping and use

It is the responsibility of ECCH employees to accept accountability for the creation, amendment, management, storage, and access to all ECCH records. For the purposes of this policy the term "employee" is used as a convenience to refer to all those to whom this policy should apply. Whilst directed at ECCH staff it is also relevant to anyone working in and around the ECCH and its premises which includes but is not limited to contractors, agency & temporary staff, student, honorary and volunteer staff.

Record Quality
To create and keep records that are adequate, consistent, and necessary for statutory, legal, and business requirements.

All ECCH records must be accurate and complete, in order to facilitate audit, fulfil ECCH's responsibilities, and protect its legal and other rights.

Management
To achieve systemic, orderly, and consistent creation, retention, appraisal, and disposal procedures for records throughout their lifecycle.

- Record keeping systems must be easy to understand, clear, and efficient in terms of minimising staff time and optimising the use of space for storage.

- In order to ensure that the information held in records is accurate and readily available where it is appropriate, record keeping systems and processes must incorporate version control numbering techniques. This will help employees to identify contemporaneous information and prevent inaccurate and out of date information being used in error. Some informatic systems may automatically provide a numbering system to help users identify the latest records however, wherever possible version control must be employed within all manual record keeping systems.

Record Creation
To ensure a full, visible audit trail of the creation, amendment, and destruction of ECCH documents is maintained.

- Each directorate, service or department must have in place a process for documenting its activities in respect of records management. These processes must take into account the legislative and regulatory environment in which the directorate, service or department operates and follow the guidelines inculcated in this section.

- Records of operational activities must be complete and accurate in order to allow employees and their successors to undertake appropriate actions in the context of their responsibilities, to facilitate an audit or examination of the organisation, its patients, staff, and any other people affected by its actions, and provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

- All records must contain a unique identifier; where relevant, this will be the NHS number. Records created by ECCH must be arranged in a record keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information. All entries must be dated and timed (using the 24-hour clock). It is essential for the patient/service user record to have both.

- Records created must have meaningful file names that will enable them to be easily recognised and quickly located and in, accordance with above, that show, where applicable, the version sequence such that the latest or current approved version can be clearly identified.

- Conventions for naming electronic documents must be co- coordinated with those for naming electronic folders, so that a document title does not contain information already present in the folder in which it is filed. Naming conventions must strike a balance between keeping titles short and useful.

- Document creators, dates of creation and modifications including version numbers, must make up the composition of the document title. In addition, the aforementioned information must also be reflected throughout a documents by using footers. In summary:
  - Names should be kept clear and as brief as possible.
  - Easy to introduce, follow and extend.
  - Logical, consistent, and easy to remember.

- Standard terms and forms of name must be used wherever it is sensible to do so. This should apply to:
  - Names of organisations, departments, and people (job titles)
  - Names of projects, functions, activities
  - Document types, topics

- Abbreviations (and Acronyms) –Acronyms and abbreviations should be avoided wherever possible. Where an Acronym or abbreviation is to be used the words should be written out in full on the first occasion with the acronym or abbreviation in brackets thereafter the acronym or abbreviation can be used. The only exception to this is within Musculoskeletal Physiotherapy where abbreviations for anatomical joints may be used where the clinical record is accompanied with the up-to-date chartered society of physiotherapists list to explain the abbreviation.

- Alterations – Errors should not be hidden. Paper records should have errors scored out with a single line and the correct entry written alongside. Corrections should be signed and dated, and name printed. Alterations in electronic records must have audit trails.

- Additions – If an addition needs to be made to a record it should be prefaced with a comment indicating that this is an additional or late entry and be separately dated and signed. Inserting notes, especially after notification of a complaint or claim is not acceptable, neither is disguising additions to a record.

- Personal comments – Only include commentary that is factual, relevant, and appropriate to the record. Records are not the place to note personal opinion, supposed humorous comments, offensive or judgmental observations about a person’s character, appearance or habits. The General Data Protection Regulation

(GDPR) gives everyone the right to have a copy of all information that is held about them.

- Dictated notes – Typed notes must be checked and signed by the professional who dictates them. Responsibility for the accuracy of the record lies with the person who created the record not the typist.

- Completeness – A record needs to contain sufficient information to be fit for purpose. Standard request forms e.g., test results or order forms should be complete. Insufficient information may lead to serious mistakes or misinterpretation of data.

- Clarity and Legibility – Records need to be clear and legible. A handwritten record should be written in permanent black ink. This will give records greater clarity and legibility when photocopied. If it is not possible for a person to write legibly the record should be typed. Thermal faxes may fade and should not be included as part of a permanent record – information should either be transcribed into the record, the original requested or an indelible copy made of the fax. All records should follow basic English grammar principles and include punctuation to maintain legibility.

Quality Assurance
To ensure ECCH Employees, including those defined above, are properly trained in and have an understanding of the operation of records management procedures

- Responsibility- If you are responsible for the supervision of, for example, preregistration students or healthcare assistants, you must remember that you are professionally accountable for the consequences of all health record entries made by such persons. You must clearly countersign any such entry and your signature should be clearly identified. You should print your name alongside the first signature. You must not use your initials only as your signature.

- Staff must be trained in record creation, use and maintenance, including having an understanding of:

    - What they are recording and how it should be recorded;
    - Why they are recording it;
    - How to validate information with patients, carers, and staff or against other records to ensure staff are recording the correct data;
    - How to identify and correct errors and how to report errors if they are found;
    - The use of information – so staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important) and;
    - How to update information and add in information from other sources

Record Keeping
To document and communicate employee responsibilities for the proper management of ECCH records

- A variety of training and guideline material is available for details on managing records including:
  - The Information Governance Framework & Policy inclusive of the Information Governance Handbook, available on ECCHO under Policies

- Paper and electronic record keeping systems must include descriptive and technical procedural documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation must provide an administrative context for effective management of records.

- The record keeping system, whether paper or electronic, must include a documented set of rules for referencing, titling, indexing, and, if appropriate, the protective marking of records. These must be easily understood to enable efficient retrieval of information when it is needed and to maintain security and confidentiality.

- Rules should include the use of reference numbers e.g. the NHS number or in the case of corporate records sequenced version numbers etc. and naming conventions e.g. ‘Restricted’ and ‘Confidential’ etc.

Record Maintenance
To control the storage and retrieval of ECCH records and ensure they can be traced whenever required

- The movement and location of records must 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 records transaction. Controls should include either a manual or, where possible, an automated booking out and in system.

- Storage accommodation for paper-based records must be clean, tidy and secure, must prevent damage to records and must provide a safe working environment for staff.

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

- When records are either no longer required or inactive but have not reached the end of their lifecycle in accordance with the Department of Health Records Management: NHS Code of Practice Part 2 retention schedules, every effort must be made to archive them. It is more economical and efficient to store paper – based records in a designated secondary storage area and electronic records, where possible, in compressed format therefore liberating file space for other uses.

- Paper-based Corporate (non-clinical) records are archived by CAS Clarks (See appendix 4)

- Community hospital in-patient and outpatient records are archived within the individual health record of the James Paget University Hospitals Foundation NHS Trust (JPUH)as are records for the Physiotherapy and Occupational Therapy services.

NB: Community Staff must be aware that once community in-patient records are placed in the JPUH records they become part of the hospital records and as such may be disclosed to the patient or their representative under the GDPR without reference to the originator.

For advice and guidance on compressing electronic files please contact the IT Service Desk

Scanning
To determine appropriate procedures for electronic scanning and storage of ECCH records

- For reasons of business efficiency or in order to address problems with storage space, ECCH may consider the option of scanning into electronic format records that exist in paper format. Where this is proposed, the factors to be taken into account include:

  - The costs of initial and then any later media conversion to the required standard, and of the maintenance of any system purchased to provide this service, bearing in mind the length of the retention period for which records are required to be kept.

  - The need to consult in advance with the local Place of Deposit or the National Archives with regard to records which may have archival value, as the value may include the format in which it was created; and

  - The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008)

- In order to fully realize the benefits of reduced storage requirements ECCH should dispose of paper records that have been copied into electronic format and stored in accordance with appropriate standards.

Version Control

- Version control is a process in which a clear audit trail of changes to the policy is created enabling historic references to be made to old versions.

- Version control is managed through the Version control table and should be updated appropriately for each new version of the document.

- The up-to-date version number of the document will be displayed on the front page of the document, and the version control log will provide details of all versions to date. It is the responsibility of the person updating or reviewing the policy to ensure that the correct version number is showing and that the version control log is completed.

- At the drafting stage, the version number will only be updated each time the draft is sent to other parties for their attention / input and changes have been made to the content.

- For all authorised versions of a document, the archiving of the document will take place via the process outlines in section 11d. Most documents will have been created using Microsoft Word. Therefore, it is important that the developmental versions are held in a collated manner by the manager responsible for that particular document and that old copies are not deleted.

Retention and Disposal Arrangements
To dispose of ECCH records at the appropriate time and in a controlled and secure manner

- It is a fundamental requirement that all of ECCH'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 ECCH's business functions.

- ECCH has adopted the retention periods set out in the Records Management: NHS Code of Practice (summarised in Appendix 2). The retention schedule will be reviewed annually.

- It is particularly important under the Freedom of Information legislation that the disposal of records is undertaken in accordance with DoH Records Management: NHS Code of Practice Part 2 Annex D (See appendices 6 and 7) and which must be enforced by properly and trained and authorised staff.

For advice and guidance on disposing of electronic files please contact the IT Service Desk.

Access
To provide clear and efficient access for employees and others who have a legitimate right of access to ECCH records, and ensure compliance with Access to Healthcare Records, Data Protection

- Access is a key part of the records management strategy. Fast, efficient access to records unlocks the information and knowledge they contain. See appendix 5 for information about retrieval of records

- In order to ensure that the requirements of section 4.10 are adhered to, no employee must be able to gain access to records either clinical or corporate (nonclinical) if they do not have a need to know the information that is contained within the record. If an individual, either an employee or patient, or an external agency needs to gain access to an extract of a record then, if the request to view the record is in accordance with GDPR, they must only be allowed to access the relevant extract.

- Computer-based systems must be designed to segregate access to information according to role using username and password credentials to authenticate acceptable use. Ways of ensuring security of access to records include establishing role-based access controls to systems and network drives and ensuring that paper based filing systems are locked away in areas that are not accessible to members of the public and other members of staff.

- Computer-based systems will also ensure the availability of audit trails to meet ECCH managerial requirements. The audit trail, as a minimum, should log details of each significant event in the life of a document in the system. The audit trail should:
  - be generated automatically by the system
  - contain date/time stamps for each event
  - be non-alterable
  - be stored in accordance with the information management policy
  - be subject to appropriate access control
  - be securely stored and backed-up

- Tracking: If appropriate, when records are removed for any reason from the file storage system, their removal and subsequent return should be recorded using a robust tracking system. As a minimum it should include:
  - The unique identifier
  - A description of the item
  - The person or department to whom it is being sent
  - The date of the transfer
  - The date of the return
  - The signature and printed name of the person returning the file

- Where external courier services (other than from an approved listed courier) are used to transfer patient/service user records between health organisations, a formal contract needs to be put in place including ensuring the documents are transported in sealed envelopes (see 8.1). The contract should include confidentiality issues. A schedule of documents should be presented to the courier for signature, which should be cross- checked by the organisation receiving the records. Utilisation of approved courier suppliers should ensure compliance with the above procedures and negate the need for a local contract to be drawn up.

- Medical Records: Employees must only send and ask for medical/health records to be transferred by recorded delivery in an emergency. Approval from the Caldicott Guardian needs to be attained in these circumstances. Registered post should only be used in exceptional circumstances and for minimally sensitive information. Normally, records transferred by internal mail should be sent in a new sealed tamper proof envelope (e.g. Polly Envelope) or purpose made container fitted with security safe tags and marked appropriately (e.g. Welco plastic security container). Procurement department. will be able to assist you in the ordering of such items.

Transporting Records

- Health or social care records or other confidential information for transportation between sites and departments must be enclosed in tamper proof sealed bags/envelopes and clearly labelled with the specific name for whom the package is to be received. For specific situations of extreme sensitivity i.e., child protection, a further statement should be added stating ‘to be opened by addressee only’.

- Larger items can be transported using plastic security containers which are security sealed (refer to the procurement department quoting Welco security transit containers).

- Only new envelopes may be used for internal post/couriers to ensure any tampering is obvious. No re-sealable envelopes to be used unless these contain a security seal. For items of high importance, tamper proof envelopes should be used.

- Records must be carried between sites or departments 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

- Transporting records from NHS premises requires vigilance and the principles of confidentiality must be maintained.

- Transfer of information slips/tracking record slips should be used to record and monitor movement of records.

- Staff may only take records home in exceptional circumstances and where a risk assessment has been undertaken and they have their line managers written approval. The records must be returned to the office on the next working day. Records or other sensitive information should not be left unattended in transit at any time. When carried in a vehicle they must be locked in the boot within a tamper

proof container. This applies to laptops too. Records must not be left in vehicles overnight.

