East Lancashire Hospitals NHS Trust
A University Teaching Trust

TRUST WIDE DOCUMENT

| | |
|---|---|
| **Delete as appropriate** | **Policy** |
| **DOCUMENT TITLE:** | **CLINICAL RECORDS POLICY** |
| **DOCUMENT NUMBER:** | **ELHT/C013 Version 5. 4** |
| **DOCUMENT REPLACES Which Version** | **Version 5.3** |
| **LEAD EXECUTIVE DIRECTOR DGM** | Director of Finance, Information & Planning (SIRO) |
| **AUTHOR(S): Note should not include names** | Directorate Manager Centralised Outpatients & Administration Services |

| | |
|---|---|
| **TARGET AUDIENCE:** | All Trust Personnel |
| **DOCUMENT PURPOSE:** | The Clinical Records Policy sets out the standards required for clinical record keeping, and details the specific requirements relating to health records management within the organisation to ensure the delivery of an effective high quality clinical records service. This policy also sets out the current legislation relating to health records. |
| **To be read in conjunction with (identify which internal documents)** | C134 Subject Access Policy |

| | |
|---|---|
| **SUPPORTING REFERENCES** | • Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2020<br>• Health & Safety Care Act – Duty to Share 2015<br>• Academy of Medical Royal Colleges – A Clinician's Guide to Record Standards<br>• Care Quality Commission the right information in the right place at the right time (2009)<br>• An organisation with a memory (2000)<br>• Confidentiality : NHS code of practice (2003)<br>• Information security management: NHS code of practice (2007)<br>Caldicott Principles<br>National Data Guardian Principles<br>• Nursing and midwifery council (2009) Record Keeping – guildance for nursing and midwives<br>• Department of Health (2010) Essence of care benchmarking for record keeping<br>• Royal College of Physicians (2008) a clinician guide to record standards part 1 & 2<br>• Royal College of Physicians (2009) generic medical record keeping standards<br>• Waste management policy C071<br>• Information Governance Alliance, Record Management Code of Practice for Health & Social Care 2020<br>• Photography & Video Records: Policy & Procedure to maintain Confidentiality & Consent, Copyright & Storage ELHT/C88<br>• Confidentiality of Personal Information ELHT/C077<br>• Health Records Casenote Archiving Procedure<br>• RDISOP003 Health Records & Research<br>• SOP4 Maternity Records – maternity service guide |

**CONSULTATION**

| | **Committee/Group** | **Date** |
|---|---|---|
| **Consultation** | Clinical Records Modernisation and Oversight Group | July 2021 |
| **Approval Committee** | Clinical Records Modernisation and Oversight Group | July 2021 |
| **Ratification date at** | August 2021 | |

| | |
|---|---|
| **Policy Council:** | |
| **NEXT REVIEW DATE:** | April 2024 (this policy focuses on paper records and will be amended in line with the Trust's migration to the electronic patient record, and/or any changes to legislation etc) |
| **AMENDMENTS:** | **V5** - Policy updated to reflect inclusion of community records following transfer of community services.<br>**V5.1** – Policy updated to reflect titles/meetings changes<br>**V5.2** – Policy updated to reflect the introduction of the Information Governance Alliance, Record Management Code of Practice for Health and Social Care 2016 following the<br><br>withdrawal of the DOH Records Management Code of Practice Parts 1 & 1.<br>Title changes<br>Inclusion of the HRSG Terms of Reference<br>**V5.3** – Policy updated to reflect the following changes:<br>- guidance in relation to the destruction of patient records in light of the Independent Enquiry into Child Sexual Abuse (IICSA)<br>- TOR<br>- Clinical Audit Schedule<br>Introduction of General Data Protection Act (GDPR) in relation to Subject Access Requests<br>**V5.4** – Policy updated to reflect the following<br>- Removal of 'TOR' and 'Audit Schedule'<br>- Renaming of the HRSG to Clinical Records Modernisation and Oversight Group<br>- Title changes<br>- Revision to supporting references<br>- Amendments to section 3 'Legal Obligations that apply to records'<br>- Amendment to section 14' Records Security and storage – inclusion of off-site record storage'<br>- Inclusion of section 12 'National Data Opt Out'<br>- Inclusion of section 13 'Guidance in relation to the Gender Recognitions Act 2004 – records management'<br>- Inclusion of section 16 'Records access and auditing'<br>- Revision to Appendix one –'Updated records management code of practice 2020' |

**TABLE OF CONTENTS**

**CLINICAL RECORDS POLICY**

## 1. Objectives of this Policy

The key objective of this policy is to ensure that a comprehensive and secure clinical records management system is in place in the Trust, and that there is a process for managing the risks associated with clinical records in all media. This policy sets out the duties, standards, managerial responsibilities and minimum retention periods for the effective management of all clinical records. This includes the creation, day to day use, storage, and maintenance and disposal procedures.

