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:	1	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	4 April 2022	
Name of Author:	Head of Data Privacy	
Name of responsible Committee:	Data Privacy Committee	
Please state if there is a reason for not publishing on website:	N/A	
Date issued for publication:	April 2022	
Review date:	September 2024	
Expiry date:	1 April 2025	
Target audience:	All clinical staff and those required to record in health records	
Type of Policy	Clinical √	Non Clinical √
Which Relevant CQC Fundamental Standards?	Reg 9 – Person Centred Care; Reg 12 - Safe care and treatment; Reg 17 Good Governance	

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
0.1	03.11.21	Initial draft of policy for consultation
1.0	28.02.22	Final Draft for Approval

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

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.

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 3) of this policy

Definitions that apply to this Policy

Accessibility	The ability to access and benefit from a system or entity. Afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services
Record	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business
Correspondence	The act of writing letters or emails to someone – an exchange of information
Creation	The recording of information on paper, printed forms, punched cards, tape, disk, or any information transmitting media
Digital Media	Information shared through a digital device or screen
Disposal	The destruction of records when they have ceased to have any operational or historical value to the organisation.
Protective Marking	An information security classification scheme that requires the prominent marking of information and documents with a short standard wording that indicates how the information should be handled from a security point of view.
Record Keeping	The act or process of creating and maintaining records
Records Lifecycle	The stages all formats of records go through from creation to disposal.
Retention	A practice by which organizations maintain confidential records for set lengths of time, and then employ a system of actions to either redirect, store or dispose of them.

1.0 Purpose of the Policy

The purpose of this policy is to establish the systematic and planned approach to the management of clinical records to ensure from the moment a record is created until its ultimate disposal, Leicestershire Partnership NHS Trust (hereafter known as 'LPT') maintains information so that it serves the purpose that it was collected for and disposes of it appropriately once it is no longer required.

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.

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.

2.0 Summary and scope of policy

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.

3.0 Introduction

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.

The Trust needs to that all health care records are created, accessed, managed and disposed of in accordance with national standards and professional accountability; and are compliant with legal, operational and information governance requirements.

The Trust must conform to a number of legislative requirements, regulations and standards (see references for further details) that outlines the management of records. 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.

Whilst it is not a legal obligation, it is the patients right to be offered the opportunity to receive a copy of any correspondence written by one professional to another. The general principle is that all correspondence which helps to improve a patients understanding of their health and care should be copied to them as a right. This is supported as good practice by the General Medical Council (GMC), Royal College of Psychiatrists (RCPsych) and the Department of Health (2003).

4.0 Duties within the Organisation

The Records Management Code of Practice for Health and Social Care 2021 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 Policy Committee is mandated on behalf of the Trust Board to adopt policies

4.3 The Trust Data Privacy Committee in conjunction with the Clinical Effectiveness Group are responsible for the approval and monitoring of this policy.

4.4 The Chief Executive has the overall accountability and responsibility for healthcare records within the Trust and this function is delegate 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.

4.5 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.

4.6 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.

4.7 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.

4.8 The Head of Information/Performance 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.

4.9 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.

4.10 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.

4.11 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.

4.12 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'*.

4.13 The patient will need to make an informed decision to consent/withhold consent on whether they wish to receive copies of correspondence (See section 10 for more detail). They will be given a choice on what information they want, who from, the address to which it should be sent and in what format (if appropriate). If a patient does not want to receive copies of correspondence, this decision will be reviewed at each formal review or when the clinician and patient deem it to be appropriate but no

longer than 12 months.

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:** Legislation to make sure that people who have a disability, impairment or sensory loss are provided within 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
- Supporting clinical audit, research, allocation of resources and performance planning
- Helping to address complaints or legal issues.

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 (casenotes)
- Electronic patient records
- Pictures and videos

7.0 Health Record Keeping Standards and Guidance

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 in the EPR and are entered via approved data entry formats where they exist.

