

Policy and procedure

Records – preservation, retention and destruction

Key messages

- All staff must comply with the [retention and destruction schedule](#) before destroying any records (paper or electronic).
- All departments must have a local retention and destruction schedule in place for records that are not identified in the Trust retention and destruction schedule.
- Any records not identified by the Trust or local retention and destruction schedule should be referred to the local records manager before destruction.
- Once the retention period has been reached the record should be destroyed in line with the Trust's [waste disposal policy](#) and [waste disposal procedure](#).

1 Scope

This policy applies to all Trust employees, including:

- staff who hold honorary contracts
- contractors working on behalf of the Trust
- the board of governors
- non-executive directors.

2 Purpose

- To inform staff of the Trust requirements in relation to retention and destruction and what is expected of them.
- To ensure that the Trust complies with the relevant legislation and codes of practice.

3 Definitions

3.1 Corporate record

A corporate record is defined as 'recorded information (excluding health records), in any media, which has been created or gathered as a result of any aspect of the work of all Trust employees.'

3.2 Health record

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

4 Introduction

This document will apply to all information recorded and held by the Trust, both corporate and health records in any format. This document provides the procedures for the preservation, retention and destruction of all Trust records both corporate and health records.

5 Responsibilities

5.1 Chief executive

The chief executive has overall responsibility for record management in the Trust. As accountable officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

5.2 Board responsibility

The director of information, systems and analysis is responsible for raising issues to the Trust board as appropriate.

5.3 Head of patient services

The head of patient services has lead responsibility for records management across the Trust.

5.4 Information governance lead

The information governance lead ensures compliance with the information governance toolkit. Oversees the work programme to ensure that all requirements are met.

5.5 Data awareness manager

The data awareness manager is responsible for ensuring that this policy is implemented throughout the Trust and processes are developed, coordinated, monitored and reviewed and for providing advice, assistance, and training to all staff.

5.6 Senior managers

The senior managers are responsible for ensuring that their staff complies with this policy and procedure.

Information governance

Information systems and analysis directorate

5.7 Local record managers (LRM) (nominated by senior managers within each department)

LRMs are responsible for ensuring that staff within their directorate/ department are informed and comply with this policy and procedure and to ensure that a local retention and destruction schedule is in place and that this is reviewed on a regular basis.

5.8 All staff

All staff must ensure that they comply with this policy and procedure. Records should be retained as per the agreed Trust [retention and destruction schedule](#) and local retention and destruction schedule.

5.9 Trust archivist

The Trust archivist is responsible for maintaining the Trust archives and processing requests for access to this material.

6 Preservation, retention and destruction of records

6.1 Retention and destruction schedule

The Trust has an approved Trust [retention and destruction schedule](#) in place that identifies the retention periods for a number of records.

In addition, all departments will have an approved local retention and destruction schedule in place that identifies all unique records created and held within the department that are not listed on the Trust [retention and destruction schedule](#). Departments are required to make the decision as to how long this information is required to operate the business and service of the department.

Local records managers are responsible for maintaining the local retention and destruction schedule and ensuring that a copy of the most up to date schedule is sent to the data awareness manager.

The local retention and destruction schedule should be regularly reviewed but as a minimum at least every two years.

[Appendix 1](#) outlines the process for producing/ reviewing a local retention and destruction schedule.

6.2 Appraisal of records

Records should be appraised in line with the Trust [retention and destruction schedule](#) and the local retention and destruction schedule to determine whether they should be retained or destroyed.

Records not identified on either of these schedules should be reviewed every five years. If the records have been retained for 30 years since the year that

Information governance

Information systems and analysis directorate

they were created then they should be considered for permanent preservation and passed to the archivist for preservation.

6.3 Records for permanent preservation

If material is in a category selected for permanent preservation, the original document must be preserved. Further guidance on this can be obtained from the Trust's archivist.

The records that should be permanently preserved are indicated in the Trust [retention and destruction schedule](#).

Records should be passed to the archivist no later than thirty years after their creation. Arrangements can be made directly with the archivist to pass records to the public records deposit earlier than this if appropriate.

