NHS
Leeds Community Healthcare
NHS Trust

Records Management Policy	
Author	Narissa Leyland Head of Information Governance and Data Protection Officer
Corporate Leads	Leeds Community Healthcare NHS Trust Executive Director of Finance and Resources
Document Version	3.0
Document Status	Final
Date approved by Clinical and Corporate Policies Group (CCPG)	15 February 2019
Date ratified by SMT	13 March 2019
Date issued	15 March 2019
Review date	March 2019
Policy Number	PL325

Executive summary

This policy ensures that Leeds Community Healthcare NHS Trust will meet records management standards and regulatory requirements, including from the Care Quality Commission and National Health Service Resolution. The policy is supplemented by guidance which directs staff to their individual responsibilities.

Compliance with this policy also ensures that the Trust is compliant with the Data Protection Act 2018 and the Access to Health Records Act 1990.

Equality Analysis

Leeds Community Healthcare NHS Trust's vision is to provide the best possible care to every community. In support of the vision, with due regard to the Equality Act 2010 General Duty aims, Equality Analysis has been undertaken on this policy and any outcomes have been considered in the development of this policy.

Records Management Policy

Contents

Records Management Policy

1.   Introduction

This policy provides the basis for managing records and information at Leeds Community Healthcare (LCH) NHS Trust. This includes paper, electronic, health and administrative records. It is supported by guidance which ensures LCH remains compliant with the NHS regulatory and statutory frameworks**.**

It is noted that this policy equally applies to information held in paper and electronic records. A number of technical measures are inherent in electronic records such as security controls, ease of locating records and an audit trail.

2.   Aims and Objectives

LCH is committed to effective records management in line with the Records Management Code of Practice for Health and Social Care 2016, both clinical and non-clinical information. It contributes to patient care and business processes by effectively managing the information created by LCH. Robust records management delivers benefits for LCH, which include better use of staff time and more efficient use of physical space and information stored electronically.

This policy contains actions necessary to comply with national standards for record keeping; these include from the Care Quality Commission, National Health Service Resolutions Standards and Data Security & Protection Toolkit.

3.   Definitions

Records management describes the process which records are managed through their lifecycle from creation and storage to final destruction or permanent place of deposit. Throughout the lifecycle all records will be kept under secure conditions and access will only be to those with a legitimate right of access. Refer to Appendix B for Retention Periods for Records.

A record - The International Standard for Records Management ISO 15489-1:2016 defines a **record** as "Information created, received, and maintained as evidence by an organization or person in the transaction of business, or in the pursuance of legal obligations, "regardless of media".'

4.   Responsibilities

All staff employed by Leeds Community Healthcare NHS Trust must work in concordance with the Leeds Safeguarding Multi-agency Policies and Procedures and local guidelines in relation to any safeguarding concerns they have for service users and the public with who they are in contact.

The following roles are responsible for delivering and achieving records management standards;

The Trust Board is ultimately responsible for ensuring that Records Management function is addressed

Chief Executive has overall accountability for Records Management within the Trust as the Accountable Officer; the role provides assurance, through a Statement of Internal Controls, that all risks to the organisation, including those relating to the management of records are effective and mitigated.

Director of Finance and Resources has the lead responsibility for the Records Management policy and for ensuring that this is implemented and becomes an active document.

Caldicott Guardian is the Medical Director; this is an advisory role and has responsibility for protecting the confidentiality of patient information and ensuring it is shared appropriately and securely. The Caldicott Guardian is supported by the Trust's Information Governance Team who provides service level support and assurance on delegated Caldicott tasks.

Heads of Service are responsible for records and information created by their staff. Heads of Service are also responsible as **Information Asset Owners (IAO)**. An IAO is obliged to enforce policies and procedures locally relating to information management and give assurances to the SIRO that they are being met. This includes an annual audit of information assets, removable media and data flow mapping.

All staff are responsible for ensuring they comply with this policy and local guidance where this exists. Staff are also directed by their professional codes of practice which may also include guidance on record keeping. Staff must report all incidents involving records via the Datix incident reporting system. This includes the loss of or missing records.

