Leicestershire Partnership NHS Trust

Electronic Health Records Policy (including Record Keeping and Management)

This policy outlines the standards expected of all staff who have access and contribute to patient electronic health care records and the management of the records

Key words: Records, record keeping, management

Version: 2.2

Approved by: Data Privacy Group

Ratified By: Finance and Performance Committee

Date this version was ratified: March 2026

Date issued for publication: March 2026

Review date: 1 March 2028

Expiry date: 30 August 2028

Type of Policy: Clinical and non-clinical – all staff required to record in health records

Contents

Policy On A Page

SUMMARY & AIM

The Trust policy sets out basic record keeping standards that apply to all healthcare records in accordance with local and national recognised standards in order to ensure that staff provide a contemporaneous and complete record of care. The standards provide a structure to enable the review of healthcare records. Compliance with standards will be monitored through the quality assurance processes on an individual basis staff appraisal process and via audit at team and service level.

KEY REQUIREMENTS

- All staff with authorised access to clinical systems and information, have a duty to keep it confidential, secure and in line with the standards and procedures set out in this and other related Trust policies; in accordance with professional standards and A Guide to Confidentiality in Health and Social Care – Treating Confidential Information With Respect (HSCIC 2013) and Data Protection legislation.

- Healthcare records must be recorded **timely, accurately, concisely** and provide an **up to date** account of the assessment and ongoing treatment of an individual patient.

- Access to patient's healthcare records is permitted where there is legitimate clinical, administrative, managerial or reporting reasons.

- Staff must only access a patients electronic patient record using their own access details and must not share their smartcards or other logon information.

- All clinical staff (registered and unregistered) must participate in the Trust's Quality Assurance Processes for record keeping.

- Support is available via the Data Privacy Team lpt.dataprivacy@nhs.net or via the Clinical Safety Officers, or LHIS Servicedesk.

TARGET AUDIENCE:

All employees working for and on behalf of the Trust. People who are not directly employed by the Trust but contribute to and support care delivery and generate health care records including contracted third parties, agency staff, locums, students/trainees, secondees, staff from partner organisations with approved access, visiting professionals, and researchers.

TRAINING

Data Security Awareness Training mandatory training for all staff annually.

There is Record Keeping Training and Prescribing Training available on U-Learn for staff to enrol and complete as required.

1.0 Quick Look Summary

This policy covers all health care records held, used or managed in all formats in use by the Trust.

This policy applies to:

- All employees working for and on behalf of the Trust. People who are not directly employed by the Trust but contribute to and support care delivery and generate health care records including contracted third parties, agency staff, locums, students/trainees, secondees, staff from partner organisations with approved access, visiting professionals, and researchers.
- Any Trust health care records held, maintained and managed by third parties under contract with the Trust.

The Trust has set out basic record keeping standards that apply to all healthcare records in accordance with local and national recognised standards in order to ensure that staff provide a contemporaneous and complete record of care. The standards provide a structure to enable the review of healthcare records. Compliance with standards will be monitored through the quality assurance processes on an individual basis staff appraisal process and via audit at team and service level.

Key points

- All staff with authorised access to clinical systems and information, have a duty to keep it confidential, secure and in line with the standards and procedures set out in this and other related Trust policies; in accordance with professional standards and A Guide to Confidentiality in Health and Social Care – Treating Confidential Information With Respect (HSCIC 2013) and Data Protection legislation.

- Healthcare records must be recorded **timely, accurately, concisely** and provide an **up to date** account of the assessment and ongoing treatment of an individual patient.

- Access to patient's healthcare records is permitted where there is legitimate clinical, administrative, managerial or reporting reasons.

- Staff must only access a patients electronic patient record using their own access details and must not share their smartcards or other logon information.

- All clinical staff (registered and unregistered) must participate in the Trust's Quality Assurance Processes for record keeping.

1.1 Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
2	12 May 2025	Updated policy in new format and review and amendment of all sections
2.1	7 October 2025	Section 13.1 added as per coroner recommendation
2.2	5 March 2026	Addition of information relating to letters and photography and video – minor change

For further information contact:
Head of Data Privacy
Email: lpt.dataprivacy@nhs.net

1.2 Key Individuals Involved in Developing and Consulting on the Document

- Sarah Ratcliffe, Group Data Protection Officer
- Julia Bolton , CCIO
- Pat Upsall, Clinical Safety Officer
- Ruth North, Clinical Safety Officer
- Tom Gregory, Clinical Safety Officer
- Kim Dawson, Classification and Terminology Manager
- Katie Tebbutt, IM&T Change Manager
- Trust Policy experts – see checklist for list of current contact details

1.3 Governance

Level 2 or 3 approving delivery group
Data Privacy Group

Level 1 committee to ratify policy
Finance and Performance Committee

1.4 Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

If you would like a copy of this document in any other format, please contact lpt.corporateaffairs@nhs.net

1.5 Due Regard

LPT will ensure that due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- Strategies, policies and procedures and services are free from discrimination.

- LPT complies with current equality legislation.
- Due regard is given to equality in decision making and subsequent processes.
- Opportunities for promoting equality are identified.

Please refer to due regard assessment (Appendix 4) of this policy

1.6 Definitions that Apply to this Policy

Consent: a patient's agreement for a health professional to provide care. Patients may indicate consent non-verbally (for example by presenting their arm for their pulse to be taken), orally, or in writing. For the consent to be valid, the patient must:

- Be competent to take the particular decision;
- Have received sufficient information to take it and not be acting under duress.
- Be regularly reviewed.

Due Regard: having due regard for advancing equality involves:

- Removing or minimising disadvantages suffered by people due to their protected characteristics.
- Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Proxy: a person authorized to act on behalf of another.

2.0 Purpose of the Policy

This policy provides a framework for the quality of healthcare records. The Trust recognises the importance of maintaining robust and accurate patient information that provides detailed account of patient care to support and enable best practice for the patient and provide justification for any clinical decision making.

The policy includes standards for record keeping and provides support to the organisation in meeting its statutory and legal obligations associated with the management of health care records.

This policy predominantly covers the use and management of electronic patient records but also accounts for any paper records created and held prior to the use of electronic patient records.

3.0 Policy Requirements

Information is the lifeblood of any NHS organisation – essential to the delivery of high-quality evidence based health care and administrative support functions on a day-to-day basis.

The Chief Executive and directors of the Trust are accountable for the quality of the healthcare records that are generated by staff working for or on behalf of the Trust which supports patient safety and quality service delivery.

All health care records must be created, accessed, managed and disposed of in accordance with national standards and professional accountability; and are compliant with legal, operational and information governance requirements. Healthcare records are

an integral part of healthcare practice which is generated on, and behalf of, all health professionals involved in all aspects of patient care (e.g. the care, service and treatment provided).

The primary function of healthcare records is to record healthcare information, which may need to be accessed by the various professionals delivering care. Health care records are generated in a variety of ways including electronic patient records, paper records and digital media.

4.0 Duties within the Organisation

The Records Management Code of Practice for Health and Social Care 2024 has been published by NHSX on behalf of the Department of Health and Social Care and is a guide for use in relation to the practice of managing records. It is relevant to organisations who work within, or under contract to, NHS and Social Care organisations in England. This also includes Public Health functions and where there is joint care provided within and across the NHS. It is based on current legal requirements and best practice.

All NHS records are public records under the terms of the Public Records Act 1958, section 3. As a result, all NHS organisations have a duty under the Public Records Act to make arrangements for the safe keeping and eventual disposal of all types of their records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

4.1 The Trust Board has a legal responsibility for Trust policies and for ensuring that they are carried out effectively. The Trust also has a 'duty of care' and a 'duty of confidentiality' to ensure that all aspects of record keeping are properly managed. The Trust must adhere to the legislative, statutory and good practice guidance requirements relating to healthcare records management. In order to meet these requirements and demonstrate effective healthcare record keeping management, it is necessary to have a clear operational policy.

