Essex Partnership University
NHS Foundation Trust

STORAGE, RETENTION AND DESTRUCTION OF RECORDS PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG9c
VERSION NUMBER	**2 (previously 7 under old numbering)**
KEY CHANGES FROM PREVIOUS VERSION	Removed all reference to records libraries Incorporated the possibility to retain records for longer than the required period Updated processes
AUTHOR	Records Manager
CONSULTATION	Information Governance Steering Committee Quality Committee
IMPLEMENTATION DATE	August 2017
AMENDMENT DATE(S)	August 2018; July 2021
LAST REVIEW DATE	July 2021
NEXT REVIEW DATE	July 2024
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE	June 2021
RATIFIED BY QUALITY COMMITTEE	July 2021
COPYRIGHT	

PROCEDURE SUMMARY

The purpose of this procedure is to ensure that the destruction of health and corporate records is compliant with the Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016, Public Records Act 18

The Trust monitors the implementation of and compliance with this procedure in the following ways:

This process is monitored via the Information Governance Toolkit and assurance reports are submitted to the Information Governance Steering Committee

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this Procedure is Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

STORAGE, RETENTION AND DESTRUCTION OF RECORDS PROCEDURE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE. BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THAT SECTION.

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

STORAGE, RETENTION AND DESTRUCTION OF RECORDS PROCEDURE

Assurance Statement

The purpose of this procedure is to ensure that the destruction of health and corporate records is compliant with the Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016, Public Records Act 1958

The implementation of these guidelines will ensure that the Trust stores, retains and disposes of records in accordance with current legal requirements and best practice.

1.0 INTRODUCTION

1.1 Records are a valuable source of information, and the intelligence they contain is vital to the quality of patient care and treatment, and provides evidence of the Trust's business decisions made.

1.2 Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016 states that *"records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time".*

1.3 The Trust may decide to keep records longer than the recommended minimum period, according to the reasoning behind its own retention schedules. However records should not be destroyed earlier than the recommended minimum period.

1.4 In 2013 the government confirmed that historical records (the Trust will decide if any records are considered to be of historical value to the public), are to be stored at The National Archives, (TNA) or Local Place of Deposit, (LPoD) after 20 years instead of 30 years. The move to a '20-year rule' represents a major change for public records and replaces the '30-year rule'.

2.0 PURPOSE

2.1 These guidelines refer to the minimum retention periods for all health and corporate records and details the minimum standards for record storage facilities in line with the relevant legislation and guidance.

3.0 LEGAL POSITION

3.1 All NHS records are public records under the Public Record Act 1958/1967, under the terms of guidance issued by the Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016

3.2 The Trust has reviewed this guidance and agreed minimum retention periods for all Trust records in line with Section 4 of the Code of Practice.

3.3 All NHS organisations have a legal responsibility to maintain records safely and securely under Article 5 of the Data Protection Act 2018.

3.4 The preservation of Trust records can be divided into two distinct categories:

- Records requiring permanent preservation
- Records to be retained for minimum periods

3.5 These guidelines refer to NHS records of all types regardless of the media on which they are held, including:

- Patients health / medical records (electronic, digital, paper based) across all specialties
- Administrative records (personnel, estates, financial and accounting, notes associated with complaint handling, etc.)
- X-ray, imaging reports, photographs, slides and other images
- Microfilm, microfiche
- Audio and video tapes, cassettes, CD-ROM, etc.
- E-mails
- Digital records
- Computerised records

3.6 The use of health and corporate records as a legal document places specific requirements upon the Trust to meet minimum periods of retention. The length of retention depends upon the type of record and its importance to the business of the organisation. For further details staff should refer to the Records Management Code of Practice: Section 4 (Appendix 1 of this Procedure).

4.0 ROLES AND RESPONSIBILITIES

4.1 All Trust staff have a responsibility for records management, and should refer to the Trust Records Management Policy (CP9) for full details of how to manage the Trust's records.