Clinical records include all clinical information relating to a patient in whatever media this is available. These may include:

- Electronic or paper-based patient health records including all specialties
- Urgent care and emergency, birth and all other registers;
- Theatre records and related registers;
- Radiology and imaging reports, output and images;
- Photographs, slides and other images;
- Audio and video tapes, cassettes, CD-ROMs
- Computerised records

Clinical Records may be referred to as:

- Medical records
- Patient records/notes
- Speciality/departmental records or assessments
- Casenotes
- Health records
- Obstetric health records
- Urgent care and casualty card

They inform the clinician of all key features which might influence the treatment proposed. They also provide a contemporaneous and complete record of the patient's treatment and related features.

In addition to ensuring good patient care, complete, accurate and timely records allow a clear picture of events to be obtained, which is imperative for managing claims and complaints, and for auditing practice and remaining proactive.

## 2. Duties and Accountability

### 2.1. Chief Executive

The Chief Executive is accountable for the quality of records management within the Trust and exercises this responsibility through delegation to the Director of Finance Information and Planning as Senior Information Risk Officer (SIRO) and via line management to the Director of Diagnostics and Clinical Support Division.

### 2.2. Directorate Manager, Centralised Outpatients & Administration Services

The Directorate Manager for Centralised Outpatients & Administration Services reports via the Divisional Medical Director for Centralised Outpatients and Administration Services to the responsible Executive Director. She/he will be the organisational lead manager responsible for Clinical Records management, and act as the Information Asset Owner (IAO) for all patient records within the Trust. She/he will jointly facilitate the Clinical Records Modernisation and Oversight Group, and will be responsible for providing exception reports where appropriate to the Clinical Effectiveness Committee.

### 2.3. Executive Directors and Divisional Management Teams

They must ensure that:-

- All staff adhere to the policy
- The policy and procedures are carried out for records consistently and appropriately.
- Record keeping standards are monitored through quality control and audit to ensure the effectiveness of the policy
- Appropriate training is given for staff to understand and comply with their responsibilities

### 2.4. Individual responsibility

All healthcare workers are professionally accountable for maintaining good record keeping practice, which includes adhering to data quality guidelines, accuracy, contemporaneous recording and best practice in relation to clinical records as defined in this policy. All staff are responsible for any record they create or use, and any records which are created are public records. All staff that come into contact with patient information have a personal common law duty of confidence. Any records identified as lost or missing must be reported as an incident. Any breach of confidentiality will result in consideration of disciplinary action.

All line managers must ensure that their staff, permanent and temporary (including agency staff, contractors, students and volunteers), whether administrative or clinical and whose NHS role necessitates the use or access of any record, are adequately trained and apply the appropriate guidelines.

### 2.5 Clinical Records Modernisation and Oversight Group

The Clinical Records Modernisation and Oversight Group is responsible for the implementation and development of the clinical records policy, and to oversee the audit and monitoring of its implementation and action recommendations. The steering group is required to report via its minutes and exception reports to the Patient Safety & Risk Committee which is the overarching operational group for risk management in the Trust

### 2.6 Clinical Effectiveness Committee

The Clinical Effectiveness Committee will receive assurance on progress with the clinical records action plan(s) via the minutes of the Clinical Records Modernisation and Oversight Group, and exception reports on specific issues or concerns from the Clinical Records Modernisation and Oversight Group. The Clinical Effectiveness Committee will provide assurance and reports to the Trust Board regarding clinical records management.

### 2.7 Clinical/Service Records Audit

The Trust/Services will undertake regular audits in line with the agreed audit plan and submit to the Clinical Records Modernisation and Oversight Group for review.

## 3. Legal Obligations that apply to records

The main legislative measures that give rights of access to health records include:

- Data Protection Act 2018 incorporating UK GDPR: gives a number of rights to citizens including the right for living individuals to access their own records. The right can be exercised by an authorised representative on the individual's behalf.
- Access to Health Records Act 1990 - gives rights of access to deceased patients health records by specified persons.
- Medical Records Act 1988 - gives rights for individuals to have access to reports relating to themselves, provided by medical practitioners for employment or insurance purposes.

