Liverpool Women's NHS Foundation Trust

Ref: PL014

Records Management Policy

Version	8.4
Designation of Policy Author(s)	Patient Records Manager
Policy Development Contributor(s)	Head of Information Governance and Patient Records
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date issued	01/04/2024
Review date	31/03/2025
Coverage	Trust Wide

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at www.nrls.npsa.nhs.uk/beingopen and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

CONTENTS Page

1 Executive Summary

1.1 Applicability and Scope

i. This Policy defines the scope of Patient Records Management, the processes it entails and how the Trust ensures that good practice is maintained for Patient Records Management.

ii. This Policy covers all aspects of patient records within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information

2 Introduction

i. The Records Management Code of Practice has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England.

ii.

iii. This document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

3 Policy Objectives

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

ii. To ensure that records are scanned accurately – when a paper record is transferred from its paper format each document must be scanned under the correct speciality and tab. Any additional documents generated after this date must be sent to the Scanning Bureau upon completion.

4 Duties and Responsibilities

4.1 Senior Information Risk Owner

- Is accountable for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control.
- Reviews and approve actions in respect of identified information risks
- Ensures that the organisation's approach to information risk is effective in terms of resource, commitment and execution
- Sets the overall objectives for Information Governance for the Trust

4.2 Caldicott Guardian

- Is agreed as the patient 'conscience' of the organisation and advises the Trust Board on matters relating to patient confidentiality.

- Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
- Approves the release of patient information where consent from the data subject is not considered necessary or appropriate

4.3 Chief Information Officer

- Has overall responsibility for the operation of Information Governance for the Trust
- Ensures the overall approach taken to managing Information Governance is appropriate

4.4 Head of Information Governance and Patient Records

- Maintains and develops the Trust Information Governance and Information Security Policy and Framework.
- Manages Confidentiality and Data Protection across the Trust as the Subject Matter Expert.
- Implements the Information Governance related directives and objectives of the Senior Information Risk Owner

4.5 Local Information Governance Leads

- Act as the primary departmental point of contact for Information Governance and Information Security related matters.
- Attend the Trust Information Governance Committee meetings.
- Co-ordinate departmental compliance to Information Governance and Information Security training and deal with any areas of non-compliance.
- Undertake local Information Governance and Information security assessments where necessary.
- Ensure the Information Governance Committee decisions are implemented within the area represented.

4.7 Patient Records Manager

- Is the operational lead for patient records management for the Trust
- Is responsible for providing advice, guidance and facilitating the introduction of, and improvements in, patient records management procedures.
-

5 Main Provisions

5.1 General Provisions – All Health Records

i. All staff will ensure, where they have responsibility for any part of the management of health records, so far as is reasonably practical:

a. Records are available whenever they are needed for any legitimate purpose.
b. Information contained within the patient records accurately reflects the events that gave rise to the need to record the information.
c. Records are protected from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled.

d. Records are filed and organised correctly and in accordance with any filing system or other obligation that the Trust deems is necessary to implement.
e. Records are retained and disposed of appropriately and in accordance with the retention and disposal procedures that the Trust decides to implement.

ii. It is the responsibility of the department that first receives a patient to ascertain whether a patient record is needed and, where necessary, to make the patient record available so that it is ready when the patient arrives

iii. Patients shall have a single health record covering all episodes of care, regardless of the specialty under which they were treated, with the exception of Genetics and Hewitt Centre who shall have separate records. Documents or partial records which have been scanned, must have the remaining document scanned.

iv. All patients shall have a single unit number that is used for all episodes of care, regardless of the speciality under which they have received care.

v. Where a member of staff wishes to retrospectively amend or make additional entries to a record, the member of staff must clearly indicate that the record is being made retrospectively, which must also include the date and time that the entry is being made.

5.2 Paper Records

i. All staff will ensure, where they have responsibility for any part of the management of paper health records that:

a. No information other than the patient's Unit Number, NHS Number and name should be visible on the outside of Casenotes.
b. No plastic folder shall be placed anywhere inside Casenotes.
c. All CTGs will be placed in the correct CTG envelope, which shall be marked with the NHS Number, patient name, Unit Number, date and time when the CTG was taken and the signature of the member of staff who took the scan. No other information will be placed on the envelope.
d. Patient Identification sheets must be placed at the front of the Casenotes.
e. All wards, departments and individual staff are expected to file documents they have generated into the notes. If the record is already scanned the document can be sent to the scanning bureau.
f. All departments must print new PID's with the correct specialty. These are inserted into the front of the notes.
g. No department should build up a backlog of documents; these must be filed as soon as received.
h. Patient information that is required to be filed shall be filed by the department that generated the information. Patient information that is to be filed may only be sent to the patient records department for filings with the agreement of the Patient Records Manager. Patients records for filing that are sent without agreement of the Patient Records Manager will be returned to the source department.
i. Information relating to legal claims, complaints or patient information leaflets must not be placed in Casenotes.

j. Correspondence and information relating to Safeguarding must be filed behind the appropriate divider and at the back of the Casenotes.