4.2 The Trust Data Privacy Group are responsible for the approval and monitoring of this policy.

4.3 The Chief Executive has the overall accountability and responsibility for healthcare records within the Trust and this function is delegated to the Medical Director and Director of Nursing, AHP's and Quality, who will be responsible for driving high quality standards of healthcare record keeping and management.

4.4 The Medical Director (and Trust Caldicott Guardian) plays a key role in ensuring that NHS and partner organisations comply with existing national guidance and relevant legislation in regard to handling and safeguarding 'Patient Confidential Data' (PCD). The Guardian will advise staff on matters relating to the management of PCD, for example where issues such as public interest conflicts with duties such as the maintenance of confidentiality.

4.5 The Data Protection Officer (Head of Data Privacy) has responsibility for providing guidance on records management issues where they relate to the processing activities under Data Protection legislation.

4.6 Divisional directors and heads of service / nursing/ allied health professionals are responsible for the quality of healthcare records generated by staff working in the Trust to ensure patient safety and quality service delivery.

4.7 The Head of Information will advise the Trust on how to maintain an efficient and effective patient information system, which complies with all the data collections required within the Trust.

4.8 Managers and team leaders have the responsibility:

- to implement and monitor the operation of this policy within their functional areas.
- Ensure that staff follow and adhere to this policy at all times.
- Ensure that staff are given opportunities for appropriate records management and standards training and awareness.
- Ensure the safe and secure care and storage of records in their remit.
- Ensure that processes and procedures are in place to facilitate effective records management.

4.9 Senior Information Risk Owner is the representative at Board level for ensuring effective management of information risks throughout the Trust which will include the management of healthcare records.

4.10 Responsibility of Staff – All NHS employees have a 'records management guardianship' role especially for any records that they create, but also generally for any records that they use on the course of their duties. This includes completion of training to meet any mandatory or additional identified learning and development needs required to fulfil those responsibilities. All staff are;

- Responsible in law for any records they create and use;
- Must be aware that any records they create are not their personal property, but belong to LPT;
- Should understand their responsibilities under Data Protection Legislation when using or communicating personal data and information;
- Should share records and the information they contain only in accordance with professional standards, local policy and information sharing agreements.

4.11 The person responsible for generating correspondence to patients (Lead professional, Healthcare Professional/Clinician) – It is the responsibility of the person writing or dictating the letter to ascertain and record in the patient's health record;

- Whether the patient wishes to receive a copy of correspondence;
- How they wish to receive it;
- The address to send it to;
- In what format;
- In the case of children, who has parental responsibility;
- Arrange with a designated person/member of the administrative team for this to take place.

NB Where the patient requests correspondence being sent electronically, please see '*Use of Electronic Messaging to communicate with Service Users Policy'*.

5.0 Record

A record comprises of recorded information in any format e.g. digital or physical of any type, in any location (e.g. central database server, PC, filing cabinet, archive store), which is created, received or maintained by LPT in the transaction of activities or the conduct of its affairs, and kept as unique evidence of such activity. A Health Record is defined in Section 205 of the Data Protection Act 2018 as;

(a) consists of data concerning health, and
(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.

Records management is the process of controlling records from their creation, usage, maintenance, and storage to their ultimate destruction or permanent preservation.

The term Records Lifecycle describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

6.0 Clinical Record Keeping

Good record keeping is an integral part of professional practice and is essential to the provision of safe and effective care. It is not an optional extra to be fitted in if circumstances allow. As well as individual Professional Codes of Practice there are also national standards, legislation and regulations that must be met to ensure good clinical record keeping practice.

These include:

- Care Quality Commission (CQC): Fundamental standards Regulation 17, Good Governance covers the record keeping requirements;
- Data Security and Protection Toolkit: Information Governance covers the way organisations 'process' or handle information and includes both corporate and clinical information. The Data Security and Protection Toolkit draws together the legal rules and central guidance and presents them in one place as a set of information governance requirements;
- Accessible Information Standard 2016: to make sure that people who have a disability, impairment or sensory loss are provided with information that they can easily read or understand and with support so they can communicate effectively with health and social care services.

6.1 Record Keeping Functions

Good record keeping has many important functions. These include;

- Supporting patient care and communications;
- Supporting the involvement of the patient in their healthcare;
- Supporting effective clinical judgements and decisions;
- Promoting better communication and sharing of information between members of the multi-disciplinary teams Helping to identify risks, and enabling early detection of complications;

- Supporting the delivery of services;
- Helping to improve accountability;
- Showing how decisions related to patient care were made;
- Making continuity of care easier;
- Providing documentary evidence of services delivered;
- Helping to address complaints or legal issues;
- Supporting clinical audit, research, allocation of resources and performance planning.

6.2 Types of Clinical Records

The principles of good record keeping apply to all types of records, regardless of how they were held. Examples of records that should be managed using the guidelines are listed below. The list includes functional areas as well as the format;

- Patient health records
- Administrative records (including, for example, personnel, estates, financial and accounting records)
- Integrated health and social care records
- Data processed for secondary use purposes – any use of personal level or aggregate level data that is not for direct patient care

Format:

- Photographs and other images
- Audio and video tapes/cassettes
- Emails – clinically relevant to the care of the patient (see *Use of Electronic Messaging to communicate with Service Users Policy'* for more detail).
- Text messages (SMS) and social media (both outgoing and incoming) – transposed into the record
- Websites and intranet sites that provide key information to patients
- Paper records (case notes)
- Electronic patient records
- Pictures and videos

6.3 Consent

As a public authority, (i.e. the NHS) the Trust does not rely on consent as a legal basis to process service user and staff information. However, staff should always consider gaining consent from service users and staff when considering whether to share information, as a balance against the common law duty of confidence. Staff should be aware that consent under common law duty of confidence is not the same as consent as a legal basis for processing and the enhanced requirements for consent under Data Protection legislation do not apply. Consent to share information should be recorded on the service user's health record and must be regularly reviewed to ensure that patients have the ability to change their preferences. Where consent is the legal basis for capturing information i.e. not for direct health care but for use of information in promotional material, patients must be provided with details when consent is sought of how they change their consent choices.

6.4 Privacy and Shared Records

Some services may feel the need, based on conversations with the service user, to store certain types of information using enhanced privacy functionality, within or outside of the Electronic Patient Record. Advice and guidance must be sought from the Data Privacy Team via lpt.dataprivacy@nhs.net prior to changes being made.

The types of information this relates to can vary but is generally deemed to have a higher level of sensitivity than other information, such as case notes/assessment interpretations about a traumatic event; formulation notes that only that clinician needs to view; uploaded documents that may support clinical working such as a postmortem report of a family member and also very specific clinical assessment tools that have stipulations from the owner of the tool (e.g. Pearson) for the information to be stored securely and that only certain individuals/clinicians can view the document.

Record Alerts and Reminders

Every user has a responsibility when accessing an electronic health record to note and act on any alerts or tasks within the record. These include but are not limited to:

- Patient Status Alerts
- Tasks
- Safeguarding
- Looked After Children
- Reasonable Adjustments

6.5 Online Services

Electronic Health Records functionality may include different types of online services for service users to directly access their health record and or communicate with health professionals. Where consent for communication preferences is recorded for a patient, this includes access to information and communication via online services.

Where a relative or carer is acting on behalf of the patient and consent has been given a consent form will be completed and signed by both parties. Where consent is not possible due to lack of capacity, proof of legal responsibility is required such as Power of Attorney. In some cases, proxy access may not be able to be granted where a safeguarding concern has been raised. For additional guidance refer to the relevant system SOP.