### 3.1. Data Protection Act 2018 Incorporating UK GDPR

This act regulates the processing of personal data held manually and on computer. It applies to personal information generally not just health records.

1. Lawful, fairly and transparency
2. Specific, explicit and legitimate
3. Adequate, relevant and limited
4. Accurate and up to date
5. Retention and disposal
6. Appropriate security
7. Responsible and accountability

### 3.2. Patient Access to Records

The Data Protection Act incorporating UK General Data Protection Regulations (GDPR) gives the right of individuals, or their authorised representative to seek access to their records. This must be completed within one calendar month from receipt of request. Please refer to the Subject Access policy. C134.

There are two main exemptions:

1. If the record contains sensitive or personal third party information.

2. If access to all or part of the record will seriously harm the physical or mental wellbeing of the individual or any other person.

Patient access requests must be made to the Subject Access Team in the Information Governance Department, Burnley General Teaching Hospital.

Under the UK General Data Protection Act, any request to viewing or provide copies of the health records of a living person is free of charge unless it is 'manifestly unfound or excessive' (especially if it is repetitive). If further copies are required, a reasonable fee based on administrative costs can be applied. This will be set out in the Subject Access policy, C134. This will now include not charging access to health records for deceased patients.

### 3.3. Access to Health Records Act 1990

The Access to Health Records Act now only affects the health records of deceased patients. It applies only to records created since 1 November 1991. The Act gives access to:

- the deceased's personal representatives (both executors or administrators) to enable them

to carry out their duties: and

- anyone who has a claim resulting from the death.

However, this not a general right of access, it is a restricted right and the following circumstances could limit the applicant's access:

- if there is evidence that the deceased did not wish for any or part of their information to be disclosed; or

- if disclosure of the information would cause serious harm to the physical or mental health of any person; or

- If disclosure would identify a third party (i.e. not the patient nor a healthcare professional) who has not consented to that disclosure.

As with the Data Protection Act, a medical professional must review and approval ALL records before release.

Under the Act, if the record has not been updated during the 40 calendar days preceding the access request, access must be given within 21 days of the request. Where the record concerns information all of which was recorded more than 40 calendar days before the application, access must be given within 40 calendar days, however, the Trust will endeavour to supply the information within 21 days.

### 3.4. NHS Trust Sexually Transmitted Diseases Directions 2000

Every NHS Trust must take all necessary steps to ensure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except:

- For the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and

- For the purpose of such treatment or prevention.

### 3.5. Common Law Duty of Confidentiality

The general rule is that information cannot normally be disclosed without the patient's consent. There are exceptions to this rule

- where disclosure is in the public interest, and
- where there is a legal duty to do so, for example a court order

For further information please refer to the Confidentiality of Personal Information Policy (ELHTC077)

## 4. Creating records

Patient records should be created and aligned to the Trust's Acute Patient Administration System and/or the Community Patient Administration System. These records must include the Trust's Patient Administration System unique reference number and/or the patient's NHS number. These two systems are currently the master source of information for patient activity within the Trust.

All records created within the Trust should 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.

Records may be retained in paper or electronic format but the same referencing system must apply.

## 5. Tracking Records

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 record transactions. Tracking Records is only applicable to paper and other original records.

Please note, when transferring casenotes on PAS, the volume number must be referenced in the comment field.

## 6. Casenote Tracking System

The PAS system is used to electronically track patient casenotes. This enables Trust staff on all hospital sites to accurately identify the physical location of Casenotes and track their movements through the transfer facility within the casenote tracking (CNT) functionality.

Following a casenote request made to the appropriate records library or department by telephone/email/writing. The staff receiving the request for records must establish that the person making the request has the authority to view the record and is only doing so with good cause. Unavailability of casenotes for clinic or inpatient attendance presents a clinical risk to the patient and therefore must be avoided wherever possible. The ward / department of residence will be the tracked location. Casenotes for patients going to theatre, x-ray or other diagnostic service will not require tracking as they will remain with the patient or escort.

*No other method of tracking should be used for casenotes. If PAS is unavailable the Health Records Department must be contacted and Business Continuity Plans will be implemented in accordance with Emergency Planning.*

**Process for Tracking Casenotes - Please refer to the PAS Casenote Tracking Manual located in the IT System Training Section on Oli**

### 6.1. Authorised Borrowers

It is the responsibility of all Managers to ensure that staff input the relevant Casenote Tracking information in order to maintain a comprehensive and up to date system,

Managers have full responsibility for ensuring that the list of Authorised Borrowers associated with their area of work is reviewed and kept up to date. The relevant updates and changes must then be forwarded to at the System Support Department at the Royal Blackburn Teaching Hospital (RBTH).