- Staff who take records and other sensitive information home will be responsible for the security and confidentiality of the records which should be kept in a locked secure environment.

Transporting Information held Electronically.

All electronic devices for the purpose of ECCH business will be provided by and managed by the ICT Team, devices will be password protected and secured in line with the latest cyber security requirements. When transporting information held on these electronic 'devices' this could be within a laptop, phone, tablet etc. it is essential that it is transported securely in a designated laptop bag or rucksack, items should never be on display. When laptops are not in use smartcards should be removed from the slot and transported separately. When working away from an ECCH base devices should always be locked when not in use, stowed securely and always kept with you. If you are travelling on public transport, walking or cycling, it is essential that you keep your devices with you at all times. Particular attention should be paid to security of devices whilst transporting it in motor vehicles and includes:

- Vehicles being locked at all times when left unattended.
- Ignition keys should be removed from the interior of the vehicle.
- Electronic devices must always be transported out of sight in the boot area of a vehicle.

Any occurrences regarding loss or theft of your electronic device must be reported immediately to the ICT helpdesk followed by logging an incident.

Audit

To Audit and measure the implementation of the records management strategy against agreed standards

- ECCH will audit its records management practices

- for compliance with this framework. Clinical records must be audited annually (National Health Safety LA Risk Management Standards) and the results reported to the Quality Committee.

- The audit will:
  - Identify areas of operation that are covered by ECCH 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 to related procedures.

- The results of audits will be reported to ECCH Board.

Training

To provide training and guidance on legal and ethical responsibilities and operational good practice for all staff involved in records management

- Effective records management involves employees at all levels. Training and guidance enable employees to understand and implement policies and facilitates the efficient implementation of good record keeping. Where relevant, all employees must receive training in local record keeping and management processes and procedures.

- Any shortfall in compliance with the policy will be:
  - Highlighted and addressed in staff annual appraisals.
  - Have action plans drawn up and implemented.
  - Require evidence of change.

- Deputy Directors and Service Managers are responsible for ensuring their staff have training related to record keeping and record management in their specific areas.

Security

To provide systems which maintain appropriate confidentiality, security, and integrity for records in their storage and use

- Records must be kept securely to protect the confidentiality and authenticity of their contents, and to provide further evidence of their validity in the event of a legal challenge. Similarly, records should only be shared, both inside and outside ECCH, in accordance with the Caldicott principles and relevant legislation.

- Unauthorised disclosure or misuse of information contained in records constitutes a serious breach of conduct that may lead to disciplinary action. Staff must guard against breaches of confidentiality by protecting information from improper disclosure at all times.

- The GDPR, NMC Code of Conduct 2008, Human Rights Act 1998, Administrative law and Common Law Duty of Confidentiality all place responsibility on everyone to maintain confidentiality of personal information. ‘Confidentiality. NHS Code of Practice’ provides further guidance and applies to all NHS employees)

- Basic principles that should be adhered to are as follows:
  - Records should never be left in a position where unauthorised persons can obtain access to them (including computer screens left on but unattended)
  - Only staff who are authorised to access patient/service user records as part of their duties in the provision of care and treatment, or in the carrying out of audit and governance duties, are permitted to do so.
  - The content of records should not be communicated with persons who are not authorised to receive them. They may be discussed on a need-to-know basis only to provide care and treatment to the patient/service user.
  - Employees must not use home IT equipment to write reports or documents involving person or business sensitive information.

Information Sharing

- Recording consent – Patient/service user consent or refusal to share information and any subsequent action taken should be recorded in the patient/service users notes. If information is shared against the patient/service users wishes, the justification for doing so should be noted in addition to who has reached the decision and the date. It is the staff's responsibility to tell patients at the earliest opportunity how their information is treated/used.

- Sharing Information with Professionals – Exchange of records requested by staff within the organisation will normally be dealt with by staff who are known to each other and the service user. If a person is unknown and makes a request, the identity of the person should be checked and if in doubt, advice sought from a service manager.

- Requests for patient/service user information from professionals outside of the Organisation should be in writing to a line manager and contain an explanation of who requires the information, for what purpose and ideally have the patient/service users consent.

- Further details relating to Information Sharing can be found by utilising the following document link: Care Record Guarantee – Connecting for Health

Legal and Professional Obligations

- All NHS records are Public Records under the Public Records Acts. Whilst not subject specifically to this legislation ECCH will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:
  - The Public Records Act 1958;
  - The Data Protection Act 2018;
  - The Information Governance Alliance Records Management of Code Practice - The Common Law Duty of Confidentiality; and - The NHS Confidentiality Code of Practice.

and any subsequent legislation affecting records management as it arises.

8. MONITORING AND REVIEW

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

9. REFERENCES

- The Records Management Code of Practice 2021 https://www.nhsx.nhs.uk/information-governance/guidance/records-managementcode/records-management-code-of-practice-2021/

- The Records Management Code of Practice 2021 Retention Schedule
  (The link will provide access to the 'The Records Management Code of Practice 2021 Retention Schedule'. The table within the link sets out the retention periods for different types of records relating to health and care. The retention periods listed in this retention schedule must always be considered the minimum period. You can browse down all the records in the retention schedule or use the search box and category filter feature to find specific records relevant to your work.)
  https://www.nhsx.nhs.uk/information-governance/guidance/records-managementcode/records-management-code-of-practice-2021/#appendix-ii-retention-schedule

10. ASSOCIATED POLICIES & PROCEDURES *(To include but not limited to)*

- Information Governance Policy & Framework
- Data Protection & Personal Information Handling Policy
- Confidentiality Policy
- Information Governance Policy for SystmOne and Summary Care Record
- (RA)Registration Authority and NHS CRS Smartcard Policy
- Standard Operating Procedures (SOP) for; Using SystmOne Effectively for Record Keeping
- Data Protection & Impact Assessment Policy & Procedure
- Access to Health Records Policy
- Freedom of Information Requests Policy
- IT Security Policy
- Information Security Incident and Incident Investigation Policy
- Mobile Solutions Policy
- Records Management Policy & Procedure
- Record Keeping Policy
- Video Interactive Guidance Policy
- Incident Reporting Policy

11. AUTHOR

DPO

12. APPENDICES

Appendix 1 – Standards for Clinical Record Keeping

These standards apply to all employees: individual directorates, departments and services may have more specific approved standards that must also be adhered to.

- Records will be a factual and accurate account of:
  - The ongoing assessment
  - Care planning
  - Treatment/ care provided
  - Evaluation/ outcome of treatment.

- Decision making/ clinical reasoning should be evident, as should any information given to or discussed with the patient.

- All encounters and interventions relating to a patient must be recording including when a patient has not been involved directly e.g. telephone calls between healthcare professions or with the patient, ordering equipment on behalf of a patient, conversations with relatives and carers.

- Records should demonstrate that where the patient has the capacity to do so, they are actively involved in continuously negotiating and influencing their care, and that relatives/ carers are appropriately with the patients care where patients consent for this to happen.

- Records should demonstrate that valid consent to assessment and treatment was obtained and that patients were offered a chaperone in line with ECCH policy.

- The record must be kept on ECCH recognised stationery and have an organised structure in which all information relating to the patient is filed.

- All documents are to be secured within the health record by the anchorage points (punched holes) using ring binders or similar or treasury tags. No documents are to be loosely filed, stapled, or taped into the health record.

- If any part of the records becomes damaged it must still be retained for legal purposes.

- Entries must be written clearly and legibly in black ink.

- Dictated notes must be typed, and then checked, corrected, and signed by the clinician who dictated them. The accuracy of dictated notes is the responsibility of the author.

- The name of the patient or client must be included on each side of each page (First name in lowercase and then surname in capitals) along with a second identifier. This should be the NHS Number and local reference number e.g., hospital number. Where these are not available the date of birth must be used whilst every effort is made to trace the NHS number.

- Alerts, allergies, and contradictions will be documented prominently at the beginning of any paper or electronic records. If it is felt appropriate to highlight, then only pink highlighter should be used.

- Records will be contemporaneous and written as soon as possible after an intervention.

- All entries will be dated (date, month, and year), and timed (24hr clock) at the beginning of the entry. Where records are written sometime after the intervention, the time of both the intervention and the time of documentation must be recorded.

- There will be a log of signatures and initials of all staff who contribute to clinical records within each directorate, department, and service. Signatory lists will be held by the appropriate executive director or Head of Service and will be made available to internal audit upon request.

- All entries will be signed, and the name and designation printed/ stamped alongside the first entry. If two or more staff are present during the intervention their names must be clearly recorded.

- Where an entry is not signed, the next person to make an entry should record ‘entry above unsigned’.

- Only abbreviations and symbols approved by the ECCH will be used. It is the responsibility of Heads of Department to maintain approved list of abbreviations which is also held by ECCH Headquarters.

- Any alterations or additions are dated, timed, and signed or initialled in such a such a way that the original entry can still be read clearly. A single line should be drawn through any error and correction fluid must not be used in any circumstances.

- Omissions must be written at the time they were realised and not squeezed into the record

- A line should be drawn through any unused areas of the record to prevent entries being made at a later date.

- A departmental policy confirms the arrangements in place to monitor the record entries of support staff e.g., health care assistants, administrative staff, students.

- Test results/ reports must be evaluated and signed by a clinician before being filed. Abnormal results and the action to be taken should be recorded.

Appendix 2 – Minimum Retention Periods for Specific Documents

(The Records Management Code of Practice 2021 - https://www.nhsx.nhs.uk/informationgovernance/guidance/records-management-code/records-management-code-of-practice2021/)

This Appendix sets out the retention period for different types of records relating to health and care. Where indicated, Appendix III should also be referred to. This sets out further detail relating to the management of specific types and formats of records.

The following information is important to ensure the retention schedule is used correctly. The retention periods listed in this retention schedule must always be considered the minimum period.

With justification, a retention period can be extended for the majority of cases, up to 20 years (refer to section five of the Code).

For more information, refer to R v Northumberland County Council and the Information Commissioner (23 July 2015). This provides assurance that it is legitimate to vary common practice or guidance where a well-reasoned case for doing so is made.

Retention periods begin when the record ceases to be operational. This is usually at the point of discharge from care when the record is no longer required for current on-going business, or the patient or service user has died. There are some exceptions to this rule, whereby the retention begins from the date the record is created (for corporate records, such as policies, the retention may start from the date of publication). These are marked with an asterisk (*) in the schedule and may also contain further information in the notes for that entry.

If a record comes back into use during its retention period, then the retention period will reset and begin again from the end of the second period of use. This may mean that records will look as if they are being kept for longer than the retention times stated here, or even maximum periods as suggested by law, but this is acceptable where retention periods reset due to use (refer to section five of the Code).

The actions following review as set out in the schedule are as follows:

- Review and destroy if no longer required: Destroy refers to the confidential and secure destruction of the record with proof of destruction. These will be records with no archival value and there is no longer an ongoing business need to retain them for longer.

- Review and dispose of if no longer required: 'Dispose of' refers to the secure destruction of a record OR the transferral to the appointed Place of Deposits (PoD). for permanent preservation. A certificate of transfer will be provided as proof of transfer (and can act as evidence of disposal). Refer to section five of the Code for further information about permanent preservation.

- Review and consider transfer to PoD: This refers to records that are more likely to be transferred to the PoD, subject to their discussion and agreement about potential accession. Not all records considered for accession will be taken by the PoD. If the record has been offered and declined to be taken, and it has no further retention value, then it must be securely destroyed. Where you have potentially a new series of records for the PoD, you must discuss accessioning them before any action is taken.

- Review and transfer to PoD: This refers to records that should be transferred to the PoD such as trust board minutes and final annual financial report - local agreement will already be in place to accession these.

It is very important that any health and care records are reviewed before they are destroyed. This review should take into account:

- serious incidents which will require records to be retained for up to 20 years as set out in the schedule

- use of the record during the retention period which could extend its Retention

- potential for long-term archival preservation - this may particularly be the case where the records relate to rare conditions such as Creutzfeldt- Jakob Disease records or innovative treatments, for example, new cancer treatments.

If setting a retention period not covered by this Code, there are a number of factors to consider including:

- Legal or regulatory obligations: There may be a specific legal or regulatory reason to keep a record, which may also provide guidance on how long that record needs to be kept to meet that obligation.

- Purpose of the record: The reasons you have created the record may also help define how long you need to keep them for. A record created for medico-legal reasons may need to be for a long period of time, whereas a record created for a specific event that has no post-event actions will attract a short retention period.

- Number of records: The number of records in a series can help you set a retention period. It is worth noting that the number of records is not directly proportionate to a longer retention period (for example, the more records created, then the longer they must be kept). It should also be noted that the number of records is also not indicative of historical value. Due to its type, one record may have historical value, where a series of 200+ records might not.

- Service delivery: The uniqueness or niche way a service is delivered may lend itself to a longer retention period. PoDs can be interested in taking records relating to services that were delivered in a unique way.

- Call or recall of records: If a record or series has a low recall rate, it could be indicative of a shorter retention period. Likewise records that are continually in use may require a longer retention period.