- **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 it 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. Username and password must not be used unless there are issues with the smartcard software/system.

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' 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 which gives them the relevant information about the Trusts purpose for collecting and using information about them.

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

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 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
- When the care being delivered has been delegated to an unregistered member of staff, the registered member of staff accountable for that patient and 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 recorded/written, wherever possible, with the involvement of the patient, carer or parent
- Be held securely and confidentially
- The information contained within records must be used for the purpose for which it was obtained and only shared appropriately and lawfully.

Clinical records <u>must not</u>:

- 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.

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. They must also be made aware that these records are an official health record and as such will need to be returned to the Trust when requested. With Community Nursing Patient held records they 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. Of 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.

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 disabling the 'consent to share out'.

In addition, requests can be made through the Data Privacy Team, to undertake regular audits of access against their clinical record.

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 soon as possible and the paper confidentially destroyed.

If the record entry is late (being written in retrospectively) the EPR entry should be dated for 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.

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. 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.

8.1.1 Consent

Patients should be informed that a health record will be created, and their consent 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.

8.1.2 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.

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.

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.

8.2 Clinical Documentation

Following an assessment of the patient, the assessment and outcomes must be recorded on the EPR on the approved templates that have been provided.

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 forms/templates 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 is not permitted as it increases the 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.

Any paper clinical documentation should be scanned and uploaded to the EPR using the approved methods outlined in the Clinical Document Scanning Policy. 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.

8.3 Deletions and Corrections

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 EPR, and only in situations where the entry is factually incorrect, or it is likely to be damaging to an individual. Otherwise, corrected entries can be made which will have an audit trail of the correction (‘mark in error’).

8.4 Retention and Destruction

8.4.1 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.

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 should be agreed with the relevant senior manager.

In addition, all EPR systems must be secure and protected by smartcard access, or by login ID and password, or similar access control mechanisms, and staff must not share their cards or credentials.

8.4.2 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 Records Management Code of Practice for Health and Social Care, by LPT.

It is therefore important that the retention and disposal of records – 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.

Records are required to be kept for a certain period either because of a statutory requirement or because there an identified specific purpose in terms of use. Records can be kept for longer than their identified retention period if LPT decides that there is an appropriate and valid rationale for this. These decisions need to be recorded locally within the Trust's Retention Schedules.

Minimum retention schedules are laid down in the Records Management Code of Practice for Health and Social Care (2021). 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. Where hard copy health records are destroyed a certificate of safe destruction i.e. Destruction Certificate, is required.

8.5 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.

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.

8.5.1 Tracking Paper records
Paper records must never be removed from site unnecessarily or without the approval of a line manager or clinical lead. When transporting paper records the following advice must be followed:

- All records must be tracked to ensure that their location is known
- Records must be carried in sealed envelopes, document/secure mail pouches or suitable secure containers
- Records must be handled carefully into vehicles to ensure that they are not damaged

8.5.2 Labelling and Packaging of 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.

8.6 Mobile and Homeworking
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.* 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 brief case, 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
- Data on laptops must be regularly backed up and archived when no longer required.

Remember, it is the individual's responsibility to safeguard the information they are using.

9.0 Scanned Records

With the implementation of the Trust's EPR there has been an increased need for paper documents to be scanned and uploaded to the patient's record. In brief, it is important that during this process:

- All documents are scanned to a standard that they will be able to be opened and read on the EPR system.
- The correct documents are uploaded to the correct patient's record
- These uploaded documents can then be found and retrieved by those who need to refer to them.

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.

The legal admissibility of scanned records, as with digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or electronic, can be admissible in court[1].

The actual process for scanning and uploading documents and more detailed guidance is set out in the *Clinical Document Scanning Policy and Procedure.*

10.0 Copying Correspondence to Service Users/Patients

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).