### 6.2. Storage Locations

It is the responsibility of all Managers to ensure that staff input the relevant casenote tracking information in order to maintain a comprehensive and up to date system. This includes keeping the details of current Storage Locations up to date including off-site storage. Managers have full responsibility for ensuring that the list of storage locations associated with their area of work is reviewed and kept up to date.

### 6.3. Transferring of Casenotes to Authorised Borrowers (non ELHT Hospitals)

Casenotes must **NOT** be sent to any other organisation without prior approval by a senior member of the Health Records Department. In exceptional cases this is permitted but only if it is deemed to be a clinical risk to the patient, therefore, in all other circumstances please send photocopies with the exception of Salford Royal Hospital and Royal Bolton Hospital.

Original casenotes must be tracked to the receiving hospital and the tracking comments must include a contact number, name and location at the receiving hospital**.**

### 6.4. Returning of Casenotes to Main Storage Location

The authorised borrower is responsible for transferring the casenotes back to the main storage location. The authorised borrower must return the casenotes to a transit location. Library staff will then return the physical casenotes to a specified storage location within the health records libraries/Off-site storage location. Health Records staff will be responsible for ensuring the casenotes storage location is updated once the physical casenotes are received and filed.

All staff are responsible for the maintenance of comprehensive and orderly casenotes whilst in their care. This means that all loose filing, nursing notes, discharge letters and reports must be filed inside the casenote folder, in the appropriate order at the point of care.

## 7. Mislaid or Lost Records

A 'missing record' is defined as a record that cannot be located or is not available for patient consultation/inpatient stay or for other purposes, i.e. complaint/incident investigation.

In the event of a missing casenote, the department/user where the notes are currently tracked must make every effort to locate the record. When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of the actions undertaken.

In the case of a clinical record, a temporary record should be created by health records personnel, clearly marked as a temporary record (for general/ANC casenotes, these are white in colour) and populated will all relevant clinical information available for the patient. When the original records are located, the temporary set of records should be merged with the originals and the missing health records log and PAS updated accordingly.

Staff in health records must maintain a log of missing casenotes and conduct regular searches. All outcomes and actions must be recorded on the log.

In the event of missing clinical paperwork, the responsible department must make every effort to locate the records and report to the Departmental/Ward Manager. When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of the actions undertaken.

## 8. Retrieving Clinical Information

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

Digital information must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format in addition to providing information about those who have accessed the record.

## 9. Systems for Alerting

Each paper record must allow for the provision of a system to alert clinicians to all identified allergies and alerts recorded on the hospital casenote.
In the event that allergies and alerts are identified in departmental record systems, these must then be recorded in the hospital casenote if one exists.

Each individual system/departmental record should have a documented approach for recording its activities, including creation, retrieval, tracking, retention, disposal and destruction of the records created.

For hospital based inpatient and outpatient and emergency care records, where the acute Patient Administration System and the Electronic Patient Tracking Systems are the main reference systems, the hospital casenote and casualty card will be the main record source.

Speciality records may be held locally to support local clinical protocols where close access is required to a patient's treatment notes e.g. obstetrics, orthodontics, and physiotherapy. Other departments/ areas where records are created must hold their own documented approach detailing the operational policies for the management of their clinical records.

## 10. The Five Basic Record Keeping Standards required by the Trust to be used by all staff –

as a minimum the Trust requires all staff to adhere to the following basic records keeping standards.

A unique patient identifier must be used in all records.

All entries must be made in chronological order, or if written retrospectively this must be noted – electronic records show timelines and chronology in summary

All entries must be written in black ink (does not apply to electronic records)

All entries must be signed, and dated or listed to a chronological identifiable date. For electronic records a unique login or e-signature are accepted.

All alterations must be made in a way so that the original documentation and alteration are clear and all alterations must be signed and dated.

## 11. Good Practice Guidelines

In order to provide comprehensive accurate and clear records, staff should conform to their professional guidelines e.g.

- Keep clear, accurate and legible records, reporting the relevant clinical findings, the decision made, the information given to patients, and any drugs prescribed or other investigation or treatment.
- Make records at the same time as the events you are recording or as soon as possible afterwards.
- Only use abbreviations that follow common conventions.
- Accurately date and time records using the 24 hour clock.
- Do not use meaningless phrases, irrelevant speculation, offensive subjective statements or irrelevant personal opinions regarding the patient/service user.