The above list is not exhaustive.

The Records Management Code of Practice 2021 Retention Schedule

(The link will provide access to the 'The Records Management Code of Practice 2021 Retention Schedule'. The table within the link sets out the retention periods for different types of records relating to health and care. The retention periods listed in this retention schedule must always be considered the minimum period. You can browse down all the records in the retention schedule or use the search box and category filter feature to find specific records relevant to your work.)

https://www.nhsx.nhs.uk/information-governance/guidance/records-managementcode/records-management-code-of-practice-2021/#appendix-ii-retention-schedule

Alternatively please use the list below:

CARE RECORDS

Record Type	Retention Period	Disposal Action	Notes
Adult health records not covered by any other section in this schedule (includes medical illustration records such as x-rays and scans as well as video and other formats. Also includes care plans	8 years	Review and consider transfer to Place of Deposits (PoD)	Records involving pioneering or innovative treatment may have archival value, and their long term preservation should be discussed with the local PoD or The National Archives. Also refer to Appendix III: ambulance service records.
Adult social care records	8 years	Review and destroy if no longer required	
Children's records (including midwifery, health visiting and school nursing) - can include medical illustrations, as well as video and audio formats	Up to 25th or 26th birthday	Review and destroy if no longer required	Retain until 25th birthday, or 26th if the patient was 17 when treatment ended.
Clinical records that predate the NHS (July 1948)		Review and transfer to PoD	Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed.
Dental records - clinical care records	15 years	Review and destroy if no longer required	Based on Limitations Act 1980. This applies to all dental care settings and the BSA. This also includes FP17 or FP17O forms.

Dental records - finance related	2 years	Review and destroy if no longer required	These include PR forms. NHS BSA may retain financial records for a minimum of 6 years.
Electronic Patient Record Systems (EPR)	Refer to notes	Review and destroy if no longer required	Where the system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain, demonstrating the destruction, then the Code should be followed in the same way for digital as well as paper records with a log kept of destruction. If the EPR does not have this capacity, then once records reach the end of their retention period, they should be made inaccessible to system users upon decommissioning. The system (along with the audit trails) should be retained for the retention period of the last entry related to the schedule.
GP patient records - deceased patients	10 years	Review and destroy if no longer required	Confidentiality generally continues after death and records should be retained for medico-legal and possible public interest (for example, research) reasons. Review retention after 10 years when possible medicolegal reasons will lapse under requirements of the Limitation Act 1980. Destroy if the record holds no value for researchers. Also refer to Appendix III: GP records.

GP patient records – living patients	Continual retention		If the patient has not been seen for 10 years, or a request for transfer to a new GP has not been received, the GP practice should check the Personal Demographics Service (PDS) for indication of death or other reason for no contact. If there is no reason to suggest no contact, then the record must be kept by the GP practice. If they have died, or transferred to a new practice, transfer the record to NHSE or the new provider respectively. These records cannot be disposed of as they may require further services as they get older. Also refer to Appendix III: GP records

Record Type	Retention Period	Disposal Action	Notes
GP patient records – de-registered cases where the reason is unknown	100 years	Review and dispose of if no longer required	These are cases where the patient has de-registered from the practice, but the reason is unknown. It would be good practice for GPs to check if there is a reason for deregistration (death, missed registration at another practice, emigration etc.). It is not suggested that a retrospective check be carried out, but it would be good practice going forward to conduct a check for these cases. Once checked under General Medical Services (GMS) regulations, records should be sent to NHSE via Primary Care Support England (PCSE) operational processes. Also refer to Appendix III: GP records
GP patient registrations form	6 years after the year of registration	Review and dispose of if no longer required	These need to be kept for 6 years as GP per capita payments are made based on registered patient numbers. Most GP practices scan the form into the patient's electronic record once it is created. The paper form can be destroyed securely once the minimum retention period has been reached, unless there is another reason to keep the form longer (this would be identified at the review stage).

Record Type	Retention Period	Disposal Action	Notes
Integrated records – all organisations contribute to the same single instance of the record	Retain for period of longest specialty	Review and Consider transfer to PoD	The retention time will vary depending upon which type of health and care settings have contributed to the record. Areas that use this model must have a way of identifying the longest retention period applicable to the record.
Integrated records – all organisations contribute to the same record, but keep a level of separation (refer to notes)	Retain for relevant specialty period	Review and consider transfer to PoD	This is where all organisations contribute into the same record system but have their own area to contribute to and the system still shows a contemporaneous view of the patient record.
Integrated records – all organisations keep their own records, but enable them to be viewed by other organisations	Retain for Relevant specialty period	Review and consider transfer to PoD	This is the most likely model currently in use. Organisations keep their own records on their patients or service users but can grant 'view only' access to other organisations, to help them provide health and care to patients or service users
Mental health records including psychology records	20 years, or 10 years after death	Review and consider transfer to PoD	Covers records made under the Mental Health Act (MHA) 1983 (and 2007 amendments). Records retained solely for any person who has been sectioned under MHA1983 must be considered for longer than 20 years where the case is ongoing, or the potential for recurrence is high (based on local clinical judgment). This applies to records of patients or service users, regardless of whether they have capacity or not.

Record Type	Retention Period	Disposal Action	Notes
Obstetrics, maternity, antenatal and postnatal records	25 years	Review and destroy if no longer required	For record keeping purposes, these are considered to be as much the child's record as the parent, so the longer retention period should be considered.
Prison health records	10 years	Review and destroy if no longer required	A summary of their prison healthcare is sent to the person's new GP upon release and the record should be considered closed at the point of release. These records are unlikely to have long term archival value and should be retained by the organisations providing care in the prison, or successor organisations if the running of the service changes hands.
Cancer/oncology records – any patient*	30 years, or 8 years after death	Review and consider transfer to PoD	Retention for these records begins at diagnosis rather than the end of operational use. For clinical care reasons, these records must be retained longer in case of re-occurrence. Where the oncology record is part of the main records, then the entire record must be retained.

Contraception, sexual health, family planning, Genito-Urinary Medicine (GUM)	8 or 10 years	Review and destroy if no longer required	8 years for the basic retention requirement but this is increased to 10 in cases of implants or medical devices. If the record relates to a child, then retain in line with children's records. (Also refer to Appendix III: records dealt with under the NHS Trusts and Primary Care Trusts (Sexually transmitted disease) direct
Creutzfeldt-Jakob Disease – patient records	30 years or 10 years after death	Review and Consider transfer to PoD	Diagnosis records must be retained for clinical care purposes
Human Fertility and Embryology Authority (HFEA) records – treatment provided in licenced centres	3,10, 30 or 50 years	Review and destroy if no longer required	These retention periods are set out in HFEA guidance.
Long-term illness, or illness that may reoccur – patient records	20 years, or 10 years after death	Review and destroy if no longer required	Necessary for continuation of clinical care. The primary record of the illness and course of treatment must be kept where the illness may reoccur or it is a lifelong condition such as diabetes, arthritis or Chronic Obstructive Pulmonary Disease.

Record Type	Retention Period	Disposal Action	Notes
Sexual Assault Referral Centres (SARC)	30 years, or 10 years after death (if known)	Review, and destroy if no longer required	These records need to be kept for medicolegal reasons because an individual may not be in a position to bring a case against the alleged perpetrator for a long time after the event. Once the retention period is reached, a decision needs to be made about continued retention. Records cannot be kept indefinitely just in case an individual might bring a case. Some individuals may never bring a case and indefinite retention may be seen as a breach of UK GDPR (keeping information longer than necessary). Consideration also needs to be given to the Police and Criminal Evidence Act 1984, Human Tissue Act 2004, and Criminal Procedure and Investigations Act 1996 legal requirements (other laws and regulations may also need to be taken into account).

PHARMACY

Record Type	Retention Period	Disposal Action	Notes
Controlled drugs - registers	2 years, (refer to notes)	Review and destroy if no longer required	Misuse of Drugs Act 2001. NHS England has issued guidance in relation to controlled drugs. Also refer to Appendix III: controlled drugs
Controlled drugs - order books, requisitions etc	2 years	Review, and destroy if no longer required	Misuse of Drugs Act 2001.
Pharmacy prescription records	2 years	Review, and destroy if no longer required	A record of the prescription will also be held by NHS BSA and there will be an entry on the patient record. Further advice and guidance on pharmacy records can be found on the Specialist Pharmacy Service website

PATHOLOGY

Record Type	Retention Period	Disposal Action	Notes
Pathology reports, information about samples	Refer to notes	Review and Consider transfer to PoD	This Code is concerned with the information about a specimen or sample. The length of time clinical material (for example, a specimen) is stored will drive how long the information relating to it is retained. Sample retention can be for as long as there is a clinical need to hold it. Reports should be stored on the patient file. It is common for pathologists to hold duplicate records. For clinical purposes, these should be retained for eight years after discharge or until a child's 25th birthday. If information is retained for 20 years, it must be appraised for historical value, and a decision made about its disposal. Also refer to Appendix III: specimens and samples

EVENT AND TRANSACTION RECORDS

Record Type	Retention Period	Disposal Action	Notes
Blood bank register*	30 years minimum	Review and Consider transfer to PoD	Need to be disposed of if there is no on-going need to retain them (such as the currently ongoing Infected Blood Inquiry), subject to any transfer to the PoD.
Clinical audit*	5 years	Review and destroy if no longer required	Five years from the year in which the audit was conducted. This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period, for example, data from adult health records would be kept for 8 years
Chaplaincy records*	2 years	Review and consider transfer to PoD	Also refer to corporate governance records.
Clinical diaries	2 years	Review and destroy if no longer required	Two years after the year to which they relate. Diaries of clinical activity and visits must be written up and transferred to the main patient record. If the information is not transferred from the diary (so the only record of the event is in the diary), then this must be retained for eight years and reviewed. Some staff keep hardback diaries of their appointments or business meetings. If these contain no personal data, they can be disposed of after two years.

Clinical protocols*	20 years	Review and consider transfer to PoD	Clinical protocols may have preservational value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (refer to corporate governance records).
Datasets released by NHS Digital and its predecessors	Delete with Immediate effect	Delete in line with NHS Digital instructions	NHS Digital issue guidance through the Data Access Request Service (DARS) process on the retention and disposal of data released by them.
Destruction certificates, or electronic metadata destruction stub, or record of clinical information held on physical media	20 years	Review and Consider transfer to PoD	Destruction certificates created by public bodies are not covered by a retention instrument (if they do not relate to patient care and if a PoD or The National Archives do not accession them). They need to be destroyed after 20 years.
Equipment Maintenance logs	11 years	Review and destroy and no longer required	
General Ophthalmic services – patient records related to NHS financial transactions	6 years	Review and destroy if no longer required	
GP temporary resident forms	2 years	Review and destroy if no longer required	This assumes a copy has been sent to the responsible GP for inclusion in the GP patient record.
Inspection of equipment records	11 years	Review and destroy if no longer required	
Notifiable diseases book*	6 years	Review and destroy if no longer required	
Operating theatre records	10 years	Review and Consider transfer to PoD	10 years from the end of the year to which they relate.

Patient property books	2 years	Review and destroy if no longer required	Two years from the end of the year to which they relate.
Referrals – NOT ACCEPTED	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record
Requests for care funding – NOT ACCEPTED	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record. NB: These may have potential PoD interest as what the NHS or social care can or cannot fund can sometimes be an issue of local or national significance and public debate. Refer to Appendix III: individual funding requests
Screening* – including Cervical screening – where no cancer or illness detected is returned	10 years	Review and destroy if no longer required	Where cancer is detected, refer to the cancer/oncology schedule
Screening – children	10 years or 25th birthday	Review and destroy if no longer required	Treat as a child health record and retain for either 10 years or up to 25th birthday, whichever is the LONGER.
Smoking cessation	2 years	Review and destroy if no longer required	Retention begins at the end of the 12- week quit period.
Transplantation records*	30 years	Review and consider transfer to PoD	Refer to guidance issued by the Human Tissue Authority
Ward handover sheets*	2 years	Review and destroy if no longer required	This information relates to the ward. Any individual sheets held by staff may be destroyed confidentially at the end of the shift

TELEPHONY SYSTEMS AND SERVICES

This is related to 111 or 999 phone calls or services, Ambulance, out of hours, and single point of contact call centres

Record Type	Retention Period	Disposal Action	Notes
Recorded conversations – which may be needed later for clinical negligence or other legal purposes*	6 years	Review and destroy if no longer required	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980. Further guidance is issued by NHS Resolution.
Recorded conversations – which form part of the health record*	Treat as a health record	Review and destroy if no longer required	It is advisable to transfer any relevant information into the main record, through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record, the recording must be considered as part of the record and be retained accordingly.
Telephony systems record*	1 year	Review and destroy if no longer required	This is the minimum specified to meet NHS contractual requirements.