4.2 The Director with responsibility for records (the Executive Chief Finance and Resourcing Officer) is responsible for Trust wide and strategic management of records. In addition the Trust has nominated officers (Head of Electronic Systems & Records / Records Manager) – responsible for ensuring compliance with the Trust's policy on the retention / preservation of records. These officers also have the responsibility to ensure that records are stored and destroyed in line with Trust policy / procedure.

4.3 All staff are responsible for the storage and confidentiality of records within their area of activity. Existing records must be stored securely and appropriately referenced, and quality assurance standards should be maintained for digitally scanned records in line with the Trust's best practice.

4.4 The Head of Electronic Systems & Records / Records Manager is responsible for co-ordinating any archiving with the local records managers / service managers / administration staff with responsibility for records and the Trust's nominated supplier / storage facility.

4.5 The Head of Electronic Systems & Records and the Director with responsibility for records will be responsible for liaising, where required, with the Public Records Office.

4.6 The Information Governance Manager will be responsible for ensuring that all information breaches in relation to the storage, retention and destruction of records are investigated and reported in line with Trust procedures to the Caldicott Guardian \ Senior Information Risk Owner.

5.0 RECORDS CLOSURE

5.1 Records must be closed as soon as they have ceased to be in active use other than for reference purposes i.e. (Dormant flag can be used). An indication that a file of paper records or folder of electronic records has been closed must be shown on the record itself, as well as noted in the index, database of the file folders / Trust information systems

5.2 Wherever possible, information on the intended disposal of electronic records must be included in the metadata when the record is created.

5.3 The storage of closed or non-current records awaiting disposal must follow accepted standards relating to environment, security and physical organisation of the files. In any event, public records must not ordinarily be kept for more than 20 years (calculated from the last entry date on the file), without being transferred to a local place of deposit[1]. If the Trust has reason to retain the records for more than 20 years (other than for statutory or active administrative purposes) it must contact the National Archive (or the LPoD[1]) for advice. Records chosen for archive must be dealt with by following the Trust's Records Management Policies and Procedures.

5.4 All staff are responsible for the safety and security of any person identifiable, confidential and/or sensitive information that is to be transported. Records must be in secure tamper proof bags, and in vehicles out of sight from the public, placed in the boot, if in a car. External contractor transportation must always meet the same Trust standards. Once transported to a LPoD the security of the records becomes the responsibility of the new keeper.

6.0 RECORD STORAGE FACILITIES

6.1 The following guidelines, based on BS5454: 2000, 'Recommendations for Storage and Exhibition of Archival Documents', must be applied to all record storage areas (archive and central 'active' records) across the Trust or held within external storage facilities on behalf of the Trust.

The LPoD for Essex records is the Essex Records Office at Essex County Council and for Bedford records it is Bedfordshire Archives Services in Bedford.

6.2 Central Record libraries (Archive)

Situation/Construction

6.2.1 The siting must not be subject to any hazard from external sources including neighbouring buildings or properties.

6.2.2 The store must be of robust construction of brick, stone or concrete, with protection against unauthorised entry, fire, flood, damp or pest.

6.2.3 The floor should be capable of bearing the weight of the records stored and the type of shelving chosen.

6.2.4 Plumbing and drains in or above or adjacent to the storage room should be avoided. There must be no pipe work containing water or other liquids positioned above the storage.

6.2.5 Any materials used should be a minimum of flammable finishes and fixtures.

6.3 Security

6.3.1 The perimeter of the storage room must be secure against unauthorised entry and vandalism.

6.3.2 The doors must be strong and fitted with mortise deadlocks or security locks and keys must be strictly controlled by archival staff.

6.3.3 Windows should be protected by bars or mesh especially on ground floors.

6.3.4 Alarms should be used to protect against intruders out of normal working hours. All alarms including fire alarms must be connected to the appropriate emergency services.

6.3.5 Access should be restricted to records staff and other authorised staff employed by the organisation.

6.3.6 A suitable CCTV system must be in place.

6.3.7 All storage transport vehicles must be unmarked in terms of contents (e.g. not say confidential storage items being transported) and must be locked and secured when not in use.