(Ref: Academy of Medical Royal Colleges – A Clinician's Guide to Record Standards)

### 11.1 Contemporaneous record

Following the retrieval, receipt and completion of records into a clinical care document, the clinical record should reflect the continuum of patient care and should be viewable in chronological order.

In operational areas documentation relating to the current admission may be divided and filed in the inpatient and bedside ring binders. These are acceptable as long as they are filed in chronological order in the patient's main casenotes following transfer/discharge.

## 12. National Data Opt Out

This is a service which enables patients/service users to register to opt out of their confidential information being used for research and service planning. This choice does not apply when their information is used to help with their care and treatment or information that is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice on Anonymisation or is aggregated or count type data. More information can be found at https://www.nhs.uk/your-nhs-data-matters/

The national data opt-out does not apply to the disclosure of confidential patient information if there is another legal basis for it to be processed for example to deliver direct care, to protect public health, for example diagnose communicable diseases, delivery and monitoring vaccination programmes or where there is an overriding public interest in the disclosure, i.e. the public interest in disclosing the data overrides the public interest in maintaining confidentiality. Examples of disclosure which may be made in the public interest include – patients fitness to drive and reporting concerns to the DVLA or DVA or reporting knife wounds in line with GMC guidance.

When a patient sets an opt-out choice, it is recorded against their NHS number on the national spine. It will remain unless the patient changes their mind, and even after they have died.

## 13. Gender Recognition Act 2004: Records Management

Transgender or Trans is an umbrella term to describe people whose gender is not the same as, or does not sit comfortably with, the sex they were assigned at birth. Trans people may describe themselves using one or more of a wide variety of terms, including (but not limited to) transgender, transsexual, gender-queer (GQ), gender-fluid, non-binary, gender-variant, crossdresser, genderless, agender, nongender, third gender, bi-gender, trans man, trans woman, trans masculine, trans feminine and neutrois.

The Gender Recognition Act 2004 gives transgender people over the age of 18 years old the legal right to live in their affirmed gender.

### 13.1 Gender Recognition Certificate

A Gender Recognition Certificate (GRC) is legal recognition that an individual has changed their gender Once a person is granted an GRC, they will from that date, but not retrospectively be entitled to be recognised as being of their affirmed gender as opposed to the gender that was registered on their birth certificate. To obtain a GRC, patients must have gender dysphoria, live for two years in their affirmed gender and intend to live permanently as such.

A GRC provides, to the person possessing this, additional legal protection against third parties inappropriately disclosing their previous gender. It is important for employees to establish if a patient has a GRC, in order to enable them to take appropriate steps to ensure the clinical records, or internal or external communication about that person is lawful.

Not all transgender people have or intend to apply for a GRC and this is not required for protection against discrimination. The gender of an individual can also be established by consideration of other factors such as name and gender a person identifies with.

Employees should not disclose patient's transgender status or gender identity history to anyone who does not need to know that information for medical care. If disclosure is relevant to care, obtain consent from the individual whenever possible

### 13.2 Maintaining Clinical Records of Adult Transgender and non-binary Service Users

Employees should work collaboratively with transgender and non-binary service users to identify how their gender identity is reflected in their clinical records. This should include changes to clinical records requested by service users who disclose a change of gender identity.

When discussing potential changes to clinical records, employees should explain and discuss the following issues with the individual

- Clarifying which name and pronouns to be used in the clinical notes.
- Explaining the importance of clinicians being able to access relevant clinical information to deliver safe and effective clinical care.
- Highlighting the risks of the unavailability of relevant clinical information in medical emergencies or sex-related health care issues (e.g. pregnancy, cancer screening).
- Providing reassurance about how their privacy will be protected.