BIRTHS, DEATHS AND ADOPTION RECORDS

Record Type	Retention Period	Disposal Action	Notes
Birth notification to child health	25 years	Review and destroy if no longer required	Retention begins when the notification is received by the child health department. Treat as part of the child's health record if not already stored within the health record.
Birth registers*	2 years	Review and Consider transfer to PoD	Where registers of all births that have taken place in a particular hospital or birth centre exist, these will have archival value and should be retained for 25 years and offered to the local PoD at the end of the retention period. Information is also held by the NHS Birth Notification Service electronic system, and by ONS. Other information about a birth must be recorded in the care record.
Body release forms*	2 years	Review and destroy if no longer required	

Record Type	Retention Period	Disposal Action	Notes
Death – cause of death Certificate counterfoil*	2 years	Review and destroy if no longer required	These detail the name of the deceased and suspected cause of death (which initially may be different to the final cause of death as stated on the official death certificate). A death notification certificate is issued if a doctor is satisfied there is no suspicious or unexpected circumstances surrounding the death, and the counterfoil retained by the setting that issued the initial cause of death certificate (which is used to obtain the full death certificate from a registrar of births, death and marriages). Cases referred to the coroner would not be able to issue a certificate as the cause would be unknown. These are unlikely to have archival value.
Death – register information sent to the General registry office on a monthly basis*	2 years	Review and Consider transfer to PoD	A full dataset is available from ONS.
Local authority Adoption record (usually held by the LA)*	100 years	Review and Consider transfer to PoD	The local authority Children's Social Care Team hold the primary record of the adoption process. Consider transferring to PoD only if there are known gaps in the primary local authority record, or the records predate 1976. Also refer to Appendix III: adoption records
Mortuary records of Deceased persons	10 years	Review and consider transfer to PoD	Retention begins at the end of the year to which they relate.

Mortuary register*	10 years	Review and consider transfer to PoD	
NHS medicals for adoption records*	8 years or 25th birthday	Review and consider transfer to PoD	The health reports will feed into the primary record held by the local authority. This means that adoption records held in the NHS relate to reports that are already kept in another file, which is kept for 100 years by the relevant agency or local authority. Consider transferring to PoD only if there are known gaps in the primary local authority record or the records pre-date 1976. Also refer to Appendix III: adopted persons health records
Post-mortem records*	10 years	Review and destroy if no longer required	The coroner will maintain and retain the primary postmortem file including the report. Hospital postmortem records will not need to be kept for the same extended time period as (subject to local policy) these reports may also be kept in the medical file.

CLINICAL TRIALS AND RESEARCH

Record Type	Retention Period	Disposal Action	Notes
Advanced medical therapy research - master file	20 years	Review and consider transfer to PoD	
Clinical trials – applications for ethical approval	5 years	Review and consider transfer to PoD	Master file of a trial authorised under the European portal, under Regulation 536/2014. For clinical trials records retention refer to the MHRA guidance. The sponsor of the study will be the primary holder of the study file and associated data. This is based on the Medicines for Human Use (Clinical Trials) Amendment Regulations 2006 (specifically, Regulations 18 and 28).
European Commission Authorisation (certificate or letter) to enable marketing and sale within EU member state's area	15 years	Review and consider transfer to PoD	
Research - datasets	No longer than 20 years	Review and consider transfer to PoD	
Research – ethics committee's and HRA approval documentation for research proposal and records to process patient information without consent	5 years	Review and consider transfer to PoD	This applies to trials where opinions are given to proceed with the trial, or not to proceed. These may also have archival value.
Research – ethics committee's minutes (including records to process patient information without consent)	20 years	Review and consider transfer to PoD	Retention period begins from the year to which they relate and can be as long as 20 years. Committee minutes must be transferred to PoD.

CORPORATE GOVERNANCE

Record Type	Retention Period	Disposal Action	Notes
Board meetings*	Up to 20 years	Review and transfer to PoD	A local decision can be made on how long to retain the minutes of board meetings (and associated papers linked to the board meeting), but this must not exceed 20 years, and will be required to be transferred to the local PoD or The National Archives (for National Bodies).
Board meetings (closed boards)*	Up to 20 years	Review and transfer to PoD	Although these may still contain confidential or sensitive material, they are still a public record and must be transferred at 20 years, and any FOI exemptions noted, or indications that the duty of confidentiality applies.
Chief Executive records*	Up to 20 years	Review and transfer to PoD	This may include emails and correspondence where they are not already included in board papers.
Committees (major) – listed in Scheme of delegation or report direct into the board (including major projects)*	Up to 20 years	Review and transfer to PoD	
Committees (minor) – not listed in scheme of delegation*	6 years	Review and consider transfer to PoD	Includes minor meetings, projects, and departmental business meetings. These may have local historical value and require transfer consideration.

Corporate records of health and care organisations and providers that predate the NHS (July 1948)		Review, and transfer to PoD	Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed. An example might be the minutes of the hospital board from 1932, or midwifery diaries dated Dec 1922.
Data Protection Impact Assessments (DPIAs)	6 years	Review and destroy if no longer required	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one -off, then 6 years from completion
Destruction certificates or record of information held on destroyed physical media	20 years	Review and dispose of if no longer required	Where a record is listed for potential transfer to PoD have been destroyed without adequate appraisal, consideration should be given to a selection of these as an indicator of what has not been preserved.
Electronic Metadata destruction stubs			Refer to destruction certificates
Incidents – serious	20 years	Review and consider transfer to PoD	Retention begins from the date of the Incident – not when the incident was reported
Incidents – not serious	20 years	Review and consider transfer to PoD	These include independent investigations into incidents. These may have permanent retention value so consult with the local PoD. If they are not required, then destroy.
Non-clinical QA records	12 years	Review and destroy if no longer required	Retention begins from the end of the year to which the assurance relates.
Patient advice and liaison service (PALS) records	10 years	Review and destroy if no longer required	Retention begins from the close of the financial year to which the record relates.

Patient surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	May be required again if analysis is reviewed.
Patient surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
Policies, strategies and operating procedures – including business plans*	Life of Organisation plus 6 years	Review and consider transfer to PoD	Retention begins from when the document is approved, until superseded. If the retention period reaches 20 years from the date of approval, then consider transfer to PoD.
Quarterly reviews from NHS trusts	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980
Risk registers	6 years	Review and destroy if no longer required	Forms are anonymous so do not contain PID unless provided in free text boxes. May be required again if analysis is reviewed.
Staff surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
Trust submission forms	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.

COMMUNICATIONS

Record Type	Retention Period	Disposal Action	Notes
Intranet site*	6 years	Review and consider transfer to PoD	
Patient information leaflets	6 years	Review and consider transfer to PoD	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.
Press releases and important internal communications	6 years	Review and consider transfer to PoD	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.
Public consultations	5 years	Review and consider transfer to PoD	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation (particularly where this resulted in changes to the services provided) and so may have historical value.
Website*	6 years	Review and consider transfer to PoD	The PoD may be able to receive these by a regular crawl. Consult with the PoD on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken.

STAFF RECORDS AND OCCUPATIONAL HEALTH

Record Type	Retention Period	Disposal Action	Notes
Duty Roster	6 years	Review and if no longer needed destroy	Retention begins from the close of the financial year
Exposure monitoring information	40 years or 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	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	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	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed, destroy	
Staff record	Keep until 75th birthday (see notes0	Review and consider transfer to PoD	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. Some PoDs accession NHS staff records for social history purposes. Check with your local PoD about possible accession. If the PoD does not accession them, then the records can be securely destroyed once the

			retention period has been reached.
Staff record - summary	Keep until 75th birthday	Review, and consider transfer to PoD	Please see the good practice box staff record summary used by an organisation. Some organisations create summaries after a period of time since the staff member left (usually 6 years). This practice is ok to continue if this is what currently occurs. The summary, however, needs to be kept until the staff member's 75th birthday, and then consider transferring to PoD. If the PoD does not require them, then they can be securely destroyed at this point.
Timesheets (original record)	2 years	Review and if no longer needed, destroy	Retention begins from creation.
Staff training records	See notes	Review and consider transfer to a PoD	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The following is recommended: clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer statutory and mandatory training records - to be kept for ten years after training completed, other training records - keep for six years after training completed

Disciplinary records	Retain for 6 years	Review and destroy if no longer required	Retention begins once the case is heard and any appeal process completed. The record may be retained for longer, but this will be a local decision based on the facts of the case. The more serious the case, the more likely it will attract a longer retention period. Likewise, a one-off incident may need to only be kept for the minimum time stated. This applies to all cases, regardless of format.

PROCUREMENT

Record Type	Retention Period	Disposal Action	Notes
Contracts sealed or unsealed	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
Contracts - financial approval files	Retain for 15 years after the end of the contract	Review and if no longer needed destroy	
Contracts - financial approved suppliers' documentation	Retain for 11 years after the end of the contract	Review and if no longer needed destroy	
Tenders (successful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
Tenders (unsuccessful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	

ESTATES

Record Type	Retention Period	Disposal Action	Notes
Building plans, including records of major building works	Lifetime (or disposal) of building plus 6 years	Review and consider transfer to PoD	Building plans and records of works are potentially of historical interest and where possible, should be kept and transferred to the local PoD
Closed circuit television (CCTV	Refer to ICO code of Practice	Review and destroy if no longer required	The length of retention must be determined by the purpose for which the CCTV has been used. CCTV footage must remain viewable for the length of time it is retained, and where possible, systems should have redaction or censoring functionality to be able to blank out the faces of people who are captured by the CCTV, but not subject to the access request, for example, police reviewing CCTV as part of an investigation.
Equipment monitoring, and testing and maintenance work where ASBESTOS is a factor	40 years	Review and destroy if no longer required	Retention begins from the completion of the monitoring or testing. This includes records of air monitoring and health records relating to asbestos exposure, as required by the Control of Asbestos Regulations 2012.
Equipment monitoring – general testing and maintenance work	Lifetime of installation	Review and destroy if no longer required	Retention begins from the completion of the testing and maintenance

Inspection reports	Lifetime of installation	Review and dispose of if no longer required	Retention begins at the END of the installation period. Building inspection records need to comply with the Construction (Design and Management) Regulations 2015
Leases	12 years	Review and destroy if no longer required	Retention begins at point of lease termination.
Minor building works	6 years	Review and destroy if no longer required	Retention begins at the point of WORKS COMPLETION.
Photographic collections – service locations, events and activities	Up to 20 years	Review and consider transfer to PoD	These provide a visual historical legacy of the running and operation of an organisation. They may also provide secondary uses, such as use in public inquiries.
Radioactive records	30 years	Review and destroy if no longer required	Retention begins at the CREATION of the waste. If a person handling radioactive waste is exposed to radiation (accidental or otherwise), then the records relating to that person must be kept until they reach 75 years of age or would have attained that age. In any event, records must be kept for at least 30 years from the date of dosing or accident. This also includes patients or service users who require medical exposure to radiation, as required by the Ionising Radiation Regulations 2017.
Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhyndrin Test	11 years	Review and destroy if no longer required	Retention begins from the DATE OF TEST.

Surveys – building or installation (not patient surveys)	Lifetime of installation or building	Review and consider transfer to PoD	Retention period begins at the END of INSTALLATION period. (See Inspection reports for legal basis for these records)

FINANCE

Record Type	Retention Period	Disposal Action	Notes
Accounts	3 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate. Includes all associated documentation and records for the purpose of audit.
Benefactions	8 years	Review and consider transfer to PoD	These may already be in the financial accounts and may be captured in other reports, records or committee papers. Benefactions, endowments, trust fund or legacies should be offered to the local PoD
Debtors' records – CLEARED	3 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Debtors' records – NOT CLEARED	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Donations	3 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Expenses	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Final annual accounts report*	Up to 20 years	Review and transfer to PoD	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with board papers for that year to keep a complete set of governance papers.
Financial transaction records	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate

			[Financial transaction records include - VAT Forms for Continence products -which should be kept for 6 years]
Invoices	6 years from end of the financial year they relate to	Review and destroy if no longer required	
Petty cash	2 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate
Private Finance Initiatives (PFI) files	Lifetime of PFI	Review and transfer to PoD	Retention begins at the END of the PFI agreement. This applies to the key papers only in the PFI.
Staff salary information or files	10 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Superannuation records	10 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Contracts	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.

LEGAL, COMPLAINTS AND INFORMATION RIGHTS

Record Type	Retention Period	Disposal Action	Notes
Complaints – case files	10 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the complaint. The complaint is not closed until all processes (including potential and actual litigation) have ended. The detailed complaint file must be kept separately from the patient file (if the complaint is raised by a patient or in relation to). Complaints files must always be separate. (Also refer to Appendix III: complaints records)
Fraud – case files	6 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the case. This also includes cases that are both proven and unproven.
Freedom of Information (FOI) requests, responses to the request and associated correspondence	3 years	Review and destroy if no longer required	Retention begins from the CLOSURE of the FOI request. Where redactions have been made, it is important to keep a copy of the response and send to the requestor. In all cases, a log must be kept of requests and the response sent
FOI requests – where there has been an appeal	6 years	Review and destroy if no longer required	Retention begins from the CLOSURE of the appeal process.
Industrial relations – Including tribunal case records	10 years	Review and consider transfer to PoD	Retention begins at the CLOSE of the financial year to which it relates. Some organisations may record these as part of the staff record, but in most cases, they should form a distinctive separate record (like complaints files).