If a record is identified for permanent preservation but is not listed on the Trust's [retention and destruction schedule](#), the nominated LRM should be contacted. The LRM will then liaise with the Trust archivist and data awareness manager to make a decision on the permanent preservation of this record.

6.4 Records that are the subject of a request for information under the Freedom of Information Act 2000

It is essential that all records that are the subject of a request for information under the Freedom of Information Act 2000 should be retained until the processing of the request for information is completed. Departmental data awareness representatives will inform the relevant staff not to destroy any information relevant to the request until otherwise informed.

6.5 Destruction of records that are not identified on the Trust or local retention and destruction schedule

For all records that need to be destroyed, that are not identified on either the Trust or local retention and destruction schedule, a review should take place as to whether the record should be retained.

The LRM should be contacted and if the destruction of the record(s) is appropriate the LRM will authorise the destruction. The LRM will log all decisions to destroy the records, recording:

- the title and description of the record
- the date of the request to destroy the record
- the reason destruction has been requested
- the date authorisation was given to destroy the record.

This log will be maintained by the LRM.

If authorisation is not given to destroy the record(s), the LRM will advise the member of staff of this decision. A decision will be made by the LRM as to

how long this record should be retained for. This record should then be included in the department's local retention schedule.

6.6 Retention and destruction of health records

The Trust has a non-destruction policy for all patient records excluding records of deceased patients and accident and emergency cards.

All health records should be destroyed eight years following the date of death with the exception of:

- children who have died in infancy/ childhood aged less than 25 years. These records must be kept until the date which would have the child's 25th birthday
- all records of mothers of the above who can be identified as such (obstetric and general records)
- obstetric and psychiatric records must be kept for 25 years and 20 years respectively regardless of whether that patient has died or not
- any individual records identified by consultant medical staff as 'do not destroy'.

Deceased patient's records are archived off site for a period of eight years, or, in the case of children up to 25 years. They are archived by type of record eg child, study, obstetric and acute and in date of destruction order. Medical records maintains a database of records, which is stored off site. Requests for the retrieval of archived notes from off-site storage should be made to medical records on extension 6613/ 3713.

Accident and emergency cards which are not filed in the casenotes because the patient was neither admitted to the hospital nor had a follow up outpatient appointment are kept in the emergency department for three months. These are then removed to the F & G basement for a further two and a half years. After this date they are archived off site for a period of eight years or in the case of children 25 years. The emergency department holds a record of all accident and emergency cards stored off site. Cards that are over eight years old, except for those held for children, are destroyed.

Personal health records of patients were microfilmed from 1972 to 1987.

Personal health records of patients who had not attended Addenbrooke's for four years were microfiched from 1990 to March 1996. Personal health records identified by consultants as 'do not microfiche' are excluded.

From 1998 an image has been created of all health records of patients who have not attended for four years. Once the records have been imaged then the hard copy is incinerated. Images are viewed via the electronic medical records system (eMR). All obstetrics records for delivered babies are held electronically, viewable by eMR excluding the most recent pregnancy that is held in paper in the acute case notes. Other imaged records are available on eMR and users are advised via reference in the paper case notes where to locate the record.

Information governance

Information systems and analysis directorate

6.7 Retention and destruction of research records

Research records should be retained in accordance with the Trust's [retention and destruction schedule](#) and any guidance applicable to the specific research.

6.8 Destruction of electronic records

Records held in a network folder/ email server must be deleted from the system (and from the recycle bin). For records held on mobile devices, if the mobile device is being reused then the record should be simply deleted from the device. If the device and its records are no longer of any use, it must be disposed of securely in accordance with the [waste disposal policy](#).

6.9 Destruction of paper records

Paper records that contain personal identifiable or business confidential information must be destroyed securely by:

- placing in a confidential bin
- shredding
- placing in a black plastic sack and contacting estates and facilities on extension 2696 to arrange collection.

Records that are not confidential can be destroyed locally in waste bins (please note waste from waste bins is treated like domestic waste and goes to landfill sites). Please refer to the [waste disposal policy](#) and [waste disposal procedure](#) for more information.