### 13.3 Updating Clinical Records - Changing names, pronouns, NHS number

Trust employees and services need to respect and respond to people in their identified gender. Therefore the process for changing a patient's clinical record is as follows;

- When a transgender person enters ELHT services for the first time: a clinical record should be created reflecting their identified gender.
- Names and titles on medical records must be changed to reflect the current gender status at the point of notification. There is no legal requirement to provide a Gender Recognition Certificate (GRC), or a new birth certificate in order for a change of gender to be recorded in clinical records. You should not ask to see someone's GRC or birth certificate
- Part of living in the affirmed gender is likely to involve a change of gender pronoun, plus administrative gender and name changes. Words we use to refer to people's gender in conversation - for example, 'he' or 'she'. Some people may prefer others to refer to them in gender neutral language and use pronouns such as they/their and hir' or 'ze' or 'zir'. Some people may prefer the title 'Mx'. It is always appropriate to ask someone who identifies as non-binary what pronouns they prefer.
- Some patients with a GRC may also choose to have their medical records changed to reflect various details including their new name and gender, without requiring a new record and NHS number.
- Patients may therefore notify the Trust of their intention to change their gender and those born in the UK do not need to produce any specific documentation. However, if they do produce documentation, it is likely to be a statutory declaration of name and gender change, which are signed on oath and witnessed by a solicitor.
- When somebody already using our services discloses they are transgender or intend to transition: a new clinical record should be updated reflecting the person's identified gender.

- If a patient requests administrative changes to their clinical records, this should be actioned from the date of the patient's request. For example, if a patient requests their name and gender to be changed on their records, any reference to their previous name and gender should be removed and their new name and gender should be used going forward.
- When someone who previously used our services in the gender they were given at birth returns to use a Trust service living in their identified (different) gender: a new clinical record should be created reflecting the person's identified gender. Any previous clinical record should be archived and only accessed, with written consent from the person themselves, if there are valid clinical reasons for doing so.

  Any information relating to the patient's previous gender identity should not be included in the new record. Employees can use gender neutral language and anonymise patient details to retain important information. For example, using phrases such as 'the patient had a smear on….' rather than 'she had a smear on…'. This is to protect confidential information and ensure the Trust is in line with the Gender Recognition Act 2004 which makes disclosing an individual's transgender history unlawful in many instances
- In relation to accessing the person's previous clinical record, it would be best practice to ask the person for written consent to do this if they have the ability and capacity to do this if access is needed for reasons of health, safety and wellbeing. In cases where a person does not consent or does not have the capacity to consent, the best interests of the safety and wellbeing of the person and those around them will need to be considered.
- The Gender Recognition Act (2004) clearly states that this information can be accessed and shared if it is being done for medical purposes by a health professional and the health professional reasonably believes that the person has given consent, is unable to give consent or the information is needed to maintain the safety of the person and/or those around them. The Act states that the term 'medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment.
- The RCN (2007) further state that records may need to be accessed when it is essential for the delivery of care for the person, but information must only be shared with people who need to know it in order to deliver safe and efficient care

## 14. Retention, Disposal and Destruction

### 14.1. Retention

The Trust will use as a minimum the Department of Health's Records Retention Schedule (Appendix 3 Related to Health Records). This appendix details the minimum retention period for each type of health record issued by the NHS Code of Practice for Records Management.

Clinical records may be retained for permanent preservation, or retained for research or litigation purposes. A formal request must be made by letter or email by the person wishing to retain a record to all record holders on the approved list (see appendix 3). This requirement will be recorded on all existing clinical records and on the relevant PAS system if one is available to ensure that these records are not destroyed.

Electronic records will be retained in line with the retention schedule and must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format. Retention periods will be reviewed and maintained by the Clinical Records Modernisation and Oversight Group (please refer to appendix 3)

### 14.2. Disposal

All documents must be reviewed annually in accordance with the Trust's clinical records retention schedule (see appendix 3).

Where records are identified for archival interest, the Directorate Manager must be contacted who will arrange for transfer of custody of these records to the National Archives.

The decision on the transfer of records from paper to electronic and the subsequent destruction of the paper record will be made by the Clinical Records Modernisation and Oversight Group/E-health programme board.

All records which have been archived electronically must be readable and referenced on the appropriate system. Access can be obtained to these records by contacting the appropriate department.

### 14.3. Temporary Suspension of the destruction of Health Records

The Independent Inquiry into Child Sexual Abuse (IICSA) chaired by Professor Alexis Jay has requested that large parts of the health and social care sector do not destroy any records that are, or may fall into, the remit of the inquiry. Investigations will take into account a huge range of records which may include, but are not limited to, adoption records, safeguarding records, incident reports, complaints and enquiries. Outside of this inquiry, it is also important to consider that these records are likely to require longer than the standard retention periods given in this Code. Before any records are destroyed you are advised to check for any further update from the inquiry website at www.iicsa.org.uk. This inquiry is due to finish in 2022.