Litigation records	10 years	Review and consider transfer to PoD	Retention begins at the CLOSURE of the case. Litigation cases of significant or major issues (or with significant, major outcomes) should be considered for transfer. Minor cases should not be considered for transfer. If in doubt, consult with the PoD.
Intel patents, trademarks, copyright, IP	Lifetime of patent	Review and consider transfer to PoD	Retention begins at the END of lifetime or patent, or TERMINATION of licence or action.
Software licences	Lifetime of software	Review and destroy if no longer required	Retention begins at the END of lifetime of software.
Subject Access Requests (SAR), response, and Subsequent correspondence	3 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the SAR.
SAR – where there has been an appeal	6 years	Review and destroy if no longer required	Retention begins at CLOSURE of appeal.

Appendix 3 – Appendix III: How to deal with specific types of records

(The Records Management Code of Practice 2021 - https://www.nhsx.nhs.uk/informationgovernance/guidance/records-management-code/records-management-code-of-practice2021/)

This Appendix provides detailed advice on records management relating to specific types of records for example, transgender records, witness protection records and adopted persons records. These are presented in alphabetical order. It also provides advice on managing certain formats of records, for example, emails, cloud-based records and scanned records.

TYPE OF RECORD Adopted persons health records
Notwithstanding any other centrally issued guidance by the Department of Health and Social Care or Department for Education, the records of adopted persons can only be placed under the new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used but more commonly the birth names are used.

Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure.

It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it were considered appropriate to do so following the adoption.

Ambulance service records
Ambulance service records will contain evidence of clinical interventions delivered and are therefore clinical records. This means that they must be retained for the same time as other acute or mental health clinical records depending on where the person is taken to for treatment. Where ambulance service records are not clinical in nature, they must be kept as administrative records. There is a distinction between records of patient transport and records of clinical intervention. If the ambulance clinical record is handed over to another service or NHS trust, there must be a means by which the ambulance trust can obtain them again if necessary. Alternatively, they can be copied and only the copy transferred, providing this is legible.

Asylum seeker records
Records for asylum seekers must be treated in exactly the same way as other care records, allowing for clinical continuity and evidence of professional conduct. Organisations may decide to give asylum seekers patient or service user held records (section below) or hold them themselves. Patient or service user held

records should be subject to a risk assessment because the record legally belongs to the organisation, and if required, they must be able to get it back. There is a risk that patient or service user held records could be tampered with or altered in an unauthorised way so careful consideration needs to be given to this decision.

Audio and visual records
Audio and visual records can take many forms such as using a dictaphone (digital or analogue) to record a session or conducting a health or care interaction using videoconferencing technologies.

The following needs considering when patient or service user interactions are captured in this way:

- Clinical appropriateness: Organisations should decide when it is appropriate to use audio or visual methods for the provision of health or care. This should be documented in organisational policies and understood by the relevant health and care professionals.
- Retention: If the recording is going to be kept elsewhere (for example, as part of the health and care record) then there is no reason to keep the original recording provided the version in the main record is the same as the original or there is a summary into words which is accurate and adequate for its purpose. If the recording is the only version or instance of the interaction, then it must be kept for the relevant retention period outlined in this Code (for example, adult, child health or mental health retention periods). Some recordings may have archival value (although this is unlikely), and this should be considered on a case-by-case basis.
- Digital continuity: You must consider the medium on which the recording is made and ensure that it is available throughout its retention period (for example, if the system or file format is becoming obsolete, then you will need to migrate it to a newer platform or format to ensure availability). If it is a digital recording and you are looking to store it in the health and care record, ensure the transfer process captures the authenticity of the recording kept.

III: How to deal with
- Storage: Ensure your recordings are stored on systems you control or are provided to you under contract. If stored with the product provider, you must give them (as controller) clear instructions on the storage and retention of those images (for example, delete one month after the date of the recording because it has been summarised into the main health and care record, or retain for 8 years from consultation with the patient or service user, then destroy). Providers acting under contract to a controller are obliged to carry out their written instruction.

- Transparency: You must be transparent with patients and service users regarding the use of audio and visual technology, and associated records, so that they have a reasonable understanding of how they will be used, why, and what will happen with the recording after the interaction. For example, it would be unfair to tell participants that the recordings are deleted if they are not.

Child school health records
Similar to family records (refer to page 94), each child should have their own school health record rather than a record for the school (with consecutive entries) or per year intake. If a child transfers to a school under a different local authority, then the record will also need to be transferred to the new school health service provider. This must only be done once it is confirmed the child is now resident in the new location. The record must be transferred securely. The recipient of the record should contact the sender to confirm receiving the record (if appropriate). If the records are kept on school premises, then access must be restricted to health staff delivering care or other staff who have a legitimate reason to access them.

Local organisations may operate a paper or digital system. Records from other Child Health Teams, following a referral, must be accepted by the receiving organisation regardless of format. This is due to safeguarding risks.

Complaints records
Where a patient or service user complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Detailed complaint information should never be recorded in the health and care record.

A complaint may be unfounded or involve third parties and the inclusion of that information in the health or care record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient or service user and the Health and Care Team. In some cases, it may be appropriate to share details of the complaint with the health and care professional involved in providing individual care in order to make improvements in care delivery. However, there may also be times where the complaint is about an individual but not care related and it might not be appropriate to share details of the complaint with that person, in case further action is required. The Complaints Team should review each complaint on a case by- case basis.

Where multiple teams are involved in the complaint handling, all the associated records must be brought together to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. A complaint cannot be fully investigated if the investigation is based on incomplete information. It is common for the patient or service user to ask to see a copy of their complaint file and it will be easier to deal with if all the relevant material is in one file. Where complaints are referred to the Ombudsman Service, a single file will be easier to refer to.

Health and care organisations should have a local policy to follow with regards to complaints, covering how information will be used once any complaint is raised, and after the complaint has been investigated, regardless of outcome. The ICO has also issued guidance on complaints files and who can have access to them, which will drive what must be stored in them.

Contract change records

Once a contract ends, any service provider still has a liability for the work they have done and, as a general rule, at any change of contract the records must be retained until the time period for liability has expired.

In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision (for current cases) upon termination of the contract. It is also the case that after the contract period has ended, the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

When a service is taken over by a new provider, the records of the service (current and discharged cases) all transfer to the new provider (unless directed otherwise by the commissioner of the service). This is to ensure that the records for the service remain complete and enable patients or service users to obtain their record if they so request it. It also makes the records easier to locate if they are required for other purposes. This will also stop the fragmentation of the archive records for the service and make it much easier to retrieve records.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also include consideration of the identity of the legal entity, which must manage the records.

In some cases, records may end up orphaned. This may happen where the organisation that created them is being disbanded and there is no successor organisation to take over the service or provision. In these cases, orphaned records need to be retained by the highest level commissioner of that service or provision. For example, if a GP practice closes, patients will be offered the choice to register with another nearby practice. When they register with the new practice, the record will follow the patient to that new practice. However, if a practice closes, and the patient does not re-register elsewhere, the record will transfer to NHS England and Improvement, who commission primary care services in England for ongoing management.

Where the content of records is confidential, for example, health and care records, it will be necessary to inform the individuals concerned about the change. Where there is little impact upon those receiving care, it may be

sufficient to use posters and leaflets to inform people about the change, but more significant changes will require individual communications. Although the conditions of UK GDPR may be satisfied, in many cases there is still a duty of confidentiality which may require a patient or service user (in some cases) to agree to the transfer, dependent upon the legal basis and the implications of their choice discussed with them. If the new provider has a statutory duty to provide the service, then consent does not need to be sought. If there is no statutory duty, then consent would need to be sought to satisfy the common law duty of confidentiality.

It is vital to highlight the importance of actively managing records, which are stored in offsite storage (refer to section three of the Code for further information on offsite storage including the importance of completing a DPIA).

These principles and guidance can also apply to non-clinical situations as well, such as when CCGs merge or a trust takes over the running of another one. Annex 1 of this Appendix summarises the considerations and actions required relating to various contract change situations.

Continuing healthcare (CHC) records
Continuing healthcare records can be split into two parts:

- Care record: The care record is the information relating to a patient or service user's care that enables the CHC panel to determine eligibility for CHC based on an assessment of needs. This can be provided directly by the patient or service user or obtained from health and care providers as part of the eligibility process. Consent to obtain this information would be required to satisfy the duty of confidence. The initial checklist completed by the referrer may also contain some level of confidential information and this may also be used to determine eligibility.

- Administrative record: The administrative record is the information used by the CCG to ensure the CHC process runs effectively - an example being appointment letters asking the patient or service user to attend a panel. CCGs require access to health and care information to determine a patient or service user's entitlement (once the CCG has been notified).

CHC activity is covered in law by the 2012 Commissioning Board and NHS CCG Regulations. This means consent is not required to process personal data in relation to CHC but consent will be required to satisfy the duty of confidence. CCGs will need to have systems in place to allow for the safe and secure sharing of patient or service user information with relevant partners as necessary, and to inform patient or service users of how their data will be used as part of this process. Digital viewing and sharing of records may be preferable to paper

copies being printed and used for CHC, due to the risk of accidental loss or disclosure.

CHC records should be kept for the same period of time as adult and child health records, from the date the case is decided by the CHC panel. Where CHC cases relate to mental health, these should be kept for the same period of time as mental health records.

Controlled drugs regime
NHS England, in conjunction with the NHS Business Services Authority, has established procedures for handling information relating to controlled drugs. This guidance includes conditions for storage, retention and destruction of information. Where information about controlled drugs is held please refer to NHS England guidance.
94 95

Duplicate records
The person or team to which the record relates will normally hold the original record however occasionally duplicates may be created for legitimate business purposes. It is not necessary to keep duplicates of the same record unless it is used in another process and is then a part of a new record. Where this is not required, the original should be kept, and the duplicate destroyed. For example, incident forms, once the data is entered into the risk information system, the paper is now a duplicate, and so can be destroyed. Some clinical systems allow printouts of digital records. Where printouts are used, these must be marked as duplicates or copies to help prevent them from being used as the primary record. Evidence required for courts.

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

Family records
Family records used to be common within health visiting teams, amongst others, where a whole family view was needed to deliver care. Whilst these records should no longer be created, they are included here for legacy reasons. Due to changes in the law and best practice, it is not advisable to create a single paper or digital record that contains the care given to all family members. Each person is entitled to privacy and confidentiality, and having all a person's records in one

place could result in a health professional or family member accessing confidential information of another family member accidentally or otherwise.

Good practice would be to create an individual file for each person but with cross references to other family members. This means that each individual has their own record, but health and care professionals can see who else is related to that person, and so can check these records where necessary. Single records also help to protect privacy and confidentiality and (if digital) keep an audit trail of access. General Practitioner records

It is important to note that the General Practitioner (GP) record, usually held by the General Practice, is the primary record of care and the majority of other services must inform the GP through a discharge note or a clinical correspondence that the patient has received care. This record is to be retained for the life of the patient plus at least ten years after death. The GP record transfers with the individual as they change GP throughout their lifetime. Where the patient has de-registered, records should be kept for 100 years since deregistration. A review is taking place to ascertain how long this period should be in the going forwards.

Current guidance advises that the content of paper Lloyd George records should only be destroyed once they have been scanned to the required standard and quality assurance of the scanned images has been completed, confirming that they are a like for like copy of the original paper records. The Lloyd George envelope itself should not be destroyed at the current time and must be kept to meet with the requirements for patient record movement. NHS England undertook a project to cease the creation of Lloyd George envelopes for all new entrants to the NHS, which was implemented in January 2021 (except in limited circumstances). They are also looking at ways to enable destruction of existing Lloyd George envelopes, though this aspect may have a longer implementation timeframe. This Code will be updated as the programme develops.
Individual funding requests (IFRs)

Similar to CHC, IFR cases are mainly administrative records, but also contain large amounts of personal/confidential patient information and as such, should be treated in the same way as CHC records.

As IFRs are unique to an individual, it may be that the care package given to the patient or service user is unique and bespoke to that person. This could mean that the record may have long-term archival value, due to the uniqueness of the care given in this way, and so potentially may be of interest to The National Archives. Local discussions should be held with the PoD to determine the level of local interest, although they would not normally get involved at this level of discussion. It would be a joint discussion on the principle and agreement to archive this type of record and then the responsibility of the health and care organisation to choose individual records that meet this criteria.
96 97

Integrated records
Since 2013, there has been an increase in the number of initiatives promoted and launched that involve integrated records. There has also been recognition nationally that joined up delivery of health and care services can increase the quality of care delivered, and also deliver those services more efficiently.