6.6 Filming and Photography in clinical care

This policy provides guidance for healthcare professionals and it ensures compliance with statutory requirements:

- Filming for clinical documentation
- Filming for education, training, or research
- Filming by patients or visitors
- Use of photography

Filming in clinical settings must comply with:

- UK GDPR and Data Protection Act 2018

- Common Law Duty of Confidentiality
- Human Rights Act 1998 (Article 8 – Right to Privacy)
- General Medical Council (GMC) and Nursing & Midwifery Council (NMC) guidance
- Caldicott Principles

There must be a fully justifiable purpose for any photography and video recordings of *vulnerable* patients, approved at consultant level. The purpose for the recording should be detailed in the record.

All clinical recordings of patients form part of the healthcare record and must be documented and stored according to policy. Clinical recordings containing patient identifiers are classed as personal data, therefore the loss of any clinical recording is a breach of security and confidentiality and must be reported.

Sensitive' photography should be managed in the same way as all images/recordings.

All recordings must be retained in line with national guidelines for health records. Recordings should be catalogued so they can be clearly identified and retrieved, preferably incorporating the patient's NHS number and the date of recording. All recordings should be stored securely as soon after the recording as is practicable.

Consent Requirements

Consent is not always required for recordings made solely for direct care (e.g. wound photography), but patients should be informed. Recordings become part of the clinical record and must be stored securely.

Explicit written consent is required when recording for Secondary Purposes (Teaching, Research, Media). Consent must be:

- Informed – patient understands purpose, audience, and use.
- Voluntary – no coercion or undue influence.
- Documented – using a standardised consent form.
- For Children and Adults Lacking Capacity consent must be obtained from a parent, guardian, or legal representative. Best interest decisions must be documented.

Consent forms for photography, filming or recording for the use in internal and external communications are available from the communications team or via StaffNet. Patients have a right to withdraw consent for the secondary use of their recordings at any time, and further processing should be stopped at the earliest opportunity.

Filming by Patients or Visitors

Patients may record their own consultations for personal use under UK GDPR exemptions. Staff should be informed and given the opportunity to consent or decline.

Covert recording is discouraged but not illegal; however, uploading such content may breach privacy laws and staff rights.

Patients/service users and the public are not permitted to make recording or take images outside of their personal consultations in a hospital setting without any prior agreement from a senior manager on site, this includes in-patient and clinic areas. This approval is needed to ensure that other individuals are not captured in recordings and to preserve privacy and dignity. In the event that this type of recording is identified individual should be asked to stop recording and the images deleted. If individuals refuse to stop recording or delete images after being asked, these individuals must be told that if they publish images or share with third parties in any way, they will be committing an offence, and the Trust may take action to report them to the relevant authorities. If unauthorised filming actions become aggravated security must be called and the police where necessary.

Where a family member, carer or friend has videoed a patient with or without their knowledge whilst they are unwell or displaying symptoms. The family member, carer or friend shows the video and/or would like to send a copy of the video to a health professional involved in the patients care. Where the patient has capacity consent must be sought. Where the patient does not have capacity, but it is in the patient's best interests then it is appropriate to view the video. Please ensure that the patient record has been updated as a full record of the considerations made.

For more detail refer to the Trust Social Media and Communication Policy.

7.0 Health Record Keeping Standards and Guidance

The purpose of a healthcare record is to facilitate the care, treatment and support of a patient. In order to ensure that healthcare records are created in a consistent and professional manner the 'Healthcare Record Keeping Standards' outlined within this policy should be adhered to at all times.

Staff must explain to the patient any care or treatment they are planning on carrying out, the risks involved and any other treatments possible. They should also inform patients how the service will share their information with others as part of their direct care. Patients should be informed about the Trust Privacy Notice and Children's Privacy Notice which gives them the relevant information about the Trusts purpose for collecting and using information about them.

The Trust's healthcare records are predominantly held on the Electronic Patient Record (EPR) which has safeguards in place to protect the integrity, accessibility and accuracy of the record. Where there are paper records, the healthcare professional is personally responsible for their compliance with standards. The principles of effective healthcare record keeping are;

- **Accessible to all staff that require access in order to enable them to carry out their duties** – information must be stored in the correct areas of the EPR and entered via approved data entry formats where they exist as defined within Service Standard Operating Procedures or seek advice if uncertain.

- **Understandable, clear and concise** – Healthcare records must avoid the use of

jargon and technical terminology as the patient must be able to read and understand what is written about them. The record may also be accessed by other professionals for the purposes of health and care delivery, and they must be able to understand what is written. Abbreviations should not be used within the healthcare record. Where a health professional wishes to abbreviate anything, this should be written in full in the first instance with the abbreviation written in brackets.

- **Factually accurate and relevant** – Healthcare records must be a factual record of care that is delivered and where possible, collateral evidence should be sought. The record must not contain irrelevant information or personal opinions.

- **Secure** – When accessing records, staff must ensure that this is done using a Smartcard and PIN or other forms of multi-factor authentication where system functionality allows.

  For Smartcard compliant systems Username and password must not be used unless there are issues with the smartcard software/system. All users are required to follow the business continuity plan for the systems they use in the event of an incident.

7.1 Minimum Dataset

All health records will contain the minimum data set of personal details in addition to any health record keeping standards. This will include but is not limited to the following;

- Full name (including first name, last name, known as and title)
- Address, postcode and Telephone number
- Gender
- Ethnicity
- Date of Birth
- Communication need
- NHS Number
- GP Address and Telephone number

- Next of Kin
- Emergency contacts
- Reasonable adjustments

7.2 Record Keeping Standards

Staff must keep clear, accurate and legible records, reporting relevant clinical findings, the decisions made, the information given to patients, and any drugs prescribed or other investigation, treatment or care. Clinical records must provide a safe and effective means of communication between appropriate members of the care team – including the patient themselves. Where there are hard copy records, the location of the records should be recorded on the clinical system. It is important that all records are able to be identified and traced in order to provide prompt access when required.

Clinical records **must**;

- Be recorded within the electronic clinical record, exceptions to this should be approved by the Data Privacy Team lpt.dataprivacy@nhs.net
- Be complete, consistent, accurate and consecutive;
- Be factual and not include unnecessary abbreviations, jargon, meaningless phrases or relevant speculation;
- Only state relevant and useful information;
- If abbreviations are used, they must be written in full in the first instance;
- Be recorded as soon as possible after an event has occurred or a contact taken place, providing current information on the care and condition of the patient. This should be within 24 hours, if not, the reason for the delay must also be recorded for retrospective record keeping;
- Scan any relevant clinical information onto the Electronic Patient Record in a timely way and in accordance with the Trust Clinical Document and Scanning Policy;
- When the care being delivered has been delegated to an unregistered member of staff, the registered member of staff accountable for that patient must ensure that relevant entries are made in the record to reflect this;
- Identify any risks or problems that have arisen and action taken to rectify them;
- Be held securely and confidentially;
- Be recorded / written, wherever possible, with the involvement of the patient, carer or patient;
- The information contained within records must be used for the purpose for which it was obtained and only share appropriately and lawfully.

Clinical records must include;

- Registration/referral details of the patient. The information recorded must include the minimum dataset (as outlined in section 7.1) including emergency contact/next of kin details. This information should be checked on first contact with the patient and then regularly to ensure that the information is up to date and accurate.
- Medical referral details and related previous medical history.
- Any alerts such as allergies and safeguarding.