5.3 Transporting Records

i. Paper health records, or any document that constitutes part of a patient health record, may not be removed from the Trust premises without the specific authority of an Approving Officer

ii. Records which are sent or returned from off-site storage company must be placed in correct storage boxes, which will be collected and returned by the company's staff.

iii. Where records are moved from one location to another within the Trust, records should be placed in a trolley with a sealed cover, which should cover the entire contents of the trolley

iv. Records must not be given to patients when transferring to another department

v. Where records are moved from one location to another then they will be correctly tracked at all times

vi. Where records are required to be moved to a remote location, and are not being transferred personally by Trust staff, the records must be sealed and sent by courier

vii Where a health record is moved from one location to another, it shall remain the responsibility of the sender until such a time as the health record has been tracked as having been received by the recipient.

5.4 Security of Records

i. Patient Records must be kept secure at all times and in all areas.

ii. With the exception of circumstances where an individual has enacted their rights under the Subject Access Provisions or Access to Health Records Act, records should not be viewable by patients.

iii. If records are stored in a trolley the cover must be used and stored in a secure room where there is no patient access

iv. Records must not be left in corridors unattended.

v. All rooms where records are stored must be locked when unattended.

5.5 Temporary Records

i. Temporary records can only be issued once a thorough search has been made for the original record.

ii. Temporary record folders may only be held in a lilac health records folder, which indicates to all staff that the original health record is still missing. Temporary Records folders are issued by the Health Records Department.

iii. Temporary records must be made up with as much as the same documents as the original folder. Where copies of information can be found this must be filed within the record.

iv. Clinical staff must be informed before the patient's attendance that the original record cannot be located.

5.6 Emergency Room Records

i. Where paper information is generated from an episode of care in the Emergency Room, all such information shall be placed in a red wallet and transferred immediately to the scanning bureau.

ii. It is the responsibility of the scanning bureau to ensure that Emergency Room records are transferred into the Electronic Document Management System (EDMS) or UCR within 48 hours of receiving them.

5.7 Structure and Maintenance of Paper Health Records

i. Anyone who records information must comply with the following:

a. Health records require a correspondence and a Safeguarding divider to be inserted into the back of the record.
b. Maternity records are to be filed on the first spine with each pregnancy to be recorded by year on the antenatal divider.
c. Gynaecology records are to be filed on the middle spine.
d. All documents are to be filed in corresponding order.
e. Plastic wallets or envelopes should not be placed in health records, which result in loose filing.
f. All documents should be secured by either hole punching and filing behind or placing on the appropriate investigation mount sheet.
g. No Sellotape, staples or paperclips should be used to secure documents.

5.8 Electronic Patient Records

i. Records required for scanning must comply with the following.

a. All patients new to the Trust and generated a new hospital number are not to have a paper casenote issued.
b. Documents are to be filed into the correct EDMS folder for that speciality.
c. EDMS folders are to be tracked throughout the Trust.
d. PID must be printed for each patient record with correct specialty.
e. All EDMS folders should be returned to the Scanning Bureau within 48 hours of completion.
f. All documents for patient records currently scanned must also have a PID printed and attached to the document.
g. Documents are to be scanned within 48 hours of receipt.
h. Documents to be scanned under the correct document type.
i. All documents are to be quality checked that they are scanned under correct Unit number and the same quality as original document.
j. All documents scanned need to be tracked to offsite storage under the correct speciality.
k. This is the current procedure until BS10008 is obtained.

BS10008 – is the 'Legal Admissibility of Electronic Content'
Any information which is held electronically must be accurate, auditable, assessable and legally admissible if required in court. The Records Department and Scanning Services must audit 100% of records before they can be considered for destruction. Only when the Trust is satisfied that the records are accurate electronically the paper can be destroyed.

Paper records marked not for destruction can still be scanned and an alert placed on UCR placed stating Do Not Destroy. The paper can still be destroyed as long as they are double checked by both the scanning company and Medical Records staff for accuracy.

The destruction of paper records must be either incinerated, or cross shredded and a certificate supplied by the company as proof that these were completed.