Examples include:

- NHS England Vanguard Programme
- Sustainability and Transformation Plans (STPs)
- Integrated Care Services (ICS)
- Local Health and Care Records (LHCR)

Depending on the agreements under which integrated records are established these may be subject to the Public Records Act. Generally, if an NHS body is at least partly responsible for the creation and control of the record, it will normally be considered a public record to be managed in accordance with the Act. The relevant PoD should be notified that this is the case. If in doubt, consult with The National Archives.

The options for organisations will depend on what local architecture and systems are already in use. There are three types of retention for integrated records, and suggested retention periods for each.

1. All organisations contribute to a single record, creating the only record for that patient or service user. Consideration must be given to how this is managed in practice (for example, some records will be retained for 8 years and some for 20 years, but they will look the same at face value) (retain for the longest specialty period involved).

2. All organisations pool their records into a single place but keep a level of separation between each type of record (retain for each specialty as applicable – because they are not merged)

3. All organisations keep their own records, but allow others to view their records, but not amend or add to (retain for each specialty as applicable – because they are not merged)

Where organisations are looking to create integrated records, they must enter into a joint controller arrangement, which detail the purpose and method of integrated records. It should also set out how disputes between controllers may be resolved. Information materials for patient or service users must also reflect how their records are used.

Increasingly, where organisations are using this type of system, the information contained within has the potential to be used for purposes other than individual care, such as Population Health Management (PHM). PHM is a tool that is increasingly being used to help plan and prepare care provision in a particular geographical area or specialty. See also the section on Integrated viewing technology and record keeping in the format section below.

NHSX has published an Information Governance Framework for Shared Care Records, which provides further guidance.

Occupational health (OH) records

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. It is permitted for reports or summaries to be held in the main staff record where these have been requested by the employer and agreed by the staff member. When occupational health records are outsourced, the organisation must ensure that:

- staff are aware of the outsourcing and how their information may be used for OH purposes
- the contractor can comply as necessary with data protection and confidentiality requirements
- there is a contract in place with the outsourced provider that has legally binding clauses in relation to data protection and confidentiality
- the contractor can retain records for the necessary period after the termination of contract for purposes of adequately recording any workbased health issues and is able to present them to the organisation if required 98 99

Pandemic records

Health and care organisations will create records as part of a response to a global pandemic. Pandemic events are rare but will nevertheless create records that need to be managed.

Both patient and service user records will be created that detail the care given to people affected by the pandemic. Corporate records will also be created which record business decisions, policies and processes that were taken in response to a pandemic.

These records should be managed in accordance with the retention schedules set out in this code. Organisations should be mindful that a public inquiry (or inquiries) is likely to take place after a pandemic so the pandemic related records could be used or requested as part of that Inquiry. The Government has already agreed to hold a public inquiry into the coronavirus pandemic that began in 2020.

If organisations have created records specifically in response to a pandemic, these should not be destroyed when they have reached their minimum retention

period, unless the public inquiry has ended, or the Inquiry has provided guidance on what type of records it will be interested in. These specific records may have historical value, so discussions should take place with your local PoD. A policy on how to manage a new admission to a care home of an individual with a coronavirus diagnosis may be of interest to the PoD, whereas the care record might not have the same value and should be managed as a health and care record. Any guidance or advice issued by The National Archives or your local PoD in relation to the preservation of pandemic records should be followed.

Patient or service user held records

Some clinical or care services may benefit from the patient or service user holding their own record, for example, maternity services. Where this is considered to be the case a risk assessment should be carried out by the organisation. Where it is decided to leave records with the individual who is the subject of care, it must be indicated on the records that they remain the property of the issuing organisation and include a return address if they are lost. Upon the discharge of the patient or service user, the record must be returned to the health or care organisation involved in the person's care.

Organisations must be able to produce a record of their work, which includes services delivered in the home where the individual holds the record. Upon the termination of treatment, where the records are the sole evidence of the course of treatment or care, they must be recovered and given back to the issuing organisation.

A copy can be provided if the individual wishes to retain a copy of the records through the SAR process. In cases where the individual retains the actual record after care, the organisation must be satisfied it has a record of the contents.

Patient or service user portals

Organisations may implement products that provide patients and service users with access to their records. Access may be either online or via an app or portal. There are increasing numbers of commercial organisations that are providing these products.

The provision of these products must comply with data protection legislation. Health and care organisations must conduct a DPIA if they are considering using such a product. Health and care organisations must remain controller for the patient or service user's information. In most cases, the supplier of the product or system will be a processor as the product facilitates access to the information held by health and care organisations.

Controllers must consider what is relevant and proportionate to include in this type of record. Some information may not be appropriate to add to the portal, for example, harmful information a patient does not know yet because the intention is to let them know in person during a consultation.

Information about the patient or service user must not be uploaded into the product until there is a clear legal basis for doing so, for example, patient consent. Individuals must be provided with information materials so that they can make an informed choice as to whether or not to sign up. The materials should also make it clear what information patients and service users can upload themselves directly to the portal if this is an option. It should also be clear to the patient or service user who controls the information.

Information stored in a product like this should be retained in line with the retention schedules outlined in this Code (for example, adult health records for 8 years after last seen).
100 101

Pharmacy held patient records
These are the records of patients that the pharmacy has dispensed medications to or had some other form of clinical interaction with (for example, given a flu jab) - similar to a hospital or care home patient record.

Records of prescriptions dispensed will be kept by NHS BSA so there is no need to keep a copy of the prescription locally except for audit purposes. Other elements of the pharmacy record, for example, vaccinations provided, should be viewed in the same way as a patient record, and should be destroyed 8 years after the last interaction with the patient. However, if there is a need to keep the record for longer, then this can be extended up to 20 years, provided there is a justified, documented and approved reasons for doing so. Information materials for patients should also be reflective of the organisation's retention period.

Prison health records
In 2013 responsibility for offender health in HM Prison Service transferred from the Ministry of Justice to NHS England. A national computer-based record was created to facilitate the provision of care and the transfer of care records associated with inmate transfers throughout imprisonment.

A significant number of paper records remain, and some offender health services operate a mix of paper and digital records. Prison records should be treated as hospital episodes and may be disposed of after the appropriate retention has been applied. The assumption is that a discharge note has been sent to the GP. Where a patient or service user is sent to prison the GP record (or social care record) must not be destroyed but held until the patient is released or normal retention periods of records have been met.

Prison health records may have archival value, but this is the exception rather than rule. Records should be kept in line with the same period as for deregistered GP records, with a view to further retention (with justification) and a potential transfer to a PoD, subject to their approval.

Private patients treated on NHS premises

Where records of individuals who are not NHS or social care funded are held in the record keeping systems of NHS or social care organisations, they must be kept for the same minimum retention periods as other records outlined in this Code. The same levels of security and confidentiality will also apply.

Public health records
A local authority normally hosts public health functions, but the functions still involve the handling of health and care information. For this reason, public health functions are in the scope of this Code. Where clinical information is being processed by the public health function it is expected to comply with the NHS Digital Code of Practice for Confidential Information.

Records relating to sexually transmitted diseases
Organisations that provide care and support under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000 must be aware of the additional obligations to confidentiality these impose on employees and trustees of organisations. These organisations include NHS Trusts, CCGs, local authority public health teams and those providing services under NHS contracts.

This obligation differs from the duty of confidentiality generally because it prohibits some types of sharing but enables sharing where this supports treatment of patient or service users. For this reason, it is common for services dealing with sexually transmitted diseases to partition their record keeping systems to comply with the directions and more generally to meet patient or service users' expectations that such records should be treated as particularly sensitive.

Secure units for patients detained under the Mental Health Act 1983
Mental health units operate on a low, medium and high-risk category basis. Not all patients on these units will have been referred via the criminal justice system. Some patients may be deemed a risk under the Mental Health Act and will need to be accommodated accordingly. Some patients may be high-risk due to the nature of a crime they have committed because of their mental health and therefore will need to be treated in a high secure hospital, such as Broadmoor.

As such, their records should be treated in the same way as other mental health records including retention periods (20 years, and longer if justified and permitted) and final disposal. A long retention time may also help staff at these units deal with subsequent long-term enquiries from care providers.
102 103

Sexual assault referral centres
Sexual assault referral centres (SARCs) are highly specialised forensic and health services co-commissioned by Police and Crime Commissioners and NHS England and Improvement. SARCs support the physical, mental health and wellbeing of service users and collect forensic evidence pertaining to alleged sexual offences.

Records generated may include forensic medical examination notes, body maps, photographic records, and DNA intelligence. Reports or statements on these records may be required as evidence in a court of law, and the records management process must facilitate this. Based on relevant guidance, legal and regulatory obligations, a minimum retention period of 30 years for SARC records has been applied by NHS England and NHS Improvement. This retention period reflects the severity of the alleged offence; the length of time for the potential bringing of criminal justice proceedings and right to appeal; and the potential for cold case review. Retaining records beyond 30 years is acceptable provided there is ongoing justification and the decision is documented and approved by the relevant committees responsible for the SARCs operational delivery.

Specimens and samples

The retention of human material is covered by this Code because some specialities will include physical human material as part of the patient or service user record (or linked to it). The record may have to be retained longer than the sample because the sample may deteriorate over time. Relevant professional bodies such as the Human Tissue Authority or the Royal College of Pathologists have issued guidance on how long to keep human material. Physical specimens or samples are unlikely to have historical value and so are highly unlikely to be selected for permanent preservation.

The human material may not be kept for long periods, but that does not mean that the information or metadata about the specimen or sample must be destroyed at the same time. The information about any process involving human material must be kept for continuity of care and legal obligations. The correct place to keep information about the patient is the clinical record and although the individual pathology departments may retain pathology reports, a copy must always be included on the patient record. Physical specimens or samples do not have to be stored within the clinical record (unless designed to do so) but can be stored where clinically appropriate to keep the material, with a clear reference or link in the clinical file, so both the material and the clinical record can be joined together if necessary.

Staff records

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the information collected through the recruitment process and this will include the job advert, application form, evidence of the right to work in the UK, identity checks and any correspondence relating to acceptance of the contract.
The central HR file must be the repository for this information, regardless of the media of the record.

It is common practice in some health and care organisations for the line manager to hold a truncated record, which contains portions of an employee's employment history. This can introduce risk to personal information (as it is duplicated), but also potentially expedient to do so. Organisations considering

whether to use, or discontinue using, local HR files, should complete a risk assessment.

Information kept in truncated staff files should be duplicates of the original held in the central HR file. If local managers are given originals as evidence (such as a staff member bringing in a certificate of competence) they should take a copy for local use and the original should be kept with the main HR file. It is important that there is a single, complete employment record held centrally for reference and probity.

Upon termination of contract (for whatever reason), records must be held up to and beyond the statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS or organisational business purposes, in accordance with Retention Instrument 122. Usually this relates to inpatient ward areas, where the ward manager will keep a small file relating to the training and clinical competencies of ward staff. Where there is justification for long retention periods or protection is provided by the Code, this will not be in breach of GDPR Principle 5. (Refer to section 5 of the Code for further information about retention of records).

Some organisations operate a weeding system, whereby staff files are culled of individual record types that are now time expired (such as timesheets). Others have just kept the whole file as is and archived it away until 75th birthday. It is not recommended to change your system from one to the other because:

- the effort involved would be disproportionate to the end result
- if you begin to weed files, you would need to do this retrospectively to all files, to avoid having two types of central HR file
- you cannot reverse the weeding process – if you decide to keep full records, it is impossible to remake historically weeded files complete again

Both systems are acceptable, regardless of media. It is noted that organisations may have a hybrid system of paper historical staff files and digital current staff files. If possible, organisations should consider moving all their files into one format to create consistency.

Where an organisation decides to use a summary, it must contain as a minimum:

- a summary of the employment history with dates
- pension information including eligibility
- any work-related injury
- any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- professional training history and professional qualifications related to the delivery of care

- list of buildings where the member of staff worked, and the dates worked in each location

Good practice for a staff record summary:
Staff record summary contains the following fields:

- name
- previous names
- assignment number
- pay bands
- date of birth
- addresses
- positions held
- start and end dates
- reasons for leaving
- building or sites worked at

Disciplinary case files should be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record, as it may be pertinent to have an indication to the disciplinary case, but the full details and file must be kept separately from the main file.

With regards to staff training records, it can be difficult to categorise them to determine retention requirements but keeping all the records for the same length of time is also hard to justify. It is recommended that:

- clinical training records are retained until 75th birthday or six years after the staff member leaves, whichever is the longer
- statutory and mandatory training records are kept for ten years after training is completed
- other training records are kept for six years after the training is completed The Chartered Institute for Personnel and Development, and the ICO have provided further information and advice on the retention of HR records.

Transgender patient's records
Sometimes patients change their gender and part of this may include medical care. Records relating to these patients or service users are often seen as more sensitive than other types of medical records. While all health and care records are subject to confidentiality restrictions, there are specific controls for information relating to patients or service users with a Gender Recognition Certificate. The use and disclosure of the information contained in these records is subject to the Gender Recognition Act 2004, (GRA) which details specific restrictions and controls for these records. The GRA is clear that it is not an offence to disclose protected information relating to a person if that person has

agreed to the disclosure. The GRA is designed to protect trans patient and service user data and should not be considered a barrier to maintaining historic medical records where this is consented to by the user.