The Infected Blood inquiry chaired by Sir Brian Langstaff has written to organisations in April 2019 to request that no documents, files or paperwork that may be of interest to the inquiry be destroyed – including medical records

Following the above directives, the Trust has made a decision to postpone the destruction of all health records during these investigations, which will be reviewed on an annual basis, based on the progress of the inquiries.

### 14.4. Destruction

All records must be destroyed confidentially either by use of a local cross cut shredder or using the Trust's approved confidential waste removal contractor or IT approved electronic destruction company. – Please refer to the Trust Waste Management Policy C071.

A record of destruction for all clinical information must be kept, this must include the records which are being destroyed and the name of the person/board who approved the destruction. Where records are destroyed by an external company, e.g. approved storage companies, a record of the destruction showing their reference, description and date of destruction and who authorised the destruction must be received and retained by the service.

## 15. Records Security /Storage & Security Standards

All staff are responsible for the safe-keeping of records which they handle. When in possession of clinical records these must be kept secure at all times and all offices where records are stored must be locked. It is the responsibility of each departmental manager to ensure appropriate access is available should a record be required out of hours.

### 15.1 Offsite Records

Archived, deceased and inactive Records are currently stored with our main storage contract provider 'Iron Mountain' who provide a storage, retrieval, delivery and destruction service. The Trust

also has a contract with 'Restore' who currently hold certain deceased and archived multi-volume records. A privacy impact assessment should be conducted on the offsite storage providers.

### 15.2 Records Security Standards

1. Clinical records contain confidential information, and it is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record.

2. Clinical records must only be accessed for clinical purposes, approved research protocols, clinical audit, complaints investigation and litigation.

3. Original records should not be sent to any other organisation without prior approval unless it is deemed to be a clinical risk (see section 6.4).

4. Clinical records transferred by hospital employees, must be placed in a sealed envelope or approved system for secure transportation.

5. Clinical records transferred by non-hospital employees must be undertaken by appropriate approved systems or contractors and should be transferred in sealed and tamperproof containers/envelopes.

6. Staff taking clinical records off premises must accept responsibility for their safe keeping and maintaining confidentiality.

7. Handheld records must be retrieved from the patient/service at the last contact. Systems must be in place for staff to obtain the handheld record from the patient following treatment.

8. All staff who use clinical records must be fully aware of their personal responsibilities and undertake regular training. (see Information Governance Toolkit and the Information Governance policy)

9. Records identified as lost or missing must be reported immediately to your line manager and if still identified as missing via an Incident report form. The Health Records department should be contacted for advice on further actions (see section 6.1).

10. In the unlikely event that records are identified as sent to the wrong address all reasonable methods of recovering these documents must be made. This will include contacting the postal service provider, or courier, and must include consideration of a staff member(s) going to the address to recover the information in person. Reasons for not undertaking any actions must be documented on the incident investigation section of the incident report.

## 16. Clinical Records Access and Auditing

**16.1** Staff must only access healthcare records (manual or electronic) when they have a legitimate professional/ clinical, administrative, managerial reason for doing so, and in adherence to any access control limits that may be implemented. Accessing records without justification may lead to an investigation and disciplinary action being taken by the Trust and/or professional body.

**16.2** Audit trails of who has accessed (viewed) the electronic record or changed (created/edited) active records may be logged and monitored.

## 17. Training and Development

Training on Record Keeping is mandatory for all Trust staff and is included in the local induction programme. Security of records is included in the Information Governance Toolkit for all Trust staff and reflected in Trust's Core and Essential Skills ( Mandatory training) Policy HR42), monitoring of this is audited in the Mandatory Training policy.

Record keeping guidance is available for reference in all services/wards, and regular updates on clinical records issues are provided via Trust communications streams and departmental/Information Governance newsletters.

All line managers must ensure that their staff, permanent and temporary (including agency staff, contractors, students and volunteers), whether administrative or clinical and whose NHS role necessitates the use or access of any record, are adequately trained and apply the appropriate guidelines.

## 18. Process for Monitoring Compliance of this Policy

The effective implementation of this policy will be monitored through a process of internal audits. These audits will be undertaken regularly to ensure compliance with this policy. **See Appendix 3 – ELHT Monitoring Compliance Table**

The audit reports will as a minimum include:-

- methodology
- findings
- recommendations
- action plan

The outcome of all records audits will be reported to the Clinical Records Modernisation and Oversight Group who will agree the action plan and include actions in the Trust Clinical Records Action Plan. The Clinical Records Modernisation and Oversight Group will monitor this plan to ensure that all recommendations have been actioned appropriately.