Head of Information Governance & Data Protection Officer has operational responsibility for the Records Management Policy and is responsible for the overall development and maintenance of the Records Management policy and for ensuring this policy complies with legal and regulatory edicts. They are also responsible for providing learning and development with key learning points from this policy and for monitoring compliance with the policy to assess its overall effectiveness. The Head of Information Governance and Data Protection Officer will give advice and guidance to inform staff of their obligations

Information Governance Group will approve guidance and procedures related to records management. This is the sub group with delegated duties to deal with information governance and overall records management issues and reports to the Audit Committee.

5. Statutory and regulatory requirements of Records Management

a) LCH is subject to several statutory and legislative requirements. The Head of Information Governance and Data Protection Officer can issue guidance and procedural notes to meet these requirements. Any procedures and guidance are approved by the Information Governance Group.

b) LCH, as an NHS body created by statute, is subject to the Freedom of Information Act 2000 (FOI) and the Public Records Act 1958. The Code of Practice issued under Section 46 of the Freedom of Information Act 2000 directs public bodies how to conduct records management.

c) The Data Protection Act 2018 (DPA) requires LCH to ensure that personal data is managed within statutory and legislative boundaries. These include keeping personal data for only as long as it is necessary and enforcing appropriate technical measures to keep relevant records secure. The FOI Act and the DPA are regulated by the Information Commissioner and the Public Records Act by the Ministry of Justice.

d) The Department of Health and Social Care requires NHS records to be managed according to the Records Management Code of Practice for Health and Social Care so it can ensure the NHS Care Records Guarantee is met.

e) All patient records and staff records are regarded as confidential and must be marked CONFIDENTIAL and their access limited to those with a legitimate right of access. Sensitive business records and those subject to further controls before release must be marked as RESTRICTED. Records not marked might be assumed to be unclassified and open to access. LCH patient records must be managed according to regulatory standards for records to ensure quality and appropriate secure storage and access. Refer to section 6.

6. Records and Information Life Cycle Management

Records and Information Management plays an integral role within LCH as it underpins effective information sharing within our organisation and externally to patients and suppliers. The law requires certain records to be kept for a defined retention period; however records are used on a daily basis for internal purposes to help make decisions, provide evidence, etc. Using the diagram below, you can learn more about each of the 5 steps in the Records Life Cycle.
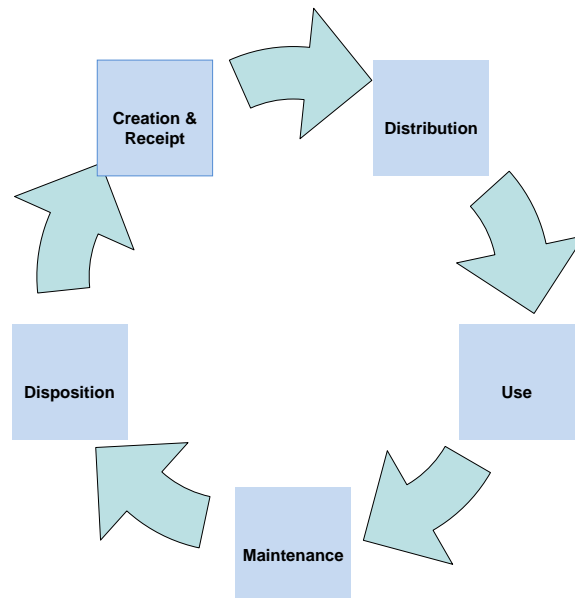
Stage 1: Creation and Receipt

This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. It can be created by internal employees or received from an external source and it is complete and accurate.

Stage 2: Distribution

Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are distributed when photocopied; printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used.

Stage 3: Use

This stage takes place after information is distributed. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other LCH operations. It is also considered the Active Phase.

Stage 4: Maintenance

Maintenance is when records are not used on a day to day basis and are stored in the Records Management system. Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be removed from a

Records Management system; the information should be copied and tracked to ensure no amendments were made.

Stage 5: Disposition

Disposition is when a record is less frequently accessed, has no more value to LCH or has met its assigned retention period. It is then reviewed and if necessary destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value to LCH will be retained for 20 years and sent to the National Archives, where they will be kept for the future of the organisation and may never be destroyed. This is the final phase of a records lifecycle. If you are unsure whether your records have historical value, please get in touch with the Information Governance Team.

7.   Record Retention Schedules

Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the Data Protection Act 2018 (DPA) and/or the Freedom of Information Act 2000. Moreover, compliance with these acts means that, for example, personal data must not be kept longer than is necessary for the purposes, for which it was collected (5th Data Protection Principle).