5.9 Retention of Records

i. Records shall be managed in accordance with the Department of Health Records Management Code of Practice but will, where necessary, vary its records retention period in accordance with the conditions specified in Paragraph 6.8.vii or in accordance with any statutory or other mandatory obligations.

ii. Where records relate to Human Fertilisation and Embryology Authority (HFEA) they shall be transported in sealed boxes

iii. Where records are transferred to the Electronic Data Management Systems, the leftover paper records shall be stored for a period of 3 months after which time unless the Trust receives notification that the original paper record must be kept.

iv. Birth Registers are kept within the Trust for a period of 16 years from the date of the registration of the birth and are then transferred to Liverpool Central Library for archiving purposes

v. Where the Trust holds a patient record, which contains records from more than one speciality, and those specialties have different retention periods, then the Trust will keep the whole record until such a time as the retention period of the longest record has been reached. At that point it will be subject to review and, if appropriate and not subject to an order to retain them, will be destroyed or deleted.

5.10 Destruction of Records

i. Where there is no longer a requirement to keep a record then they shall be destroyed in accordance with the Records Management Code of Practice.

~~ii.~~ With the exception of Genetics and HFEA notes the records are retained for the longest period.

iii. The Patient Records Manager will authorise the offsite storage company to destroy records that can be destroyed.

iv. The Patient Records Manager will ensure that certificated records are kept of each instance of records that have been destroyed.

v. The Patient Records Manager will ensure that tracking information for each patient whose records have been destroyed is updated within the relevant Trust system.

vi. Records that are stamped “Do Not Destroy” shall not be destroyed until their destruction is specifically authorised by the Patient Records Manager

5.11 Access and Disclosure of Information for Healthcare Purposes

i. Where it is considered reasonable and justified, the Trust will share healthcare information with other organisations.

ii. Where information is to be shared for healthcare purposes, the applicant will be expected to comply with all reasonable requests made by the Trust in order to verify the identity of the requester, check the validity of the request and ensure the instance of sharing is reasonable and justified.

iii. The sharing of information shall at all times comply with the Data Protection Act 2018 (General Data protection Regulations).

iv. Where information is shared, the requester will, in all instances, be required to submit a written application to release the information to the Patient Records Manager.

v. Unless there are essential or mandatory reasons not to do so, the sharing of healthcare information shall be approved by a clinician

vi. The Patient Records Department shall be only responsible for the sharing of healthcare information where the stated reason for sharing is for the purposes of the continuity of care of the patient whose health record is to be shared.

vii. The sharing of information that are covered by the Subject Access Provisions of the Data Protection Act 2018 shall be managed by the Information Governance Department

viii. Unless there is a legal or other mandatory obligation to do so, records relating to fertility or sexual health shall only be released with the explicit consent of the persons whose health records they are.

ix. Where an individual is seeking the support of the Information or Patient Records Departments, which includes the extraction or processing of patient identifiable information and is not for the provision of direct care or is not enacted as a legal obligation: -

- and the intention is for the information to be used for clinical audit purposes then the request shall not be processed unless prior approval has been given by the Clinical Audit Manager (or Deputy)

- and the intention is for the information to be used to research purposes then the request shall not be processed unless prior approval has been given by the Research and Development Manager (or Deputy)

- and the declared intention is for financial purposes then the request shall not be processed unless prior approval has been given by the Head of Income and Contracts (or Deputy)

- and the declared intention is for clinical coding purposes then the request shall not be processed unless prior approval has been given by the Head of Information and Performance (or Deputy)

- and the declared intention is for service improvement purposes then the request shall not be processed unless prior approval has been given by the Quality Improvement Lead (or Deputy)

- and the declared intention is for any other purpose then the request shall not be processed unless prior approval has been given by the Head of Information Governance and Patient Records (or Deputy)

5.12 Access to the Patient Records Department

i. The Patient Records Department now operates from a Central Records Library. These records can only be accessed by Patient Records Staff.

ii. General Health Record services are available between 0830 hrs and 1630 hrs Monday to Friday. All notes can be requested by contacting the Patient Records Department.

5.13 Authority to Act

i. Approving Officers are, for the purposes of this Policy:
- The Chief Information Officer
- Patient Records Manager
- Head of Information Governance and Patient Records

ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer

iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest.

iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Committee at the first opportunity.

5.14 Reporting

i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control.

ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

5.15 Audit

i. The Patient Records department will have authority to carry out spot check audits on records held in various departments. The audit will check that all records are tracked correctly on the Case note tracking function in Meditech.

ii. Clinical Record keeping audits will be carried out annually to monitor the information recorded both electronically and on paper is accurate, Clinical staff will be responsible for this audit. All patient demographic details will be checked against the PAS, this can be supported by the administration staff.

6 Key References

i. The Data Protection Act 2018
ii. The General Data Protection Regulations
iii. The Information Security NHS Code of Practice

iv. The NHS Confidentiality Code of Practice
v. The Records Management NHS Code of Practice
vi. Freedom of Information Act 2000
vii. The Computer Misuse Act
viii. IICSA – Independent Inquiry into Child Sexual Abuse (Guidance notes – Retention Instructions and Data Protection Requirements
ix. BS1008

7 Associated Documents

i. All associated documents are available via the Trust Intranet at: http://imt012/Policies_Procedures_and_Guidelines/default.aspx

8 Training

i. All Trust staff will be made aware of their responsibilities for record keeping. Refer to mandatory training policy for further details.