All audit reports submitted to the Clinical Records Modernisation and Oversight Group will be reviewed at least once each calendar year to monitor whether the format for audit reports has been achieved. This audit will be presented to the Clinical Records Modernisation and Oversight Group and will monitor whether actions plans have been reviewed. If any deficits are identified, the Trust's clinical records action plan will be updated accordingly.

The process for monitoring the Clinical Records and Modernisation Oversight Group is via the Clinical Effectiveness Committee.

## 19. Introduction/Revision of Clinical Documentation for inclusion in the hospital record – Paper/Electronic

- **ALL** Clinical Documentation (paper or electronic) must be agreed locally at the local Quality and Safety Board and subsequently submitted to the Clinical Records and Modernisation Oversight Group for approval.

## Appendix 1

**Health Records Retention Schedule – Please refer to the Records Management Code of Practice 2020 pages 51 to 71 as per the link below.**

***Records Management Code of Practice - NHSX***

***See Section 14.3. Regarding the temporary suspension of the destruction of health records***

## Appendix 2

### Principles to be used in Determining Policy Regarding the Retention and Storage of Essential Maternity Records

British Paediatric Association

Royal College of Midwives

Royal College of Obstetricians and Gynaecologists

United Kingdom Central Council for Nursing, Midwifery and Health Visiting

### Joint Position on the Retention of Maternity Records

1. All essential maternity records should be retained. 'Essential' maternity records mean those records relating to the care of a mother and baby during pregnancy, labour and the puerperium.

2. Records that should be retained are those which will, or may, be necessary for further professional use. 'Professional use' means necessary to the care to be given to the woman during her reproductive life, and/or her baby, or necessary for any investigation that may ensue under the Congenital Disabilities (Civil Liabilities) Act 1976, or any other litigation related to the care of the woman and/or her baby.

3. Local level decision making with administrators on behalf of the health authority must include proper professional representation when agreeing policy about essential maternity records.
   'Proper professional' in this context should mean a senior medical practitioner(s) concerned in the direct clinical provision of maternity and neonatal services and a senior practising midwife.

4. Local policy should clearly specify particular records to be retained AND include detail regarding transfer of records, and needs for the final collation of the records for storage. For example, the necessity for inclusion of community midwifery records.

5. Policy should also determine details of the mechanisms for return and collation for storage, of those records which are held by mothers themselves, during pregnancy and the puerperium.

6. List of maternity records retained should include the following:

6.1 Documents recording booking data and pre-pregnancy records where appropriate.

6.2Documentation recording subsequent antenatal visits and examinations.

6.3 Antenatal in-patient records.

6.4 Clinical test results including ultrasonic scans, alpha-feto protein and chorionic villus sampling.

6.5 Blood test reports.

6.6 All intrapartum records to include, initial assessment, partograph and associated records including cardiotocograph.

6.7 Drug prescription and administration records.

6.8 Postnatal records including documents relating to the care of mother and baby, in both the hospital and community setting.

**Appendix 3 – Monitoring Compliance**

| Aspect of compliance being measured or monitored. | Individual responsible for the monitoring | Tool and method of monitoring | Frequency of monitoring | Responsible Group or Committee for monitoring |
|---|---|---|---|---|
| Outpatient Casenote Availability and Trends | Deputy Health Records Manager | Information is extracted from PAS via business intelligence tool | Monthly | Clinical Records Modernisation and Oversight Group (CRMOG) |
| Datix Records related incidents 'Problems with Patient Records' | Health Records Manager | Datix Reporting tool – Action Plan | Monthly | Clinical Records Modernisation and Oversight Group (CRMOG) |
| Recent Care Audit /Basic record keeping standards | Clinical Audit with Medical Staff | Review of case notes | Annual | Clinical Records Modernisation and Oversight Group (CRMOG) |
| Case Note Storage | Health Records Manager | Audit tool / SOP | (previously Annual) to move to Monthly | Clinical Records Modernisation and Oversight Group (CRMOG) |
| Rationale for Clinical decision making, | | To be agreed | To be agreed | |
| Correct consultant (new 2021) | Ward managers/ Consultants | On ward EPTS/ Case notes | Monthly | Individual ward action plan |
| NAPF documentation audit (new 2021) | NAPF team | Trust wide documentation audit | One off | Individual ward action plan |
| IG audit | IG team | Area visit and observations | | Individual ward action plan |

**Appendix 4 - Introduction/Revision of Clinical Documentation for inclusion in the hospital record – Paper/Electronic**