Records should only be destroyed in accordance with the LCH's Records Retention and Disposal Schedule, Appendix B. It can be a personal criminal offence to destroy requested information under either the Data Protection Act (Part 6 - Enforcement) or the Freedom of Information Act (Section 77). Therefore clear destruction must take place in accordance with proper retention procedures.

The Code of Practice on Records Management, issued under Section 46 of the Freedom of Information Act 2000, requires that records disposal 'is undertaken in accordance with clearly established policies that have been formally adopted'. The Business and Corporate Records Retention Schedule is a key component of LCH's information compliance and allows it to standardise its approach to retention and disposal.

The recommended retention periods shown on the Business and Corporate Records Retention Schedule apply to the official or master copy of the records. Any duplicates or local copies made for working purposes should be kept for as short a period of time as possible. Duplication should be avoided unless absolutely necessary. It should be clear who is responsible for retaining the master version of a record and copies should be clearly marked as such to avoid confusion, this is maintained as part of the Information Asset Register.

Some types of records which may be created and kept locally are the responsibility of the local department, but may be found under a different function on the retention schedule: for example where recruitment is carried out by departments, the department shall be responsible for ensuring the disposal of the records relating to unsuccessful candidate, this type of record is listed under Human Resources in the retention schedule.

8. Record Access Arrangements

There are a range of statutory provisions that give individuals the right of access to information created or held by LCH such as a data subject access request, Freedom of Information request and correspondence on how a decision was made. The Data Protection Act 2018 allows individuals to find out what personal data is held about them. The Freedom of Information Act 2000 gives the public the right of access to information held by public authorities.

8.1 Record Disclosure

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

Only certain staff members have the authority, which is dictated by their role, to disclose records. Staff members with this authority should make a record of any copies of records they have disclosed, and to whom.

8.2 Record Closure

Records should be closed, for example, made inactive and transferred to secondary storage as soon as they have ceased to be in active use other than for reference purposes, in the case of paper corporate records.

If a record is deleted / destroyed once its retention period has been reached, then a Records Disposal Certificate must be completed and saved in order to prove that the record existed, met its retention and was then disposed of.

8.3 Record Appraisal

Appraisal refers to the process of determining whether records are worthy of permanent archival preservation, as certain records created by LCH may be of historical interest to The National Archives. For further advice contact the IG Team.

The purpose of the appraisal process is to ensure the records are examined at the appropriate time to determine whether or not they are worthy of archival

preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

It is the responsibility of the staff member who is leaving their current post or the organisation, and their Line Manager, to identify as part of the exit procedure specific records that should be retained in line with LCH's Business and Corporate Record Retention Schedule.

8.4   Record Transfer

Records selected for archival preservation and no longer in regular use by LCH should be transferred to an archival institution, for example a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities.

Following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, non-active records are required to be transferred no later than 20 years from the creation date of the record, as required by the Public Records Act 1958.

The Head of Information Governance & Data Protection Officer will identify LCH's Place of Deposit and assist in the transfer of those records identified.

8.5   Record Disposition

Disposal is the implementation of appraisal and review decisions and the term should not be confused with destruction. A review decision may result in the destruction of records but may also result in the transfer of custody of records, or movement of records from one system to another.

Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records consumes time, space and equipment use, therefore disposal will aid efficiency.

Unnecessary retention may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Act 2018. If LCH continues to hold information which we do not have a need to keep, we would be liable to disclose it upon request. The Data Protection Act 2018 also advises that we should not retain personal data longer than is necessary.

8.6   Records Security: Work base, home working agile working

All person identifiable data or commercially sensitive data must be saved with appropriate security measures.

Staff must not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of LCH.

Removable Media should be LCH owned and encrypted by IT. Ideally, personal confidential data should not be stored on any removable media, however if there is no other option ensure this data is stored on a corporate encrypted device and deleted once transferred to identified secure area folder.

When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.

LCH has an Information Handling Policy in order to ensure that staff are aware how to receive personal information in a secure manner at a protected point.

In non-clinical areas, each department should have at least one designated safe haven contact point. Ideally, all information transmitted to the organisation should pass to these contact points. Clinical environments should operate in accordance with safe haven principles and the organisation should operate safe haven procedures for all flows of person identifiable information.