6.10 Disclosure of information

At any stage in a record's life cycle a record's author can ask the data awareness manager to review the record, to establish if an exemption under the Freedom of Information Act 2000 is appropriate that would close the record or part of the record from disclosure for a period of time or permanently. Any decision to close a record would be recorded on the record.

7 Monitoring compliance with and the effectiveness of this policy

Compliance with this policy including the NHSLA Risk Management Standard 1.8 requirements in relation to the process for retention, disposal and destruction of records will be monitored as follows:

Key standards to be monitored:

- records are retained, disposed of and destroyed as per the retention and destruction schedules
- that all departments have in place a local retention and destruction schedule.

The above standards will be monitored by the information governance team and medical records staff by the following means:

Corporate records

- local records managers (LRMs) will be required to undertake an annual retention and destruction audit
- the data awareness manager (or nominated representative) will issue a checklist/ audit sheet to each LRM to complete and return on an annual basis
- an action plan, specific to each local area, will be produced by the data awareness manager as appropriate and sent to the LRM
- compliance with the action plan will be monitored by the data awareness manager in conjunction with the LRM
- the results of the audits and actions plans will be reported to the information governance steering group
- reports are sent to the information services project board (ISPB) and the board for information.

Health records

- a quarterly audit ensuring correct retention, disposal and destruction of health records is undertaken by medical records. The medical records coordinator spot checks that records within the confidential disposal bags have been tracked on the hospital information support system ([HISS](#)) accordingly ie 'destroyed' / 'disked' and are destroyed in accordance with this policy. The results of the audit are summarised in the health records quarterly report presented to the medical records review group (MRRG) on a quarterly basis
- the MRRG is responsible for reviewing the results of the audits undertaken and for identifying and taking further actions as required
- reports are sent to the ISPB and the board for information.

8 References

Access to Health Records Act 1990
National Health Service Litigation Authority
Common Law on Confidentiality
Data Protection Act 1998
Freedom of Information Act 2000 – Section 46
Information Governance Toolkit
Public Records Act 1958
Records Management Code of Practice

9 Associated documents

- [access to health records policy](#)
- [access to health records procedure](#)
- [confidentiality of personal health information policy and procedure](#)
- [data protection policy and procedure](#)
- [developing Trust documents policy](#)
- [information security policy](#)
- [internet and email use policy](#)
- [medical records procedures](#)
- [records management policy](#)
- [retention and destruction schedule](#)
- [standards for health record keeping policy and procedure](#)
- [waste disposal policy](#)
- [waste disposal procedure](#)

Equality and diversity statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

Disclaimer

It is **your** responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

Document management

Approval:	Information Governance Steering Group (IGSG) 12 October 2011		
Owning department:	Information Governance		
Author(s):	Michelle Ellerbeck, Information Governance Lead		
File name:	Records preservation retention and destruction policy Version7 October 2011.doc		
Supersedes:	Version 6, June 2011		
Version number:	7	Review date:	October 2014
Local reference:		Media ID:	443

Appendix 1: Process to set up/ review a local retention and destruction schedule

Setting up a new local retention and destruction schedule

1. Review the Trust schedule and identify if the department keeps any records that are not covered by the Trust schedule.
2. List these records (not covered on the Trust schedule) on the local schedule. Please use the [local retention and destruction schedule template](#) on Connect.
Please note:
Do not include records identified on the Trust schedule unless for specific business reasons the department wishes to retain these for a longer period than that identified on the Trust schedule
3. Decide with relevant staff in the department how long these records should be retained for. Records should only be retained for as long as needed to meet business and departmental needs; do not retain records 'just in case'; justify why they need to be kept.
4. Once the local retention and destruction schedule has been approved by the department a senior manager/ associate director of operations (ADO) should sign off the schedule.
5. A review date should be set for two years on from the date of approval.
6. Forward a copy of the approved schedule to the data awareness and training manager.

Review of a local retention and destruction schedule

1. The local retention and destruction schedule can be reviewed and updated at any time but as a minimum should be reviewed at least every two years.
2. Check the contents of the schedule against records that are held locally and the Trust retention and destruction schedule. Remove or add records as appropriate. Check the length of retention period for the records and ensure that this is still appropriate. Follow steps 3 to 6 above.

Further guidance is available from the data awareness manager.