When writing clinical letters after a discussion, they should be written to the patient rather than to the healthcare professional, in line with the Academy of Medical Royal Colleges' guidance on writing outpatient clinic letters to patients. Send a copy of the letter to the patient (unless they say they do not want a copy) and to the relevant healthcare professional. 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 copied to the person with legal responsibility, for instance a parent or guardian.

[1] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31

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

10.1.1 Systems and recording

- **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.

10.1.2 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)

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.

However, as noted in the section above, a health professional may make 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.

10.1.3 Consent to receipt of letters: identifying appropriate recipients
In line with the overall NHS policy of informed consent, it is for each patient/service user to decide whether they wish to receive copies of letters written about them by health professionals, as an Opt-In mechanism.

The aim is that within a consultation, the possibility of receipt of the letter 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 copies of letters, an assessment of their capacity can be undertaken by the treating clinician and recorded in the patient/service users clinical records.

- Carers: 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.

10.1.4 People with information and communication support needs

In line with the Accessible Information Standard (July 2015), patients/service users and their carers should be able to receive copies of letters in a form they can understand and use. The Trust must comply with the Equality Act 2010, Data Protection Legislation (UK GDPR/ DPA 2018) and the Human Rights Act 2000.

Some people cannot read well enough to understand a copied letter. Such people are often reluctant to admit the problem, and it may fall to them to seek someone to help them to read the letter.

Consideration should be given to the needs of people with all types of information and communication needs, including learning disabilities. Identifying their needs is key to ensuring that we are able to support their right to receive clinical correspondence.

10.1.5 Correcting inaccurate records

Healthcare professionals who routinely share records with patients/service users report that patients/service users and carers often identify inaccuracies or mistakes. There should be arrangements to amend/annotate their records to ensure they are correct. Whilst it may initially be time-consuming, the result should be improved and more accurate records that comply with the provisions of the UK GDPR/DPA 2018 and benefit the overall quality of the service.

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 it is not possible to resolve the matter or the requested change is clearly incorrect the record should be annotated and the data subject advised accordingly. It may be appropriate to agree with the data subject that their alternative account is filed alongside the original that they wish to object to.

In all cases where a correction cannot be made, or the data subject is dissatisfied with the outcome, the Trust's Head of Data Privacy must be informed.

10.1.6 Protecting Confidentiality

In reviewing their security and confidentiality procedures, health professionals copying letters should assess and take steps to minimise the following risks:

- Breaches of confidentiality of information of third parties
- 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 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. Envelopes must be marked ‘NHS Confidential’ (in line with NHS protective marking guidance) and the patients/service user’s address routinely checked. 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.

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

11.0 NHS Number

Using the NHS Number as the national identifier for patients significantly improves safety by ensuring patients are identified correctly. In clinical care the use of the NHS number is of particular importance because it:

- Is the only National Unique Patient Identifier
- Support safer identification processes
- Helps create a complete record, linking every episode of care across the organisation

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 therefore for 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

11.1 NHS Number Standard

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 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 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.

11.2 Use of NHS Number in 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.

11.3 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.

11.4 Additional NHS Number guidance[2]

11.4.1 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

[2] Guidance on Adopted Persons, Transgender Persons and Witness Protection from the Records Management Code of Practice for Health and Social Care 2021

birth names are used.

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.

11.4.2 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 can be issued 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.

11.4.3 Witness Protection Health Records
Where a record is that of someone known to be under a witness protection scheme, 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.

11.4.4 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 patient 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.

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 misspelling 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 duplicate record has been identified, a merge is required to combine the two into one complete record.
Inconsistencies in the names or date of birth may be a reason to cancel or reject a request to merge a record. If there are inconsistencies, contact Leicestershire Health Informatics Application Support who will support with investigating if it is an appropriate merge request.

13.0 Digital Media

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).