When transferring data, ensure security measures and precautions have been actioned by the sender and receiver. A robust contract or Information Sharing Agreement should be in place detailing responsibilities if the information is being transferred to a third party. Please contact the Information Governance team for more advice.

9.   Responsibility for Inactive Records

Records that are no longer used must also be managed until they are not needed for patient care or statutory retention.

Records that are no longer required will be destroyed confidentially. Confidential destruction includes using the designated shredding bins for site shredding. For digital media the Computer Helpdesk will take ownership of the media and arrange for it to be crushed by a service accredited to the appropriate destruction standards. Inactive records will be held securely, stored and managed to restrict access to only those who have a legitimate right to see them. This will ensure that an integral, authentic, reliable and usable record is maintained.

Where local conditions cannot be maintained to appropriate standards, the records must be moved to a place where they meet standards. Appendix B reference

10. Risk Assessments

This policy requires any non-compliance to be risk assessed and incidents to be reported where they occur. Where the guidance issued by the Head of Information Governance cannot be implemented, the Service Manager escalates this risk of non-compliance and is entered onto the service risk register.

Non-compliance with this policy must be reported as an incident via the Datix® reporting system. The learning must be communicated to staff through the most appropriate communication channels. These include staff meetings, Community Talk or intranet notice. Additional training may also be identified.

11. Training Needs

For staff training refer to the Statutory and Mandatory Training Policy (including Training Needs Analysis). Course details are available on the Intranet.

The Head of Information Governance delivers bespoke training to individual services to meet their needs as and when requested. Training will cover the organisation's policies, guidance and specific areas directed by NHS Resolution and the Care Quality Commission in respect of records management.

12. Approval and Ratification process

The policy has been approved by the Clinical and Corporate Policies Group and ratified by SMT behalf of the Board.

13. Dissemination and Implementation

Dissemination of this policy will be via the Clinical and Corporate Policy Group to services and made available to staff via the intranet.

Implementation will require:

- Operational Directors/ Heads of Service/General Managers to ensure staff have access to this policy and understand their responsibilities for implementing it into practice.
- The Head of Information Governance will provide appropriate support and advice to staff on the implementation of this policy

14. Review arrangements

This policy will be reviewed in three years following ratification by the author or sooner if there is a local or national requirement.

15.   Associated documents

The following Information Governance policies are associated with effective records management:

Confidentiality Code of Conduct – PL306
Information Governance Policy and Framework – PL317
Internet Policy - PL370
Network Security Policy – PL350
Information Handling Policy – PL301
Waste Management Policy PL341

16.   References

Care Quality Commission
Care Quality Commission – Essential Standards of Quality and Safety 2009
Data Protection Act 2018
Freedom of Information Act 2000
Human Rights Act 1998
Access to Health Records Act 1990
Public Records Act 1958
The Health and Social Care Act 2012
Data Security & Protection Toolkit (annual updates)
NHS Resolutions
ISO Code
Records Management Code of practice for Health and Social Care 2016

Appendix A – Patient Records Management

Managing Patient Held Health Records
Prior to creating a new patient health record the relevant patient registration system must be checked to ensure the patient does not already have health records. This will ensure a complete record of the patient's record of care is available, and also serve to minimise risk and duplication.

When a new health record is created, an entry must be made into the relevant registration system so all staff are aware of this. They must be securely contained in a folder, with the outside marked confidential with the patient's name and NHS number. The creation and format of clinical records must include the following elements:

Bound and stored so that loss of documents is minimised – additional information securely fastened to the Clinical Records
Health practitioners use the approved LCH documentation when completing clinical records.
A designated section on the front of the records for recording alert notices such as hypersensitive reactions, special conditions for retention of records (e.g. because patient is taking part in a clinical trial).
Clear structure and be divided into sections e.g. medication section
Instructions for filing printed on the inside of the Health Record or on any dividers being used where these have been agreed
Flaps or pockets only used for the storage of patient labels not for filing.
A medication list detailing all prescribed items completed for relevant patients

Records must be completed contemporaneously in line with professional and organisational standards. This may be achieved in a variety of ways according to the nature of the record held by the service e.g. entering information into electronic system at the time of the intervention or immediately on return to base or completing patient held records at time of intervention. If the record is not available, interventions undertaken must be recorded via means agreed within service and added to the record as soon as this becomes available. All entries should be timed, dated and signed.