There are established processes in place with NHS Digital for patients undergoing transgender care in relation to the NHS number and the closing and opening of new Spine records. In practice, nearly all actions relating to transgender records will be based on explicit consent. Discussions will take place between the GP and the patient regarding clinical care, what information in their current record can be moved to their new record and any implications this decision may have (for example, they may not be called for a gender specific screening programme). Patients should be offered ways to maintain their historical records. This could include editing previous entries and removing references containing previous names and gendered language. Any decisions made regarding their record must be respected and the records actioned accordingly.

Any patient or service user can request that their gender be changed in a record by a statutory declaration, but the Gender Recognition Act 2004 provides additional rights for those with a GRC. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Panel issues a Gender Reassignment Certificate. At this time a new NHS number can be issued, and a new record can be created, if it is the wish of the patient or service user. It is important to discuss with the patient or service user what records are moved into the new record and to discuss how to link any records held in any other health or care settings with the new record, including editing previous records to remove names, gender references or details. The content of the new record will be based on explicit consent under common law.

However, it is not essential for a transgender person to have a GRC in order to change their name and gender in their patient record and receive a new NHS number. They do not need to have been to a Gender Identity Clinic, taken any hormones, undergone any surgery, or have a Gender Recognition Certificate. Under the Equality Act (2010), Transgender people share the protected characteristic of ‘gender reassignment’. To be protected from gender reassignment discrimination, an individual does not need to have undergone any specific treatment or surgery to change from their birth sex to their preferred gender. This is because changing physiological or other gender attributes is a personal process rather than a medical one. An individual can be at any stage in the transition process – from proposing to reassign their gender, to undergoing a process to reassign their gender or having completed it.

Protected persons health records

Where a record is that of someone known to be under a protected person scheme, the record must be subject to greater security and confidentiality. It may become apparent (via accidental disclosure) that the records are those of a person under the protection of the courts for the purposes of identity. The right to

anonymity extends to health and care records. For people under certain types of protection, the individual will be given a new name and NHS Number, so the records may appear to be that of a different person.

Youth offending service records
Due to the nature of youth offending, it is common for very short retention periods to be imposed on the general youth offending record. For purposes of clinical liability and for continuity of care the health or social care portion of the record must be retained as specified in this Code, which will generally be until the 25th birthday of the individual concerned.

Cloud-based records
Use of cloud-based solutions for health and care is increasingly being considered and used as an alternative to manage large networks and infrastructure. NHS and care services have been given approval to use cloud-based solution, provided they follow published guidance from NHS Digital and information on GOV.UK.

Before any cloud-based solution is implemented there are a number of records considerations that must be addressed as set out by The National Archives. The ICO has issued guidance on cloud storage. Organisations must complete a DPIA when considering using cloud solutions.

Another important consideration is that at some point the service provider or solution will change and it will be necessary to migrate all of the records, including all the formats, onto another solution. Whilst this may be technically challenging, it must be done, and contract provisions should be in place to do this.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever-increasing storage instead of good records management will not meet the records management recommendations of this Code. For example, if digital health and care records are uploaded to cloud storage for the duration of their retention period, then they must contain enough metadata to be able to be retrieved and a retention date applied so it can be reviewed and actioned in good time.

Personal data that is stored in the cloud, and then left, risks breaching UK GDPR by being kept longer than necessary. This information would also be subject to Subject Access process, and if not found or left unfound, would be a breach of the patient or service user's rights.

Email and record keeping implications
Email is widely accepted as the primary communication tool used every day by all levels of staff in organisations. They often contain business (or in some cases clinical) information that is not captured elsewhere and so need to be

managed just like other records. The National Archives has produced guidance on managing emails.

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

The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Solutions such as email archiving and ever-larger mailbox quotas do not encourage staff to meet the standard of storing email in the correct business context and to declare the email as a record.

Where email archiving solutions are of benefit is as a backup, or to identify key individuals where their entire email correspondence can be preserved as a public record.

Where email is declared as a record or as a component of a record, the entire email must be kept, including attachments so the record remains integral - for example, an email approving a business case must be saved with the business case file. All staff need to be adequately trained in required email storage and organisations need to:

- undertake periodic audits of working practice to identify poor practice
- have a policy in place that covers email management - including the appraisal, archiving and disposal of emails
- take remedial action where poor practice or compliance is found

Automatic deletion of email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information, even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation. Legal holds can take many forms and records cannot be destroyed if there is a known process or a reasonable expectation that records will be needed for a future legal process such as:

- local inquiries into health or care issues
- national inquiries
- public inquiries
- criminal or civil investigations
- cases where litigation may be reasonably expected, for example, a patient has indicated they will take the organisation to court
- a SAR (known or reasonably expected)
- a FOI request (submitted or reasonably expected)

This means that no record can be destroyed by a purely automated process without some form of review whether at aggregated or individual level for continued retention or transfer to a PoD.

The NHSmail system allows a single email account for every staff member that can follow the individual through the course of their career. When staff transfer from one NHS organisation to another NHS organisation, they must ensure that no sensitive data relating to the former organisation is transferred. It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of classified information. This is facilitated by staff storing only emails that need to be retained on an ongoing basis. Emails that are the sole record of an event or issue, for example, an exchange between a clinician and a patient, should be copied into the relevant health and care record rather than being kept on the email system or deleted.

Instant messaging records

Health and care services are increasingly using instant messaging apps or platforms to share patient and service user information between health and care professionals or to contact patients or services users in a transactional way, such as appointment reminders. NHSX has published guidance on this issue. Instant messaging apps or platforms should not be used as the main, or primary, record for a person. Where possible, information shared in this way also needs to have a place in the health or care record of that person. This could be a printout of the exchange; contents transcribed into the record; or a progress note accurately covering the exchange entered into the record. If the app or platform is the only place that information is stored, then it must be managed in line with this Code.

Transactional messages, such as GP appointment reminders or pharmacy notifications that your prescription is ready for collection, have a short shelf-life and will no longer be needed once the appointment is attended or prescriptions collected. Organisations that use these systems should keep a record of messages sent to a person, in case they are needed later (such as proof that the patient was reminded of their appointment), but once it is clear that the purpose of the message has been fulfilled, there is no requirement to keep these messages.

Integrated viewing technology and record keeping

Many record keeping systems pool records to create a view or portal of information, which can then be used to inform decisions. This in effect creates a single digital instance of a record, which is only correct at the time of viewing. This may lead to legacy issues, especially in determining the authenticity of a record at any given point in the past. When deciding to use systems that pool records from different sources, organisations must be assured that the system can recreate a record at a given point in time, and not just be able to provide a view at the time of access. This will enable a health or care provider to show what information was available at the time a decision was made. Consideration should also be given to the authenticity and veracity of the record, particularly if there is conflicting information presented by two or more contributors to the record. Some conflicts

may be easier to resolve than others (for example, a person has a different address with two systems), however more complex conflicts would require organisations to have a process or procedure to agree how to resolve these.

Scanned records
This section applies to health and care records as much as it does to corporate records. When looking to scan records, organisations need to consider the following:

- the scanned image can perform equally as well as the original paper
- scanned images can be challenged in court (just as paper can)
- ability to demonstrate authenticity of the scanned image
- ensure technical and organisational measures are in place to protect the integrity, usability and authenticity of the record, over its period of use and retention
- discussions need to take place with the local PoD over records that may be permanently accessioned - they will need input into the format of the transferring record
- where the hard copy is retained, this will be legally preferable to the scanned image

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or digital, can be admissible as evidence.

The Archives and Records Association has produced a flow chart to support scanning processes. The British Standards Institution has published a standard that specifies the method of ensuring that electronic information remains authentic. The standard deals with both ‘born digital’ and scanned records. The best way to ensure that records are scanned in accordance with the standard is to use a supplier or service that meets the standard following a comprehensive procurement exercise, which complies with NHS due diligence. Using an BSI10008 accredited supplier, or an in-house accredited service would be seen as best practice.

For local scanning requirements or for those records where there is a low risk of being required to prove their authenticity, organisations may decide to do their own scanning following due diligence and internal compliance processes. This may require a business case to be drawn up and approved, and procurement rules followed to purchase the necessary equipment.

Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original, unless the format of the original has historical value, in which case consideration should be given to keeping it with a view to permanent transfer. Where paper is disposed of post-scanning, this decision must be made by the appropriate group or committee. A scan of not less than 300 dots per inch (or

118 dots per centimetre) as a minimum is recommended for most records although this may drop if clear printed text is being scanned. Methods used to ensure that scanned records can be considered authentic are:

- board or committee level approval to scan records
- a written procedure outlining the process to scan, quality check and any destruction process for the paper record
- evidence that the process has been followed
- technical evidence to show the scanning system used was operating correctly at the time of scanning
- an audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- fix the scan into a file format that cannot be edited Some common mistakes occur in scanning by:
- only scanning one side and not both sides, including blank pages - to preserve authenticity, both sides of the paper record, even if they are both blank, must be scanned (this ensures the scanned record is an exact replica of the paper original)
- scanning a copy of a copy - leading to a degraded image
- not using a method that can show that the scanned record has not been altered after it has been scanned – questions could be raised regarding process and authenticity
- no long-term plan to enable the digitised records to be stored or accessed over the period of their retention

Once you have identified digital records that are suitable for accessioning to your local PoD or The National Archives (for national bodies, it is recommended to follow published The National Archives guidance on the accessioning of digital records.

Social media

Organisations must have approved policies and guidance when using social media platforms. It is acknowledged that social media will mainly be used for promoting activities of the organisation, rather than as a way of communicating care issues or interventions with patients or service users. Information posted on social media may also be classed as a corporate record and appropriate retention periods set where applicable.

Information posted on social media (such as details of upcoming meetings, or published policies) will usually be captured elsewhere in an organisation’s corporate records’ function, and where this is the case, there is no value in retaining the information held in the social media platform, as it will be a duplication of the corporate records management function.

The National Archives have begun to capture social media content of NHS bodies that have a national focus, such as NHS England and Improvement. Where requested, this can also be extended to local NHS bodies, but this would be the exception not the rule.

Website as a business record

As people interact with their public services, more commonly it is the internet and websites in particular that provide information, just as posters, publications and leaflets once did exclusively. A person's behaviour may be a result of interaction with a website and it is considered part of the record of the activity.

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate or there must be some other method to recreate what the website or intranet visitor viewed. It may be possible to arrange regular crawls of the site with the relevant PoD but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record. The UK Government Web Archive (part of The National Archives) undertook two central crawls of all NHS sites in 2011 and 2012 and may have captured some from 2004 onwards but the information captured will not include all levels of the sites or some dynamic content.

National NHS organisations have their websites regularly captured by The National Archives and can (upon request) capture local organisation's websites, where regional information would be captured that would not necessarily go to the local PoD (such as a CCG closing down). Local Authorities' websites are not87 routinely captured by the WebArchive Team at The National Archives, but they can do so in exceptional circumstances and if requested by the Authority.

Appendix 4 – Copying Letters to Patients

Patients have a right to be able to receive copies of clinicians' letters about them. To enable safe compliance of this requirement the following standards will be adopted:

- Patients will be asked, at initial assessment and at regular intervals thereafter, to identify whether they would like to receive a copied letter and in what format.
- All clinical correspondence will contain the patient's NHS Number
- Letters that contain identification of a third party also require the consent of that party before the information is released.
- Letters that should be copied to patients include:
    - Letters or form of referral
    - Letters from NHS health professionals to other agencies
    - Letters to Primary Care, hospital consultants or other professionals - Letters should not be copied:
    - When a patient does not want a copy
    - Where the clinician feels that it may cause harm to the patient e.g.: child protection or mental health issues
    - Where the letter includes information about a third party who has not given consent
- The patient must consent to receiving the letter and the person responsible for generating the letter should for ensuring provision is made for obtaining that consent.
- Clinical staff will avoid unnecessary technical terminology. If necessary, the content of the letters will be explained to patient and this explanation documented.
- When the patient has identified, they would like to receive copies of letters, this will be recorded in the patient's record.
- For those patients identifying they wish to receive copies of letters, it will be documented that a copy of the letter has been sent to the patient.

Appendix 5 – Conventions Associated with Electronic Records Management

Introduction

The principles for naming, labelling and structuring records should be used for the management of electronic records. The purpose of good Records Management in the working environment is to:

- establish and maintain a structure through which records are kept
- enable authorised colleagues to access records
- enable the fulfilment of legal and operational requirements
- prepare records for long-term storage / archives by labelling them whilst they are current, using current knowledge and expertise

It is the responsibility of senior management, in conjunction with their staff, and mindful of the organisation's policy, to determine the ways in which records generated by the department will be named and catalogued.

Conventions for names, standard terms, filing structures and cataloguing systems must be the same across all records irrespective of format. However, the following points should be considered with regard to electronic records.