9 Policy Administration

9.1 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	14/02/2023	None
Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes		
External Stakeholders			
Trust Staff Consultation via Intranet	Start date: 02/2023		End Date: 02/2023

Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)	By Whom will this be Delivered?
The policy is existence already	

Version History

Date	Version	Author Name and Designation	Summary of Main Changes
Oct 2020	8	Wendy Clarke	BS10008 information added
June 2020	7	Wendy Clarke – Patient Records Manager	Up dated retention and destruction information. Further work will be required as new EPR is implemented
July 2018	6	Wendy Clarke – Patient Records Manager	Up dated policy to incorporated EPR
May 2017	5	Wendy Clarke – Patient Records Manager	Amendments added for EPR
January 2014	4.2	Louise Florensa – Corporate admin manager, Wendy Clarke – Patient Records Manager	Amendments subsequent to staff consultation period
October 2013	4.1	Louise Florensa – Corporate admin manager	Inclusion of corporate record management policy
August 2013	4	Wendy Clarke – Patient Records Manager, Louise Florensa – Corporate Admin Manager	Review of previous policy updates & amendments required
August 2010	3	Wendy Clarke - Health Records Manager	Changes to format
May 2017	5	Wendy Clarke – Patient Records Manager	Amendments added for EPR
January 2014	4.2	Louise Florensa – Corporate admin manager, Wendy Clarke – Patient Records Manager	Amendments subsequent to staff consultation period
31/03/2022	8.1	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
31/03/2023	8.3	Russell Cowell, Head of Information Governance and Records	General wording review and re-approval by Information Governance Committee. Update to job title of Head of Information Governance to add “and Records” to title. Re-allocation of policy sponsorship to the Chief Information Officer
31/03/2024	8.4	Russell Cowell, Head of Information Governance and Patient Records	General update and wording review. No significant changes.

10 Equality Impact Assessment

Does The Policy Affect:	Staff		Patients		Both	X

Section 1: **Title of Project Proposal:**	Information Governance and Information Security Policy and Framework
Brief Description of the Project Proposal	Information Governance and Information Security Policy and Framework
EIA Carried Out By (Name & Job Title):	Russell Cowell, Head of Information Governance and Patient Records
Date:	14th April 2023
EIA Authorised By **(Name & Job Title):**	
Date:	
Consultation/Engagement Guidance note: How have stakeholders been consulted with? Who were the stakeholders? What level of engagement took place?	Via the Information Governance Committee

Equality Group	Impact (Positive/Negative/Neutral)
Race (All Ethnic Group)	Neutral
Disability (Inc Physical, long term health conditions & Mental Impairments)	Neutral
Sex	Neutral
Gender Re-Assignment	Neutral
Religion Or Belief	Neutral
Sexual Orientation	Neutral
Age	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Other e.g., caring responsibilities, human rights	Neutral

etc.	

For each protected characteristic, consider whether the impact is positive. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)

Not Applicable

For each protected characteristic, consider whether the impact is negative. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)

Not Applicable

If your assessment has identified any negative impacts, please detail any actions that have been put in place to mitigate these (upon approval of EIA these actions will be shared with the Equality, Diversity and Inclusion Committee):

Outcome	Actions Required	Time Scale	Responsible Officer

Is there evidence that the s. 149 Public Sector Equality Duties (PSEDs) will be met? Consider whether the proposed policy will…

- Eliminate discrimination, victimisation, harassment, and any unlawful conduct that is prohibited under this act
- Advance Equality of opportunity
- Remove or minimise disadvantages suffered by people who share a relevant protected characteristic that are connected to that characteristic
- Take steps to meet the needs of people who share a relevant protected characteristic that are different from the needs of people who do not share it
- Encourage people who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such people is disproportionately low.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. (Consider whether this is engaged. If engaged, consider how the project tackles prejudice and promotes understanding - between the protected characteristics)

Explain your answers below.

The policy is an administrative policy, which implements established legal obligations neutrally.

Does the EIA have regard to the need to reduce inequalities for patients with access to health services and the outcomes achieved? (this section is a requirement for any services outlined within the NHS England and Improvement Core 20 Plus 5 approach to health inequalities) Explain.

The policy is an administrative policy, which implements established legal obligations neutrally.
Section 2: **To be completed by the EDI Manager authorising the EIA** **Anything for noting or any recommendations for consideration by the Board** *Guidance Note: Will PSEDs be met? Are Core 20 Plus 5 services considering patient health inequalities?*

Review Date:	
Additional Supporting Evidence and Comments:	