6.4 Fire Protection

6.4.1 Automatic smoke detectors and fire alarms should be fitted throughout the stores.

6.4.2 Fire extinguishers must be provided with advice from the fire prevention officer.

6.4.3 Lighting should be by fluorescent tube fitted with diffusers.

6.4.4 Smoking should be prohibited.

6.5 Environment & Storage

6.5.1 Constant temperatures should be maintained in line with the Records Management Code of Practice Parts I and II.

6.5.2 Shelving should possess sufficient load bearing strength for the items to be stored.

6.5.3 Films should be stored in dust free metal cabinets.

6.5.4 Tapes should be stored in metal, cardboard or inert plastic containers, placed vertically on metal shelving.

6.5.5 Records retrieved from archive - should be securely kept at the service or unit. Cabinets / drawers / rooms containing confidential records must be kept locked or electronically stored where available

6.5.6 Electronic records must be stored on shared drives and not on local C:\ drives (this includes Desktop, My Documents, etc.).

6.6 Electronic Records

6.6.1 All records stored on the Trust's electronic records systems will need to follow both system / manufacturer guidance and also trust policies and be in line with BS: 100008 Legal Admissibility

7.0 PERMANENT PRESERVATION OF RECORDS

7.1 Documents detailing major changes within the provision of health care, research and those of specific organisational historical data, may be of public interest and therefore suitable for permanent preservation.

7.2 Examples of records requiring permanent preservation are as follows: - (List is not exhaustive)

- Documents detailing history of the Trust
- Major events/notable events. (e.g. major incidents, including pandemics, or substantial changes in the provision of local healthcare)
- Major projects and plans (e.g. opening of new buildings; healthcare plans/strategies)
- Industrial Relations documents
- Documents detailing research work / development (these may include health records.

7.3 The appropriate directorate Director will be responsible for identifying to the Head of Electronic Systems & Records, those records that may require permanent preservation at the point they are to be archived.

7.4 Those records identified for permanent preservation should not be included in an 'ordinary' archive box of records but should be passed to the Head of Electronic Systems & Records as individual items.

7.5 The Head of Electronic Systems & Records Manager will be responsible for identifying records for permanent preservation. .

7.6 Once identified and selected the Trust Executive Team will be required to authorise final preservation in line with the national Information Governance Records Management Code of Practice

7.7 Local county councils already possess many of the original documents relating to important changes in the provision of local healthcare. Close co-operation is required between the nominated officers and the LPoD to ensure samples of records are transferred at the appropriate time to the Public Records Offices, Chelmsford and Bedford. The Public Records Office must be advised, by the nominated officer, of the type and nature of any record held by the Trust in excess of 20 years of age.

8.0 RECORDS TO BE RETAINED

8.1 Records Not Requiring Permanent Preservation

The Trust's agreed minimum retention time for non-permanent records is shown in the summary guidance at Appendix 1, to ensure that the Trust meets its statutory duties and may provide evidence in case of future litigation

8.2 The agreed time-scales balance the need to retain records and the resources available to meet the costs of storage. It is also recognised both nationally and locally that some documents may be destroyed before notification of a legal claim has been registered.

8.3 General correspondence, memos, emails etc. not directly related to any of the categories identified should be retained for a maximum of three years. Local judgement should be used to determine the minimum retention period, particularly where storage space is limited.

9.0 RETRIEVAL OF RECORDS

9.1 Active Records

9.1.1 Only authorised staff have permission to request retrieval of active records. These may be administration staff, health professionals involved with the patient, medical secretaries and the Head of Electronic Systems & /Records / Records Manager. All requests to be sent to [redacted]

9.1.2 All records must be replaced in their original place of deposit when no longer required and the system updated.

9.2 Archive Records – see below for supplier specifics

9.2.1 Suppliers / external storage companies will be reviewed for suitability by the Head of Electronic Systems & Records, and Trust's Records Manager with the Contracts Department, decide on the approved supplier for archiving services in line with Trust policy for tendering / contracts.