- Clinical observations: examinations, assessments, tests, diagnoses, medications, and any other treatments.
- Other relevant information/assessments/forms such as Assessment of Capacity (Mental Capacity Act), Lasting Power of Attorney, Advanced Directives, or statements.
- Evidence of the care planned, risks assessed, the decisions made, the care delivered, and the information shared.
- Evidence of actions agreed with the patient, including consent to care and treatment.
- Relevant disclosures by the patient – pertinent to understanding the cause or affecting the care/treatment.
- Details of facts and information given to the patient
- Correspondence to and from the patient, referrer and/or other parties
- Appropriate discharge/transfer of care documentation
- Record keeping can be delegated to undergraduate students so that they can document the care they have provided. As with any delegated activity, the appropriate registered professional is required to countersign all undergraduate student entries.

.

Clinical records must not;

- Include coded expressions of sarcasm or humorous abbreviations;
- Be kept for longer than is necessary;
- Contain references to complaints – complaints may be unfounded or involve third parties and inclusion of this within the health record will mean that information will be preserved for the life of the record and cause detrimental harm and /or prejudice to the relationship between the health care professional and the patient;
- Include references or entries to private work conducted by a Trust clinician – where Trust clinicians are also undertaking private work outside of their NHS work, it is important that any documentation relating to this work is not record or saved onto the patients NHS record or letters recorded on Trust headed documents.
- An alternative record must not be created outside of the Trust record unless there has been approval from the Data Privacy Team based on a risk assessment.

Third Party Information:

Where information is needed to be added to the patient's EPR that has been provided by a 3rd Party, and this must be considered for redaction from any Subject Access Request (SAR) or from online access by the patient themselves.

- It is recognised that there are many reasons why this might be required for example where a parent is unable to support your patient in their normal capacity due to health or social care needs.
  Or,
- When a patient relative shares information or concerns about the patient that needs to be added to the EPR but may result in potential risk to the relative if this is shared to the patient directly.

Third party information should only be entered into the clinical record on an occasion

when work is completed with family member or carers that supports planning care for the patient, often identified in group or family therapy work. The detail is recorded in the patient EPR but does not pertain to the patient.

Where your service uses SystmOne the 3rd Party Information Template can be used. A trust wide template has been developed and published on the clinical tree in all SystmOne units as 'Third party information template'. Any information regarding a third party which is appropriate to be recorded must be recorded in this template and saved using the 'zzz Third party information on patient record (redacted online)' option in the event details template. This will redact the information from the patient's online record, in line with the current NHS England guidelines on redacting information for online records access.

Patient or Parent Held Records

Where patients/or parents hold their own, or their child's records, they must be made aware of the importance of these records for health care professionals and the need to keep them safe. Where these records are required to remain the property of Trust, patients/or parents must be made aware that these records are an official health record and as such will need to be returned to the Trust when requested and where possible collected at the final contact.

Patient held records must have the contact details of the team delivering the care and treatment so that the record can be returned to the team when required. On completion of the care and treatment any patient held record must be scanned and uploaded to the EPR. The record should be scanned as a complete document as determined by the Service Standard Operating Procedure.

Staff as Patients

It is recognised that there may be occasions where members of Trust staff will be receiving services within the Trust. It is important to remember that **all** patients/service users expect that their confidentiality is respected and that their health records are maintained accurately and securely.

Where a staff member is being treated as a patient, it is important for their lead clinician to ensure that they understand the need for recording the care and treatment provided and provide assurance on the functions with the electronic clinical system to ensure only those involved in their care, have access to all relevant information.

The need to explain the 'sharing preference' within the clinical system is imperative, in order to ensure that the correct settings are enabled and where the staff member indicates, restrict the sharing through using dissent to share.

In addition, in the event of a concern being raised requests can be made through the Data Privacy Team, to undertake audits of access to the clinical record as part of an investigation.

7.3 Retrospective Record Keeping

Record keeping standards state that the healthcare professional should make a record at the time that the event occurs or as soon as possible afterwards. However, it is recognised that it is not always possible e.g. if the EPR is not available. In these cases, an electronic document (e.g. Word) should be completed and saved at the time and uploaded or copied into the patient record when next connected.

A paper written record should be a last option used and staff must ensure the information noted in this way is entered into the EPR as a full record on the relevant template/recording tool within the system as soon as possible. The paper record must be confidentially destroyed after consideration is made whether the document also needs to be scanned onto the system.

If the record entry is late (being written in retrospectively) the EPR entry should be dated at the date and time of the contact with the patient. The entry should start with the date the notes were taken and a brief reason why there was a delay in entering them. If someone has recorded an entry in the time before your contact and your writing up, then you should use your judgement to decide if you take any further action to keep them informed and ensure this is recorded.

8.0 Record Lifecycle and Management

8.1 Creation of a Health Record

Records must provide a contemporaneous and complete record of care. The content should be in a standardised format and layout. The records must be completed with relevant information contained in chronological order, within the appropriate sections see Section 7.1 for expectations.

Once a new patient has been received into a Trust service, if a record does not already exist, a record will be created via the registration onto the EPR see Section 8.1.1. Where it is evident that the patient is not registered on the clinical system, the team who have received the referral will register the patient. Details of the patient will be collated from the referral (which will be linked to the registration), and if possible, supplemented or backed up by information gained directly from the referrer or the patient themselves.

8.1.2 Creation of a local electronic or patient record

There are specific instances where the creation of a local patient record is permitted:

Electronic:

- Where an existing record cannot be located, in the first instance the known GP should be contacted to verify information
- Overseas visitor where they are not registered for an NHS Number or with a GP

Paper refer to Section 7.3:

- Where there is a requirement for personal safety i.e. witness protection based on advice from the legal team
- Business continuity in the event of system failure after referring to the

service level business continuity plan

8.1.3 Consent

In general, consent to treatment means a person must provide permission before receiving any medical treatment, test, or examination. This principle is supported by both legal and ethical considerations, reflecting a patient's right to make decisions about their own body. However, there are exceptions, particularly within the context of the Mental Health Act (MHA) and specific provisions related to treating individuals with mental disorders. There is a difference between consent to treatment and consent under the Data Protection Act 2018. The Trust's Privacy notice outlines the basis for recording of health and care information which is summarised below:

Personal data provided to the Trust for the purpose of healthcare delivery, management and treatment:

> 6(1)(e)Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Special Category Personal Data provided to the Trust for the purpose of healthcare delivery, management and treatment:

> 9(2)(h) Necessary for the reasons of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

Patients should be informed that a health record will be created, and their consent preferences for sharing of their record and contact preferences obtained by the clinician who is seeing them.

Staff must advise patients who can access the record, where it will be shared and the purpose for the access. This should be clearly recorded in the consent template within the system.

If a patient wishes to dissent from having an electronic record advice should be sought from the Data Privacy Team, who will advise on the legal basis for holding information relating to healthcare.

8.1.4 Audit Trail

All electronic health records will have an audit trail comprising of the date it was created, details of all the additions, changes, deletions, and access. The audit trails are record of the digital fingerprint of the record. All staff must ensure when accessing records that they provide sufficient detail to the record to identify reason for access.

Staff should be aware that patients have a right to request a copy of the audit trail that belongs to their record, as part of their right of access under Data Protection legislation and also under the Computer Misuse Act 1990 where a concern has been identified.

Privacy alerts may be generated where a record is accessed that is not registered or currently part of an active caseload. This will prompt staff with the appropriate access to review the rationale provided on accessing a record and where inappropriate record access is suspected lead to an investigation.

Where records are being accessed for the purposes of research evaluation a reason for accessing the record must be added, including, role, name, research number (Integrated Research Application System number) to aid openness and transparency.

8.2 Clinical Documentation

Following an assessment of the patient, the assessment and outcomes must be recorded on the EPR using the approved clinical recording tools within the system. Paper records must only be created by exception and based on a clinical need.

It is recognised that different services and specialities require specific documentation to meet their professional requirements, but the Trust is committed to ensure consistency in the documentation and processes across the organisation. There is an expectation that with relevant clinical tools created within the EPR, information will be entered directly into the system, therefore reducing the risk of errors and loss of information.