Naming conventions: documents and folders
Conventions for naming electronic documents must be co-coordinated with those for naming electronic folders, so that a document title does not contain information already present in the folder in which it is filed. Naming conventions must strike a balance between keeping titles short and keeping titles useful; using specific titles and grouping items under broader titles

Document creators, dates of creation and modifications including version numbers, must makeup the composition of a document title. In addition, the aforementioned information must also be reflected throughout a documents be using footers.

Principles of naming conventions:

- Names should be kept clear and as brief as possible
- Easy to introduce, follow and extend
- Logical, consistent, and easy to remember

Standard terms:
Standard terms and forms of name must be used wherever it is sensible to do so. This should apply to:

- Names of organisations, departments, and people (job titles)
- Names of projects, functions, activities

- Document types, topics

Standard phrases should be:

- Sensible and short
- standardized across the organisation and preferably in common use
- be whole words; avoid acronyms, abbreviations

Length and readability in titles and pathways

In the electronic environment, folder structures tend to contain more folders each containing fewer documents than occurs in the paper environment. This can lead to a greater depth in the folder structure itself. The length of folder (and document) titles can become an issue where a long pathway is built up through the folder hierarchy. In most cases, an average of about 16 - 20 characters is adequate, care must be taken to avoid repetition and redundancy. Long folder titles lead to very long pathways for an individual document, with the possible result that the relevant information is not available to the right people at the right time.

Version control

Consistent naming rules can link different versions of the same document, by including a version number as part of the title. This will also help to provide an audit trail for future tracking of document development; but does depend for success on disciplined use and careful tracking of versions. There is a danger of inconsistency if a document version is updated separately by different users without co-ordination, so that varying versions may exist each with different parts, but neither with all, of the full updated content. Well-developed and robust procedures must be implemented for control of document versions in a multi-user environment. Accurate version numbers must be used to indicate the version of a document.

Attachments

Staff may add the following attachments to mail messages:

- Word
- Excel
- Power Point presentations
- Text documents

Staff may not send:

- Executable files (applications or files containing macros)
- Screen savers
- Movie files of any description
- Recreational/joke attachments
- Any other files likely to breach the security of ECCH’s or receiving sites’ security

Patient Information/Personal Staff Information/Confidentiality

It is not permitted to send person identifiable and/ or business confidential information by external email unless specifically sanctioned by the ECCH's Information Governance lead. Access to other staff's email is restricted and will only be granted on written request from a Service Manager or a Director of ECCH. Person identifiable and business confidential data must not be distributed to employees who have no need to know about the information they contain.

At no time will an employee inappropriately disclose confidential or sensitive information to any other individual or organisation, be they NHS employees or not, by means of the Internet.
The user will not inappropriately disclose personal information about employees or patients of the ECCH to any individual via the Internet. No information that could be used to identify a specific individual will be passed via the Internet, i.e., demographics, NHS Numbers, National Insurance numbers or similar, unique sets of symptoms or unique sets of personal circumstances.

Employee Privacy
Employees cannot expect any email messages composed, received, or sent on the ECCH's networks to be for private viewing only. In order to protect ECCH action from inappropriate material being circulated all mail is automatically scanned. Should a problem be suspected, the message will be marked for human intervention. This may mean the mail is read in-transit. Employees should understand that this is common business practice and will almost certainly also occur at the receiving end.

Penalties for breach of this policy or the common law will result in disciplinary action being considered

Appendix 6 – The Archive and Retrieval of Corporate Records: Protocol

Access to CAS Clark archiving services is controlled by Estates & Facilities – all requests for access must be made via ecch.estatesandfacilitieshelp@ecchcic.uk

Required Information

Name:	Joe Blogs
Site:	Hamilton House
Email Address:	j.blogs@ecchcic.uk Password:
Password of your choice Access Level:	

ECCHTH	Therapies (Physio etc.)
ECCHCH	Community Hospitals
ECCHSG	Safeguarding
ECCHFI	Finance
ECCHSL	Speech & Language Therapy
ECCHHR	Human Resources

Estates will obtain from CAS Clark a username, which will be emailed to you with a copy of the instructions: - latest version:

1. Label each box with the corresponding label from CAS – Each label will have its own identification number e.g., TH10123 (Label ordering guidance below.)

   Subgroup: Physio
   Period: 2017 - 2018
   Description: Referrals, A – Z

2. NOTE: Keep your own record for each box number including details of what is within. (If you need to recall a box you will have to refer to your own records.)

3. Once all sections have been completed add each box to the “Basket”.

4. (Check your basket to ensure all boxes you want collecting are listed.)

5. Ensure that each box is closed securely for transport.

6. From your basket select “process basket” where you will be able to edit/update your delivery/collection details. Complete your site information and select delivery type standard.

7. NOTE: Collections/deliveries for ECCH are every Tuesday.

8. Please ensure, where necessary you include special instructions e.g. If your site does not open until 10am.

9. To complete click “Submit request”

TO ORDER MORE BOXES, LABELS or SACKS
Email: boxtransfer@archive-storage.com
Please specify the number of boxes and/or labels required, in multiples of 10 and confirm delivery address.

FORGOTTEN PASSWORD or LOG-IN
Email: ecch.estatesandfacilitieshelp@ecchcic.uk
For Deceased Patient Records Prior to 1/1/2000
Ancora

For advice and guidance on archiving electronic files please contact the IT Service Desk on either:

- 01502 719 550
- ict@ecchcic.nhs.uk

Appendix 7 – Protocol for the Permanent Disposal of Records

In line with organisational policy, all directorates must keep comprehensive catalogues that detail the nature of records placed into off-site storage.

Provider Services
District Nursing
Human Resources
In-Patient care
Occupational Therapy
Physiotherapy
Podiatry

For advice and guidance on the permanent disposal of electronic files please contact the IT Service Desk on either 01502 719 550 or ict@ecchcic.nhs.uk

Appendix 8 – The Safe Disposal of Confidential Waste: Protocol*

The Freedom of Information Act 2000 (FOI) confers a responsibility on public authorities to store and make available, subject to certain exemptions contained within the Act, information that they generate. Virtually everything that the ECCH does, pending any request for release under the terms of the Act, should be regarded as information in confidence.

Staff in all disciplines keep prime files both in order to discharge daily business properly and meet the organisation's responsibilities under FOI, and the retention and disposal of these prime documents is the subject of this policy. However, in order to facilitate meetings many copies of documents are made and circulated to committee members. It is copies of documents such as these committee papers that will form confidential waste if members feel no lasting need to construct files of their own on any given subject.

Locked blue bins are provided for the safe disposal of this ad-hoc confidential waste, which are removed on a weekly basis and the contents destroyed by Confidential Data Shredding Services.

Metal tags, paperclips, and staples should be removed from documents before placing them in Confidential Waste bins.

Staff who identify a need for a similar facility at sites other than headquarters are asked to discuss their needs with the Office Manager at Beccles HQ - Telephone 01502 719500, who will make the necessary arrangements.

***NB: Clearly, patients' records, in use at a great many of the ECCH's premises, are confidential, but their safe disposal will ordinarily be governed by the retention schedules earlier referred to within the policy, following a period of archiving**

See also Appendix 9 for the management of electronic records

Appendix 9 – Management of Electronic Records

Introduction

- An electronic records management system is the only viable way to gain control over the number of records in existence and those being created on a daily basis. The physical records file room, while still in existence, is being replaced by the virtual records file room, which is actually thousands of desktops, network storage devices, and portable media.

- This Appendix concentrates on the management of electronic records, recommending the controls by which the principles expressed below can be made concrete and achievable by defining what needs to be done. The structure broadly follows the natural lifecycle of the record. It addresses five topics:
    - the need for procedures and how these can be developed from policy
    - creation and capture of electronic documents into record-keeping systems
    - keeping and management of electronic records within record- keeping - systems
    - inventory control, appraisal, selection, and disposal of electronic records - long-term and permanent preservation, and transfer to appropriate archives.

- Effective electronic records management works hand-in-hand with effective records management to achieve common aims. It does so by creating a closer fit between user behaviour in handling information, record-keeping requirements and organisational development, and in demonstrating the value which electronic records add to the enterprise and to government as a whole. Records management is concerned with gaining control over the recorded information which any institution needs to do business – and is therefore vital to the continuing success ECCH.

Principles

- Electronic records must be maintained to ensure that the content, context, and structure is accessible, comprehensible, and managed for as long as record keeping requirements determine.

- ECCH should protect its electronic records from inappropriate or unauthorised access.

- Electronic records must be maintained for as long as record keeping requirements determine, without loss of information. appropriate.

- For so long as the data or may be required by ECCH, electronic records must be backed-up at appropriate intervals and that back-up stored securely in such a manner as to be readily available in the event it is needed to effect recovery
- Electronic records of continuing value should be migrated through successive upgrades of hardware and software in such a way as to retain the context, content and

structure and the integrity of the electronic records created in earlier systems, utilising approved technological standards.

- Electronic records must be disposed of in a secure manner when no longer required to ensure they cannot be restored, recovered, or recreated.

Procedures and Practices

- Access
  - Access to electronic records will be managed in accordance with the relevant ECCH Policies and standards, including this Policy.
  - Access will be restricted to appropriately authorised individuals.
  - Where appropriate, electronic records will be protected by appropriate encryption in accordance with NHS standards.

- Retention
  - Electronic records will be retained in accordance with the specific requirements to be found in Appendix 2 to this Policy.

- Back-up & Archiving
  - Computer systems will be backed-up to appropriate electronic media at prescribed intervals in accordance with user needs, based on an agreed Recovery point Objective (RPO).
  - Back-up will be securely stored at a location where the media can be accessed in the event of a serious disruptive incident denying access to data processing facilities.
  - Electronic records no longer required on a day-to-day basis but still within the retention period prescribed in Appendix 2 will be copied to a secure archive for long-term storage.

- Data Compatibility
  - Stored and archived data will be maintained in such a manner as to ensure compatibility with the current hardware and software configuration of ECCH IT systems.
  - Care must be taken to ensure that, where more than one copy of a record may exist, all copies are destroyed at the same time, including both primary and working copies.
  - Electronic records will be disposed of in such a manner as to ensure:
    - Records are not permanently erased before the retention date specified in accordance with Appendix 2 of this Policy
    - Electronic information is appropriately authorised for disposal
    - Once destroyed, data cannot be restored or recreated by any means.

For advice and guidance on backing-up or disposing of electronic files please contact the IT Service Desk on either 01502 719 550 or ict@ecchcic.nhs.uk

Audit Trails

- Where appropriate, electronic records will be supported by audit trails according to the risks associated with specific data. These will record details of all additions, changes, deletions, and viewings. Typically, the audit trail will include information on:
    - who – identification of the person creating, changing or viewing the record;
    - what – details of the data entry or what was viewed;
    - when – date and time of the data entry or viewing; and
    - where – the location where the data entry or viewing occurred.

- Audit trails are important for legal purposes as they enable the reconstruction of records at a point in time. Without its associated audit trail, there is no reliable way of confirming that an entry is a true record of an event or intervention.

13. EQUALITY & DIVERSITY IMPACT ASSESSMENT

In reviewing this policy, the Group considered, as a minimum, the following questions:
- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so is this planned?

Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, sexual orientation.

Blank version of the full Equality & Diversity Impact assessment can be found here:

http://eccho/Home/FormsGuidance.aspx?udt_575_param_index=E&udt_575_param_page=2

14. DOCUMENT CONTROL

Version Date	Version No.	Author/ Reviewer	Comments
May 2012	1	IG Admin	ECCH Policy created from NHSN and N&W
July 2013	2	Q&A Team	
June 2016	3		4.7.5 CAS Clarkes added 4.7.7
May 2018	4	DPO	Updated for GDPR
July 2019	5	DPO	4.12.9 removed as no longer relevant
April 2022	6	Risk & IG Team Lead DPO	Updated to new policy template added policy statement, scope, references and associated policies and procedures. Updated in line with Records Management Code of Practice 2021 – retention Appendix 2 & 3 updated.
November 2022	7	Head of Corporate Governance and Risk Management	VAT forms archiving clarification added to retention schedule.
December 2023	8	Head of Corporate Governance and Risk Management	Review of policy. Added section on page 17 - Transporting Information held Electronically.
October 2025	9	Head of Corporate Governance and Risk Management	Review of policy no changes required

DOCUMENT CONTROL SHEET

Name of Document:	ECCH Records Management Policy & Procedure
Version:	9
File Location / Document Name:	ECCHO
Date Of This Version:	October 2025
Produced By (Designation):	Data Protection Officer
Reviewed By:	Caldicott & Information Governance Group
Synopsis And Outcomes of Consultation Undertaken:	No adverse impact identified
Synopsis And Outcomes of Equality and Diversity Impact Assessment:	No adverse impact identified
Ratified By	Caldicott & Information Governance Group
Date Ratified:	27/10/2025
Distribute To:	ECCHO– Intranet
Date Due for Review:	October 2028
Enquiries To:	Data Protection Officer
Approved by Appropriate Group/Committee	✓ Date: 27/10/2025 Caldicott & Information Governance Group