Tracking Records
Paper records are either: in the base/department, patient's home, with a staff member, or in archive.
Each service must have a registration system as a means of identifying where the record is at any given time (this may be paper based or electronic). Examples of processes which may be used are:

A tracking book which includes information (date, time and name of staff) when the record is removed and returned from the base.
Assigning the records by caseload to a staff member who takes full responsibility until the patient is discharged.

Using electronic systems to identify which staff member has the paper record through the last entry.

For more detail on tracking and the information that must be recorded refer to the Information Handling Policy (including Transfer of Paper Records, Removable Media, Email and Safe Haven).

Process for Retrieving Records
Records will either be in the base, with another team/staff member or in commissioned storage. In the first instance, the electronic record can be used to determine where a record is located. If the record is with another team they are requested to provide the record. Where local records indicate the patient file is in storage they can be retrieved through contacting the records centre.

Appendix B – Clinical and Non-Clinical Retention Schedule

Broad descriptor	Record Type	Retention Start	Retention period	Action at end of retention period	Notes
Care Records with standard retention periods	Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Care Records with standard retention periods	Adult social care records	End of care or client last seen	8 years	Review and if no longer needed destroy	
Care Records with standard retention periods	Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.

Care Records with standard retention periods	Electronic Patient Records System	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.
Care Records with Non-Standard Retention Periods	Contraception, sexual health, Family Planning and Genito-Urinary Medicine (GUM)	Discharge or patient last seen	8 or 10 years (see Notes)	Review and if no longer needed destroy	Basic retention requirement is 8 years unless there is an implant or device inserted, in which case it is 10 years. All must be reviewed prior to destruction taking into account any serious incident retentions. If this is a record of a child, treat as a child record as above.
Care Records with Non-Standard Retention Periods	HFEA records of treatment provided in licenced treatment centres		3, 10, 30, or 50 years	Review and if no longer needed destroy	
Care Records with Non-Standard Retention Periods	Medical record of a patient with Creutzfeldt-Jakob Disease (CJD)	Diagnosis	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of CJD must be retained. Where the CJD records are in a main patient file the entire file must be retained. All must be reviewed prior to destruction taking into account any serious incident retentions.

Care Records with Non-Standard Retention Periods	Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care. The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.
Pharmacy	Information relating to controlled drugs	Creation	See Notes	Review and if no longer needed destroy	Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years.
Pharmacy	Pharmacy prescription records *see also Controlled Drugs*	Discharge or patient last seen	2 Years	Review and if no longer needed destroy	See also 'Controlled Drugs'. There will also be an entry in the patient record and a record held by the NHS Business Services Authority. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy-records/

Event & Transaction Records	Clinical Audit	Creation	5 years	Review and if no longer needed destroy	
Event & Transaction Records	Clinical Diaries	End of the year to which they relate	2 years	Review and if no longer needed destroy	Diaries of clinical activity & visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.
Event & Transaction Records	Clinical Protocols	Creation	25 years	Review and consider transfer to a Place of Deposit	Clinical protocols may have archival value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (see Corporate Records).
Event & Transaction Records	Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	
Event & Transaction Records	Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	20 Years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by an instrument of retention and if a Place of Deposit or the National Archives do not class them as a record of archival importance they are to be destroyed after 20 years.
Event & Transaction Records	Equipment maintenance logs	Decommissioning of the equipment	11 years	Review and consider transfer to a Place of Deposit	
Event & Transaction Records	Inspection of equipment records	Decommissioning of equipment	11 Years	Review and if no longer needed destroy	

Event & Transaction Records	Notifiable disease book	Creation	6 years	Review and if no longer needed destroy	
Event & Transaction Records	Referrals not accepted	Date of rejection.	2 years as an ephemeral record	Review and if no longer needed destroy	The rejected referral to the service should also be kept on the originating service file.
Event & Transaction Records	Requests for funding for care not accepted	Date of rejection	2 years as an ephemeral record	Review and if no longer needed destroy	
Births, Deaths & Adoption Records	NHS Medicals for Adoption Records	Creation	8 years or 25th birthday	Review and consider transfer to a Place of Deposit	The health reports will feed into the primary record held by Local Authority Children's services. This means that the adoption records held in the NHS relate to reports that are already kept in another file which is kept for 100 years by the appropriate agency and local authority.
Clinical Trials & Research	Advanced Medical Therapy Research Master File	Closure of research	30 years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.gov.uk/guidance/advanced-therapy-medicinal-products-regulation-and-licensing For clinical trials record retention please see the MHRC guidance at https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials
Clinical Trials & Research	Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014	Closure of trial	25 years	Review and consider transfer to a Place of Deposit	