Cutting and pasting of information within and out of the EPR presents increased risk of information being incorrectly inserted into the wrong patient record, omission of key information leading to documentation/records being incomplete, and inadvertently recording an amendment to a record on the electronic fingerprint. Where a staff member has two records open at the same time care must be taken to avoid the risk of pasting information to and from the wrong record. Where services are required to copy and paste information from an external agency into the record the service should ensure a SOP is in place and regular accuracy audits are in place.

Individuals must always ensure that any information copied into the record is accurate and complete based on the available documentation.

Emails are able to be copied and pasted into the record for the approved process please refer to Use of Electronic Messaging to Communicate with Service Users Policy.

Where an approved method of Artificial Intelligence is used to generate clinically relevant information the approval process must include the safety guidance around how this is transferred into the clinical record. For more information contact lpt.dataprivacy@nhs.net and your directorate Clinical Safety Officer.

Any paper clinical documentation should be scanned and uploaded to the EPR using the approved methods outlined in the Clinical Document Scanning Policy. Where Optical Character Recognition must only be used when scanning where advice has been sought from the Data Privacy Team lpt.dataprivacy@nhs.net..

Historic paper records cannot be scanned onto the EPR; however, they must be stored securely in line with the Records Management Code of Practice for Health and Social Care 2021 for advice contact lpt.dataprivacy@nhs.net.

Paper records kept in the home must be collected on discharge or when care is ended and scanned on the EPR. When staff take patient records to the home environment, it is essential that the clinician makes it clear what records are the responsibility of the Trust and will be retrieved on discharge/death.

See section 6.3 for confidential paper records that have been approved to have controlled access.

8.3 Retention and Destruction

8.3.1 Keeping Records Secure

Maintaining the integrity of information is important for all records and this includes keeping records secure. More specifically maintaining the security and confidentiality of information is vital for clinical records to protect patient confidentiality. Where paper records are in active use the reasons for holding a repository separate to the Trust clinical systems specific approval needs to be sought from the Data Privacy Team.

A sensible balance needs to be maintained between the needs of accessibility and convenience of records and the security and confidentiality required.

Record files and encrypted portable equipment should be stored under lock and key when not in use. Staff should not leave computers, paper records or files containing confidential information unattended in vehicles or in easily accessible places. Staff should not normally take health records home, and where this cannot be avoided, procedures for safeguarding the information effectively must be agreed with the relevant senior manager.

In addition, all EPR systems must be secure and protected by smartcard access, or by Multi Factor Authentication or similar access control mechanisms, and staff must not share their cards or credentials. For further information refer to the Information Security Risk Policy and the Digital Acceptable Use Policy.

8.3.2 Process for Retention and Disposal

Under Data Protection legislation, all health records may be subject to disclosure even if they have been held outside of the NHS England Records Management Code of Practice by LPT.

It is therefore important that the retention and disposal of records which is defined at the point in the records lifecycle when they are either transferred to an archive or destroyed in accordance with clearly established procedures, local and national schedules and enforced by appropriately trained and authorised staff.

Minimum retention schedules are laid down in the Records Management Code of Practice NHS England 2024. This code of practice will form the basis of LPT's local retention schedules which will be developed over time with local decisions on retention recorded against the national schedules and made available to staff.

All clinical health records are confidential so, when required, they must be destroyed using confidential destruction methods and must only be destroyed via confidential shredding onsite. Where hard copy health records are destroyed a certificate of safe destruction i.e. Destruction Certificate, is required.

8.4 Storage and Security – Paper Records

The location and storage of paper records is important as it can impact on their availability and their long-term preservation. Records held on local sites must be stored in locations which are easily available to any member of staff who may need to retrieve them and not retained there for more than 3 months. See Section 8.1.2 for information on when it is appropriate to create a local paper record.

Paper records must always be kept securely and contained in a locked room or cabinet when on local Trust sites. A sensible balance must be achieved between the need for security and accessibility. The record store must be in an environment that does not cause damage or decay to the documentation.

Secure off-site storage is available and should be used to store all paper clinical records that are not required for active use. Clinical paper records are retained in off-site storage for the remainder of their retention period until the requirement for confidential destruction.

For further information refer to the Digital Acceptable Use Policy.

Where it is not possible to meet the above requirements contact the Data Privacy Team for advice.

8.4.1 Labelling and Packaging of paper records for transporting

When records are being delivered to another location they must be;

- Correctly addressed to a named individual detailing their role, service / department and location;
- Marked ‘NHS Confidential’.

It is the senders responsibility to ensure the records are sent to the correct location by secure means whether this is internal transport (portering service), recognised courier or off-site storage provider transport.

It is good practice to email the recipient to notify them that the records are being sent and to ask for a confirmation email when they have arrived. This ensures that records are transferred in a timely manner and any non-delivery can be followed up promptly.

8.5 Mobile and Home Working

It is recognised that there is a need for some staff to work from other locations including at home. There are more specific requirements and guidelines relating to this in the Trusts *Information Security and Risk Policy* and *Agile Working Policy and Information Record Lifecycle Policy.* Staff undertaking this type of work must refer to that guidance

as well as these relevant points.

- Staff must have permission from their managers to undertake mobile or homeworking and be aware of their responsibilities;
- Ensure appropriate security measures are identified and followed for both electronic and hard copy records. This includes encryption of electronic data and logging out when you are not using your laptop. The use of secure containers for paper records in transit and at locations e.g. lockable briefcase, secure mail pouch or filing cabinet;
- Confidentiality: records must not be accessible to unauthorised persons e.g. family or friends at home or by commuters whilst travelling;
- Tracking: records must be able to be traced;
- In some circumstances it may be necessary to store clinical or corporate documents on the desktop for a short period which is more secure than printing and carrying paper records. It is essential that this is only for copies of records that are held primarily within the clinical or corporate systems or networks. Any documents stored in this way must be deleted at the earliest opportunity.
- Where paper notebooks or diaries are used personally identifiable data must not be included.
- All paper notes and documents including notebooks and diaries must only be disposed of at a Trust site via confidential waste and this must be completed regularly to ensure that sensitive and commercial information is not at risk of breach.

Remember, it is the individual's responsibility to safeguard the information they are using and noncompliance with policy could result in disciplinary action. For further information refer to Section 10 of the Agile Working Policy.

9.0 Scanned Records

The primary clinical record is now held in an electronic format which brings many benefits to the care of the patient. Where paper is created it is a requirement that these records are scanned and added to the electronic record in a timely way to ensure that records are complete and contemporaneous. The full process for scanning and uploading documents and more detailed guidance is set out in the Clinical Document Scanning Policy and Procedure.

For scanned records, the main consideration is that information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an authentic record and there are technical and organisational means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.

10.0 Sending Correspondence to Service Users / Patients and Other Health Professionals

Where sending communication electronically to service users please also refer to the Trust's Use of Electronic Messaging to Communicate with Service Users Policy.

Shared decision making is a collaborative process that involves a person and their healthcare professional working together to reach a joint decision about care. It could be care the person needs straightaway or care in the future, for example, through advance care planning (NICE NG197 Shared Decision Making). This includes all correspondence sending electronically and via paper.

When writing clinical letters after a discussion, they should be sent to the patient (unless they say they do not want a copy) and to the relevant healthcare professional.

Care must be taken not to leave a letter in draft format. All letters must be sent in a timely way in accordance with national guidance and local standard operating procedures. This is to ensure that clinical care is based on accurate finalised information.

Where the people who use services are not legally responsible for their own care (for instance a young child, or a child in care), letters should be sent to the person with legal responsibility, for instance a parent or guardian.