When recording information on these devices full patient details should not be used. The use of abbreviated identifiers is recommended e.g. the patient's initials and last four numbers of their NHS Number – AB7890. The identifier should be sufficient for other staff involved in the use of the information to link to the patient's record but not for anyone else to be able to identify the person. Any tapes or separate recoding media associated with these devices should be individually identifiable by that service e.g. Tape SLT001, tape SLT002.

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 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.

14.0 Video recording

As the EPR does not support video files, these should be stored on a secure local server/secure cloud storage and their location recorded in the patient's record. The saving of video files should be carefully considered to justify the requirement i.e. for a specific clinical reason. 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 records have been made the video files do not need to be retained unless there as a specific professional clinical reason. Care should also be taken to ensure other children are not included in any recording without their specific knowledge and consent (or parental consent).

The digital media should be treated as a clinical record and kept in accordance with relevant policies and guidelines including information security and records retention.

15.0 Training needs

There is no training need associated with this policy as Record Keeping Training is a separate clinical requirement

16.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	Staff should inform patient about the use of information	Section 7	IG Spotcheck	Data Privacy Committee	Annually
	Staff must keep clear, accurate and legible records	Section 7.2	Record Keeping Monitoring	Clinical Effectiveness Group	Defined by services
	Patients consent preferences are recorded	Section 8.1.1	Record Keeping Monitoring	Clinical Effectiveness Group	Defined by services
	Assessment and outcomes recorded on approved templates	Section 8.2	Record Keeping Audit	Clinical Effectiveness Group	Defined by services
	All paper records must be tracked	Section 8.5.1	Records Management Audit	Data Privacy Committee	Annually

17.0 Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
All staff have undertaken record keeping training commensurate with their role	Mandatory Record Keeping Training on a 3-yearly basis

18.0 References and Bibliography

The policy was drafted with reference to the following:

Regulations/Standards/Guidance

A Guide to Confidentiality in Health and Social Care – Treating confidential information with respect (HSCIC 2013)

General Medical Council. Good Medical Practice. https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/good-medical-practice/domain-3---communication-partnership-and-teamwork

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, NHSX, Dec 2021 https://www.nhsx.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/

Equality Act 2010 https://www.legislation.gov.uk/ukpga/2010/15/contents

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

Use of Electronic Messaging to communicate with Service Users Policy

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	x
Respond to different needs of different sectors of the population	☐
Work continuously to improve quality services and to minimise errors	x
Support and value its staff	☐
Work together with others to ensure a seamless service for patients	x
Help keep people healthy and work to reduce health inequalities	☐
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	x

Appendix 2

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Hannah Plowright	Data Privacy & Governance Manager
Claire Mott	Records Exploitation Manager
Girish Kunigiri	Consultant Psychiatrist/CCIO
Jacquie Newton	
Victoria Clarke	Clinical and Quality Governance Manager, DMH

Circulated to the following individuals for comment

Name	Designation
Dr Avinash Hiremath	Medical Director/ Caldicott Guardian
Sharon Murphy	Director of Finance & Performance/SIRO
Members of Data Privacy Committee	
Members of Clinical Effectiveness Group	

Appendix 3

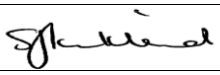
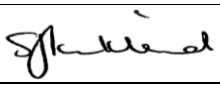
Due Regard Screening Template

Section 1	
Name of activity/proposal	Electronic Health Records Policy (including management)
Date Screening commenced	07/11/2021
Directorate / Service carrying out the assessment	Enabling/Data Privacy
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland, 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 <u>tick</u> 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		**Date**	06/12/2021
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed		**Date**	28/02/2022

Appendix 4

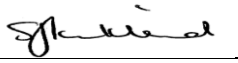
DATA PRIVACY IMPACT ASSESSMENT SCREENING

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:	**Sam Kirkland**	
Job title	**Head of Data Privacy**	**Date: 28/02/22**

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:	**Sam Kirkland, Head of Data Privacy** 
Date of approval	**28/02/22**

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