Clinical Trials & Research	European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states area	Closure of trial	15 years	Review and consider transfer to a Place of Deposit	
Clinical Trials & Research	Research data sets	End of research	Not more than 20 years	Review and consider transfer to a Place of Deposit	
Clinical Trials & Research	Research Ethics Committee's documentation for research proposal	End of research	5 years	Review and consider transfer to a Place of Deposit	For details please see:http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/ Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a place of deposit may be interested in holding the research. It is best practice to consider this at the outset of research and orphaned personal data can inadvertently cause a data breach.

Clinical Trials & Research	Research Ethics Committee's minutes and papers	Year to which they relate	Before 20 years	Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a place of deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/
Corporate Governance	Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Corporate Governance	Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Corporate Governance	Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings

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

Communications	Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Communications	Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Communications	Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Communications	Website	Creation	6 years	Review and consider transfer to a Place of Deposit	
Staff Records & Occupational Health	Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.

Staff Records & Occupational Health	Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file.	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Records &	Staff Record	6 years after	75th	Place of Deposit	Good Practice for a Staff Record Summary:

Occupational Health	Summary	the staff member leaves	Birthday	should be offered for continued retention or Destroy	· Name · Previous names · Assignment number · Pay bands · Date of birth · Addresses · Positions held · Start and end dates · Reason for leaving · Building or sites worked
Staff Records & Occupational Health	Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer2 Statutory and mandatory training records - to be kept for ten years after training completed3Other training records - keep for six years after training completed.
Procurement	Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	

Procurement	Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Procurement	Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	
Estates	Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
Estates	CCTV		See ICO Code of Practice	Review and if no longer needed destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Estates	Equipment monitoring and testing and maintenance work where asbestos is	Completion of monitoring or test	40 years	Review and if no longer needed destroy	

	a factor				
Estates	Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed destroy	
Estates	Inspection reports	End of lifetime of installation	Lifetime of installation	Review	
Estates	Leases	Termination of lease	12 years	Review and if no longer needed destroy	
Estates	Minor building works	Completion of work	retain for 6 years	Review and if no longer needed destroy	
Estates	Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.
Estates	Radioactive Waste	Creation	30 years	Review and if no longer needed destroy	
Estates	Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Nynhydrin Test	Date of test	11 years	Review and if no longer needed destroy	

Estates	Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to Place of Deposit	
Finance	Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Finance	Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. Where benefactions endowment trust fund/legacies - permanent retention.
Finance	Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	
Finance	Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Expenses	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible
Finance	Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	

Finance	Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Finance	Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Finance	Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Finance	Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Legal, Complaints & information Rights	Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.
Legal, Complaints & information Rights	FOI requests where there has been a subsequent	Closure of appeal	6 years	Review and if no longer needed destroy	

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

Policy dissemination and implementation plan

Name of author who is leading with disseminating the document		Title of Document	
	Actions	**Dates**	**Comments**
	Induction Sessions required - provide dates:		
	Launch Event required - provide dates:		
	Raising at meetings, provide dates/which meetings:		
	Specific Instructions for disseminating the document		
	Lead for audit and monitoring		
	Do you require a link through to Leeds Health Pathways?		
The following will be actioned by the Quality and Professional Development Administrator:			

- Email services and departments requesting dissemination of document to applicable services
- Document uploaded on the LCH intranet
- Document forwarded to Leeds Health Pathways for uploading if relevant
- Superseded documents removed from the Intranet
- Article submitted for to the next Community talk

Policy Consultation Process

Title of Document	Records Management Policy
Author (s)	Head of Information Governance
New / Revised Document	Revised
Lists of persons involved in developing the policy	Head of Information Governance
List of persons involved in the consultation process	Richard Slough - Assistant Director of Business Intelligence Bryan Machin - Director of Finance and Resources Catherine Duff - Interim Quality Lead for Children's Business Unit Dr Ruth Burnett - Interim Executive Medical Director Joanne Sykes - Clinical Safety Officer Mr Martin Harris - Head of Information Technology