People need to be offered resources in their preferred format to help them understand what was discussed and agreed. This could be a printout summarising their diagnosis, the options and decisions or plans made, and links to high-quality online resources. Ideally, people should be given this material to take away or provided it very soon after the discussion. A discussion in this context is any interaction (in person or remote) between a healthcare professional and a person using services in which a healthcare decision might be made.

Ensure that information provided after discussions includes details of who to contact with any further questions.

Additional support should be offered to people who are likely to need extra help to engage in shared decision making, this could include encouraging them to record the discussion, explaining in writing the decisions that have been made or arranging follow up by a clinical member of staff or a suitable alternative.

The letter should do three main things;
1. Record relevant facts about the patient's health and wellbeing;
2. Present information in a way that improves understanding;
3. Communicate a management plan to the patient and the referrer.

10.1 Consent to Receipt of Letters and Recording Correspondence Preferences

In line with the overall NHS policy of supporting health and care through communication service users may be contacted using a variety of methods. It is for each patient/service user to decide whether they wish to receive copies of letters, care documents or communications about them by health professionals. This choice can be recorded into the electronic patient record using the appropriate functionality within the record.

The aim is that within a consultation, the possibility of receipt of communications should be raised as part of the wider discussion about ‘what will happen next’. In other words, patient/service users should routinely be asked during a consultation and any related tests or interventions, and there should be a clear process for recording their views, similar to that for recording their consent to treatment.

If there are any doubts about the patient/service user's mental capacity to make a decision about receiving communications, an assessment of their capacity can be undertaken by the treating clinician and recorded in the patient/service users clinical records.

The following should be adhered to when recording communications:

- **Where recorded:** In almost all cases, the discussion with the patient/service user and his/her response to having copies of letters will be recorded on their electronic patient record.

- **Recorded by who:** Usually, the clinician in overall charge of the care of the patient/service user will complete the record. For detained patient/service users, this will be the responsible clinician however, other clinicians can make entries in the record when relevant

- **When recorded:** The patient/service user should be asked about receiving copy letters as early as possible in their care and treatment episode (or pathway) within the Trust. Their reply should be kept under review by the clinician in charge of treatment.

- **Has contact information been verified:** The patient/service user should be asked regularly to verify the contact information held for them and this clearly recorded alongside the contact information along with the date of verification. This includes postal address, email address and phone number and details where the numbers belong to a third party. For further guidance refer to service Standard Operating Procedures or seek advice.

10.2 Sharing Correspondence

- **Adults:** Some adults have carers, family members or others who are actively involved in their care. Frequently patients/service users want information shared with their carers and/or family members. With patient/service user consent, copies of letters can be sent to these persons. Copies of letters to carers may be particularly important where medication is changed following discharge from hospital. In the absence of a clear legal framework for deciding what to do, health professionals will often have to exercise judgement in deciding whether it is in the patient/service user's best interests to share information with a carer. If the person is a young carer, any information must be appropriate to age and understanding of the young person. Best interest decisions made by clinicians on behalf of patients/service users who lack capacity to make a decision on the involvement of a carer must be fully recorded in the patient/service user's record.

  Sometimes the patient/service user will not want a letter copied or shown to the carer. Both the patient/service user and the carer have the right to expect that information provided to the service will not be shared with other people without their consent. In such circumstances, unless there is an over-riding reason to breach

confidentiality, the wishes of the patient/service user must be respected. The DH expects that carers of people with mental illness should be provided with as much information as possible to enable them to carry out their caring role as effectively as possible without breaking the patient/service user's confidentiality.

- **Children and young people:** It is expected that young people aged 16 and 17 will be offered copies of letters. It is up to healthcare professionals to assess the competence of younger children to understand and made a decision (referred to as Gillick competence). It is good practice to offer adolescents consultations alone so that they have the opportunity to speak freely and give information that they may be unwilling to talk about in front of their parents. In such cases, young people may prefer to collect in person copies of letters giving personal information rather than having them sent to their home.

  The issue may arise as to whether a letter should be copied to the young person or their parents. Some initiatives in copying letters have been developed in children's services, and the general reported experience is that there are few difficulties, as long as the issue is discussed with the family. Often adolescents appreciate the letter being sent to them. Where parents are separated, it is important to discuss who should receive the copies of letters.

10.3 Circumstances When Copying Correspondence is not Appropriate

There may be reasons why the general rule of copying letters to patient/service users should not be followed. These include;

- Where the patient/service user has expressed the wish not to receive a copy. A reason does not have to be given;
- Where permitting access to information contained in the letter would be likely to cause serious harm to the physical or mental health condition of the person to whom the letter relates or any other person (including a health professional); a decision not to disclose a letter or report applying the 'serious harm' test. This will be a matter of clinical judgement. The provision to withhold information has a statutory basis in the Data Protection (Subject Access Modification) (Health) Order 2000. If a letter is withheld, the reason must be recorded in the patient/service user health records.
- Where information in the letter relates to a third person unless that person has consented to the disclosure or could be fully anonymised. Another health professional is not deemed to be a third party (refer to the Trust Data Protection, Caldicott and Confidentiality Policy for more detail on this exemption);
- Where there are specific security considerations particularly in secure settings;
- Where a case is particularly sensitive, for example, child protection, it may not be appropriate to copy the letter. A child protection matter may have been reported and is under investigation. The best interests of the child must come first;
- Giving of 'bad news' is not in itself enough to justify not copying a letter. When the DH introduced this initiative, pilot studies showed that sometimes the case that health professionals are anxious to protect patient/service users, who themselves often wish to have as much information as possible, even if it may be 'bad news' or uncertainty.

10.4 People with Information and Communication Support Needs

The information needs of patients and their preferred methods of communication must always be considered by Trust staff when preparing information. In 2016 the 'Accessible Information Standard' was launched and has now been superseded by the reasonable adjustment digital flag.

This directs and defines a specific, consistent approach to identifying, recording, flagging, sharing, and meeting the information and communication support needs of patients, service users, carers, and parents, where those needs relate to a disability, impairment, or sensory loss. The Standard is a legal requirement and applies to service providers across the NHS and adult social care system. Effective implementation requires organisations to make changes to policy, procedure, human behaviour and, where applicable, electronic systems.

Organisations must follow the Standard and complete five distinct stages or steps leading to the achievement of five clear outcomes and must also record where there are no needs:

1. Identification of needs
2. Recording of needs
3. Flagging of needs
4. Sharing of needs
5. Meeting of needs.

To this end, the following must be recorded in patient records:

- The information given to service users, their families, and carers at key points on their care pathway
- The format the information was provided in to meet the needs of the patient
- If a patient information leaflet has been provided to the service user, family, or carer to support such discussions, this should be clearly documented in the health care record stating the full title and version number. Where practical a copy of the leaflet should be retained in their record
- Where a service user makes clear (verbally or non-verbally) that they do not wish to be given this level of information, this too should be documented in their health records

If it is not clearly documented, the discussion did not take place. Auditing of reasonable adjustment flags should be reviewed within record keeping audits.

10.5 Correcting Inaccurate Records and Record Deletion

Where an entry has been made in error there is the ability within electronic health records to "mark in error" an incorrect entry. This will show as a striked through entry within the record and clearly shows that it has been marked in error. This allows there to be an audit trail of actions taken within the record.

A health record entry must only be removed or deleted when approved by the staff member who holds the Caldicott Guardian access rights within the Electronic Patient

Record, and only in certain situations.

A data subject (the patient/service user) has a right to have inaccuracies corrected and also to have opinions revised if based on inaccurate information. In every case where the accuracy of data is challenged by the data subject, the matter must be fully and promptly investigated.

A challenge to the accuracy of data should normally be made in writing however, if the challenge is made by the data subject in person and their identity is not in doubt, the challenge can be dealt with. All reasonable steps should be taken to resolve the issue and the data subject must be informed of any corrections made. Where a request has been made to amend factually accurate information within the clinical record the data subject has a right to have a note added to the record to add a comment to the record that they are not happy with the entry that cannot be removed or amended.