9.2.2 Only authorised staff have permission to retrieve archive records. These may be the Head of Electronic Systems & Records or the designated person(s) at the external record library. Teams / individuals requiring the return of archived records must, in writing to [redacted] request retrieval through the local processes as agreed with the Head of Electronic Systems & Records.

9.2.3 All requests for record retrieval must be via email to [redacted] and must include details of the archived box number and / or file barcode number), budget code and address for delivery. This information will be obtained from the original archive record sheet, which will be held locally by individual teams / services.

9.3 Returning Records to Archive

9.3.1 All requests for returns to the archive facility must be via email to [redacted] and contain the information as in 9.2.2 above.

9.4 Records Requests for off-site storage

9.4.1 All requests for records to be archived via the Trust's offsite storage providers are administered by the dedicated records staff and records e-mail address, [redacted]
Local procedures are available from the dedicated records staff.

9.4.2 As instructed in the local procedure, barcodes will need to be used to both identify the boxes and the individual health files. Corporate files do not require file barcodes. A list should be maintained of the records contained in each box on the specific templates. This applies to both corporate records and health records.

9.4.3 The lists of records are sent to the [redacted] e-mail address where the dedicated records staff then transfers this information onto a main catalogue of stored records.

9.5 Records Requests from off-site storage – Retrieval from Archive

9.5.1 All requests for records to be retrieved from archive via the Trust's offsite storage provider are administered by the dedicated records staff and records e-mail address [redacted]

9.5.2 Using the designated templates, and completing as instructed this form is sent to [redacted], where the dedicated records staff will request the relevant records directly from the offsite storage provider.

10.0 DESTRUCTION OF PAPER BASED RECORDS

10.1 This section of the procedure should be read in conjunction with the Trust's Confidential Waste Procedure.

10.2 The Head of Electronic Systems & Records / Records Manager will be responsible for ensuring that the destruction of scanned and or paper records is carried out once all quality assurance checks have been validated and the Director with responsibility for records has authorised such destruction.

10.3 The Trust retains responsibility for ensuring confidentiality throughout all stages of the destruction process and any contractor employed to remove records must demonstrate satisfactory safeguards against accidental loss or disclosure.

10.4 At all stages during the destruction process confidentiality must be fully maintained. The Trust's preferred method of destruction, therefore, will be by incineration or shredding only.

10.5 Following destruction of any health records, all Certificates of Destruction must be forwarded to the Head of Electronic Systems & Records / Records Manager who will be responsible for maintaining the records of destruction, in line with the Information Governance Alliance Code of Practice, Section 4,

10.6 The Head of Electronic Systems & Records / Records Manager or their representative will provide confirmation of destruction at the Information Governance Steering Committee. This information will be in the form of number of boxes / records destroyed (paper), and not by individual file name. For electronically held records destruction will be maintained within the specified parameters in the Trust's electronic system as determined by this procedure.

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

10.8 There will be the need to retain records for a longer period where direct instruction is given to the Trust for various reasons i.e. relevant national enquiries, legality reasons, investigations etc. These will be advised by the Executive Team and disseminated out to all staff.

11.0 DESTRUCTION OF ELECTRONIC RECORDS

11.1 This section of the procedure must be read in conjunction with the Trust's Scanned Records Quality Control to Disposal Procedures Electronic records due for deletion from the Trust's electronic scanning system are strictly controlled by technical restrictions for access, controlled by passwords and smart cards, with different access levels according to the status of the user.

11.2 A log of electronic records destroyed must always be maintained, showing the reference number, description and reason for deletion.

12.0 REFERENCE TO OTHER POLICIES AND PROCEDURES

12.1 When processing records in any capacity reference should be made to any Trust policies relating to records as well as to local and professional guidance.

12.2 Other documentation will include:

- Records Management Policy (CP9)
- Data Protection Act 2018 and Confidentiality Policy / Procedure
- Information Sharing and Consent Procedure
- Secure Handling and Disposal of Confidential Waste Procedure
- Scanned Records Quality Control to Disposal Procedures

END