In all cases where a correction cannot be made, or the data subject is dissatisfied with the outcome, the Trust's Data Protection Officer must be informed. The Data Protection Officer may contact the Trust's Caldicott Guardian for a final judgement.

10.6 Protecting Confidentiality

When health professionals send letters or other correspondence via a digital solution or paper, staff should ensure they consider security and confidential procedures to minimise the following risks:

- Breaches of confidentiality of the patients/service users own information where communications are misdirected or read by someone other than the patient or his or her authorised agent;
- Breaches of confidentiality of information of third parties;
- Breaches of confidentiality of letters kept insecurely.

Procedures must be in place to minimise the likelihood of information being accessed by unauthorised people and ensure patients/service users who choose to have information posted are aware of the risks. The patients/service user's address must be routinely checked to avoid confidentiality breaches. Patients/Service user's full names, rather than initials, should be used as a matter of good practice. It is also good practice to check whether two people with the same name live at one address.

There must be clarity about who is responsible for checking and recording:

- The patient/service user's address and full name for addressing a letter
- The patient/service user's preference on the method of communication and format.
- If the address for correspondence differs to the home address within the record

The above should be included in a local standard operating procedure.

11.0 NHS Number

With the use of electronic systems and the need to improve clinical records management there is a need to ensure linking of every episode of care with the relevant NHS Number. Staff are responsible for;

- Verifying the NHS Number of a patient at the start of an episode of care;
- Ensuring that the patient is clearly identified on all care records, requests, referrals and results, using the NHS Number;
- Promoting the use of the NHS Number.
- Searching for patients using the NHS Number where this is available

The aim of the NHS Number standard is to;

- Ensure that there is a means to create and maintain an accurate and reliable link between a patient and the records of their care;
- Enable patient records to be safely transferred across organisational boundaries;
- Facilitate electronic referrals and prescription activity;
- Facilitate requests and reports for tests and investigations;
- Accurately and safely identify the patient in all communications;
- Help to create a complete record, enabling the linking of every episode of care across organisations;
- Encourage or ensure the use of the NHS Number (where appropriate) and contribute to an improved service provider and receiver culture.

The general principles of the NHS Number standards that staff must follow are;

- ***Find It** – find the NHS number for the person as soon as possible in the care pathway, ideally on initial contact with the service;*
- ***Use it** – use the NHS Number to link a person to their record; use the NHS Number to search for an electronic record; use the NHS Number on wristbands, documents and reports for the care of the person;*
- ***Share it** – share the NHS Number with other organisations so they can use it; include the NHS Number in all correspondence and electronic messages.*

11.1 Using the NHS Number

Staff working in NHS organisations, social care, and those contracted to provide services for the purposes of care e.g. opticians, pharmacists, dentists, audiologists, use the NHS Number to:

- Confirm and update patient demographic details
- Synchronise patient demographic details with the NHS Spine
- Enhance patient safety by ensuring the right records are connected to the right patients
- Accurately link the patient to their health records
- Ensure safe and efficient coordination of social care with healthcare
- Send electronic prescription messages
- Track patient test requests, results and outcomes
- Identify patients in all communications
- Perform research and analysis
- Support the contracting process.

11.2 Sharing Information for Direct Care

Two duties came into force on 1 October 2015 as part of the Health and Social Care (Quality and Safety) Act. These are:

- A requirement for health and adult social care organisations to use a consistent

identifier (the NHS Number) for sharing data for the direct care of patients;
- A legal duty requiring health and adult social care bodies to share information with each other for the direct care of patients.

For a person's direct care, the default position should be to share unless there is a reason not to. The Act aimed to address the 'culture of anxiety' with regards to data sharing that was identified by the 2013 Caldicott Report. If there are any concerns around sharing please contact the Data Privacy Team for advice lpt.dataprivacy@nhs.net.

11.3 Changes to NHS Number

11.3.1 Adopted Persons Health Records

Not withstanding any centrally issued guidance by the Department of Health and Social Care or the Department of Education, the records of adopted persons can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.

https://www.england.nhs.uk/long-read/key-principles-for-ensuring-continuous-health-records-of-adopted-children/

Depending on the circumstances of adoption there may be a need to protect from disclosure any information about a third party. Additional checks before disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure.

It is important that any new records, if created, contain sufficient information to allow for continuity of care. At present the GP would initiate any change of NHS Number or identity if it was considered appropriate to do so, following the adoption.

Any healthcare professional involved in the care and treatment of a child going through adoption process should ensure they are aware of the latest guidance.

11.3.2 Health Records of Transgender Persons

A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined by the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS Number may be issued by the GP and a new record can be created, if it is the wish of the patient. It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record. For further information refer to the Trust Transgender and Non-binary Service User Policy.

11.3.3 Witness Protection or Sensitive Health Records

Where a record is that of someone known to be under a witness protection scheme or

the record is marked as sensitive, the record must be subject to greater scrutiny and confidentiality. It may become apparent (such as via accidental disclosure) that the records are those of a person under the protection of the courts for the purposes of their identity. The right to anonymity extends to medical records. For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person. Where records are marked as sensitive and are not able to be accessed to support patient care contact your Clinical Safety Officer for guidance.

11.3.4 No NHS Number

Only patients registered with the NHS will have an NHS Number. This will normally be done at birth or the first time that you receive NHS care or treatment.

It is therefore possible that patients who have never registered with a GP, are visitors to the country or asylum seekers, will not have an NHS Number.

Where this is the case, it is still important to register them for care within your service, but you will be unable to 'spine match' (connect them through the Patient Demographic Service – PDS) them. This will mean that they will have a 'local record' only i.e. no one else will be able to see information about the patient as all information is only held within the Trust. Also, there will be no access to GP or other third party organisations health information on the patient.

Where it is possible it would be good practice to support the patient with registering with Online GP registration. If the patient is able to register online and provide the details of the GP Practice staff Identify the GP applied for.

12.0 Merging Records

There are occasions where it may be necessary to merge records within the electronic clinical system. This is normally where there are duplicate records, which can occur for the following reasons;

- The patient was registered under two different names (Mr and Master, or mis-spelling of a name);
- The patient was initially registered with a temporary status and then fully registered (had a local record created)
- The patient was registered without an NHS Number and then with an NHS Number (previous local record existed).

When a possible duplicate record has been identified, a thorough investigation should be undertaken.

For support with merging patient records, contact the LHIS Service Desk.

.

13.0 Digital Media Use and Storage

It is recognised that the use of electronic devices such as dictaphones, digital cameras and specialist medical equipment is a requirement in some services within the Trust. As these devices (and their output/media) may not be suitable for encryption, it is important that staff consider the confidentiality and security of the information and reduce the risk of loss of any Personal Confidential Data (PCD).

All digital media types in use and any use of systems or removable media must have prior approval from the Data Privacy Team prior to use. Digital media containing clinical information and must be treated as a clinical record and kept in accordance with relevant policies and guidelines including information security and records retention.

The preferred use of recording is to use a digital device that flows information directly into the clinical record. Where this is not possible it should be recorded in the record the location of the digital file. Digital media that needs to be retained specific to a patient should be labelled as with any other record and where practical included in the patient's clinical record. A consent form detailing the reason for the use of video and recording the relevant consent should be uploaded to the record. If the video is being used to write up an assessment or record observations, then once these are written up and records have been made the video files do not need to be retained unless there as a specific professional clinical reason.

A note of the existence of this digital media record should be made in the clinical record. If the digital media cannot be stored with the clinical record a note of the storage location must be recorded in the record.

Where video files are created and need to be retained as part of the clinical record these must be stored within the electronic patient record, where this is not possible due to technical limitations, these files must be securely stored with a note added to the clinical record to reference the separately held clinical information.

13.1 Videos of patients taken by family members, carers or friends

Where a family member, carer or friend has videoed a patient with or without their knowledge whilst they are unwell or displaying symptoms and the family member, carer or friend asks a staff member to view the video and/or would like to send a copy of the video. It is important that the patient's wishes are considered and that a record is made of the interaction.

If the patient has capacity, and the knowledge that the video has been taken will not cause the patient or anyone else harm or distress, you must ask the patient for their consent before you view the video or receive a copy. Please record the patient's consent on their Electronic Patient Record (SystmOne). Any copies must be sent securely and saved securely on the appropriate clinical drive.

If the patient does not have capacity, but it is in the patient's best interests for you to see the video, then it is appropriate to do so under the Data Protection Act 2018/UKGDP Article 9 (c) processing is necessary to protect the vital interests of the

data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

The video must be sent to your work mobile device securely. Once received, the video should be saved on the "S" drive in your team's clinical network folder using the patient's NHS number and initials as an identifier. The date the video was received should also be noted so it can be deleted at the end of the retention period (see NHSE Records Management Code of Practice for more information on retention schedules). Once the video is safely stored in the network folder it should be deleted from the work mobile device and email folder.

The video's existence and a brief description should be added to the Patient's Electronic Patient Record.

14.0 Training Needs

Data Security Awareness Training mandatory training for all staff annually.

There is Record Keeping Training and Prescribing Training available on U-Learn for staff to enroll and complete as required.

SystmOne training is available via the Learning Management System for staff to complete as required. Further quick reference material is available on SystmOne by accessing the Guides area via the Home Screen.

For support using other Trust electronic health records contact your local manager or the LHIS ServiceDesk.

15.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self- assess-ment	Process for Monitoring	Responsible Individual / Group	Frequency of monitor-ing
15.0	Data Security and Awareness Training	95% training target being met	Through Per-formance on a Page	Data Pri-vacy Group	Bi-monthly

16.0 References and Bibliography

The policy was drafted with reference to the following:

Regulations/Standards/Guidance

Royal College of Psychiatrists - https://www.rcpsych.ac.uk/members/supporting-you/writing-clinic-letters

Records Management Code of Practice for Health and Social Care, NHS England, Dec 2024 https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

Accessible Information Standard (July 2015) https://www.england.nhs.uk/ourwork/accessibleinfo/

Academy of Royal Colleges – Guidance on writing outpatient clinic letters to patients (Sept 2018) - https://www.aomrc.org.uk/reports-guidance/please-write-to-me-writing- - outpatient-clinic-letters-to-patients-guidance/

Shared Decision Making – NICE Guideline [NG197] 17 June 2021 - https://www.nice.org.uk/guidance/ng197/chapter/recommendations#discussion

Legislation

Public Records Act 1958, section 3 https://www.legislation.gov.uk/ukpga/Eliz2/6-7/51

Data Protection Act 2018 https://www.legislation.gov.uk/ukpga/2018/12/contents

UK General Data Protection Regulation, 2021 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Human Rights Act 2000 https://www.legislation.gov.uk/uksi/2000/1851/contents/made

Health and Social Care (Quality and Safety) Act https://www.legislation.gov.uk/ukpga/2015/28/contents

Gender Recognition Act 2004 https://www.legislation.gov.uk/ukpga/2004/7/contents

Trust Policies

Clinical Document Scanning Policy and Procedure
Agile Working Policy
Digital Acceptable Use Policy
Information Security Risk Policy
Use of Electronic Messaging to communicate with Service Users Policy
Transgender and Non-binary Service User Policy.

17.0 Fraud, Bribery and Corruption Consideration

The Trust has a zero-tolerance approach to fraud, bribery and corruption in all areas of our work and it is important that this is reflected through all policies and procedures to mitigate these risks.

Fraud relates to a dishonest representation, failure to disclose information or abuse of position in order to make a gain or cause a loss. Bribery involves the giving or receiving of gifts or money in return for improper performance. Corruption relates to dishonest or fraudulent conduct by those in power.

Any procedure incurring costs or fees or involving the procurement or provision of goods or service, may be susceptible to fraud, bribery, or corruption so provision should be made within the policy to safeguard against these.

If there is a potential that the policy being written, amended or updated controls a procedure for which there is a potential of fraud, bribery, or corruption to occur you should contact the Trusts Local Counter Fraud Specialist (LCFS) for assistance.

Appendix 1 The NHS Constitution

- The NHS will provide a universal service for all based on clinical need, not ability to pay.
- The NHS will provide a comprehensive range of services.

Shape its services around the needs and preferences of individual patients, their families and their carers Answer No

Respond to different needs of different sectors of the population Yes

Work continuously to improve quality services and to minimise errors No

Support and value its staff Yes

Work together with others to ensure a seamless service for patients No

Help keep people healthy and work to reduce health inequalities Yes

Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance No

Appendix 2 Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Sarah Ratcliffe	Head of Data Privacy/Group Data Protection Officer
Hannah Plowright	Data Privacy and Information Governance Manager/Deputy Data Protection Officer
Claire Mott	Records Manager
Julia Bolton	CCIO
Pat Upsall	Clinical Safety Officer
Ruth North	Clinical Safety Officer
Tom Gregory	Clinical Safety Officer

Circulated to the following individuals for comment

Name	Designation
Bhanu Chadalavada	Medical Director/ Caldicott Guardian
Sharon Murphy	Director of Finance & Performance/SIRO
Members of Data Privacy Group	
Policy Expert Group	

Appendix 3 Due Regard Screening Template

Section 1	
Name of activity/proposal	Electronic Health Records Policy (including record keeping and management)
Date Screening commenced	
Directorate / Service carrying out the assessment	Enabling/Data Privacy
Name and role of person undertaking this Due Regard (Equality Analysis)	Head of Data Privacy
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: To outline the principles and rules associated with recording in an Electronic patient record but including how to manage information captured within it. This includes the standards to which they are expected to adhere to.	
OBJECTIVES: To provide guidance to staff on capturing clinical information within an EPR and how to manage the information they capture	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	No Impact
Disability	Positive – guidance on ensuring meeting the Accessible Information Standard
Gender reassignment	Positive – guidance on managing the records of those going through the gender reassignment process
Marriage & Civil Partnership	No Impact
Pregnancy & Maternity	No Impact
Race	No Impact
Religion and Belief	No Impact
Sex	No Impact
Sexual Orientation	No Impact
Other equality groups?	

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	**x**

Section 4		
If this proposal is low risk please give evidence or justification for how you reached this decision:		
The policy covers guidance on how information should be captured for those with particular needs but the policy generally covers all patients/service users		
Signed by reviewer/assessor	Sarah Ratcliffe	**Date; June 2025**

Appendix 4

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy. **The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.**			
Name of Document:	**Electronic Health Records Policy (including management)**		
Completed by:			
Job title	**Head of Data Privacy**	**Date:**	
Screening Questions		**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.		Yes	**At each contact with the patient to enable accurate information to inform clinical decision making**
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.		Yes	**As part of their clinical contact with the relevant clinicians providing them with a service**
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?		Yes	**In response to the refer and where it is necessary for onward referral**
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		**No**	
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.		No	
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?		Yes	**Potentially where there is a safeguarding or other legislative reason in their best interests**
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.		Yes	**There is a duty of confidence expected with each contact with a clinician and the health record must be kept secure and available to only those who have a legitimate relationship**
8. Will the process require you to contact individuals in ways which they may find intrusive?		**No**	
If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt.dataprivacy@nhs.net **In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy**			
Data Privacy approval name: Sarah Ratcliffe	**Head of Data Privacy**		
Date;	**13/07/2025**		

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust