NHS
Bedfordshire Hospitals
NHS Foundation Trust

CORPORATE AND CLINCAL POLICIES

Policy X **Clinical Policy**

Policy Document Title: **Health Records Policy**

This document is relevant for staff at:	Luton Hospital site	Bedford Hospital site	Both Hospital sites
			X

Document Author
Heidi Walker, Head of Information Governance and DPO
Suthakar John Edison, E-Health Records Lead

Policy Developed in Consultation with:
Health Records Working Group

Is this policy document new or revised / or has minor amendments?
Revised

Reason for amendments: Please highlight all amendments in your document.
To update in line with latest guidance and to develop cross site.

Document Number:	Version Number:
IG17T	2

Target Audience/Scope:
All Staff

Associated Trust Documents:
Incident Reporting Policy
Duplicate Registration & Merge Policy
All IT Policies
Information Governance Policy

Date of Approval:	Review Date:
19th December 2022	December 2025
Approved by:	Policy Approval Group
Chair /Chief Executive Signature:	David Carter, CEO

Contents

1. Introduction

This Policy sets out how Bedfordshire Hospital NHS Foundation Trust (the Trust) will manage patient Health Records (in whatever format, paper or electronic).

The Trust is committed to ensuring there are comprehensive and effective procedures in place for the composition, completion, use, storage, availability, retrieval and disposal of patients' Health Records.

Information is predominantly stored with the Trust's electronic patient record system which encompasses multiple best of breed applications best suited to their unique purpose. For example a Picture Archiving and Communication System (PACS) for Imaging and an electronic patient record system (Nervecentre) for patient Assessments, Observations and so forth.

Well managed Health Records play a significant role in patient care and provide a communication channel inter-departmentally and inter-professionally through the accurate and prompt recording of information.

All NHS records are Public Records under the Public Records Acts and must be kept in accordance with the following statutory and NHS guidelines:

- Public Records Acts 1958 and 1967
- Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- NHS Code of Practice on Confidentiality, 2003
- NHS Records Management Code of Practice 2021
- NHS Litigation Authority (NHSLA)
- Clinical Negligence Scheme for Trusts (CNST) (relating to maternity)
- Standards for Better Health

The governing principles in respect of health records within the Trust are outlined in this policy and have been established in order to support:

- Continuity of patient care
- Day to day business processes which underpin delivery of care & treatment
- Clinical Governance
- Clinical decision making including care pathways
- Compliance with relevant Care Quality Commission (CQC) standards and the NHS Litigation Authority (NHSLA) health record criterion
- Improvements through research and audit
- The sharing of patient information where there is a legal requirement or justified need
- Confidentiality

Well-managed records are key contributors in the reduction of:

- Clinical risk to patients
- Patient complaints
- Disputes
- Legal action against the Trust

2. Scope

This policy covers the creation, maintenance, archiving and disposal of patient's clinical health records. These can exist in many different media: digital stored on servers, CD's, DVD's, local

hard drives; or paper stored physically or on microfiche. This policy highlights the need for accurate record keeping, the secure storage of records and the relevant disposal of records once they have exceeded their retention period. Sharing and transportation of records are also included.

This policy relates to **all health records, in all Media,** including, but not limited to:

- Paper records (including Event Pack),
- Scanned and Electronic Health Records
- ALL patient records held on ALL electronic systems
- All Imaging Modalities – CT/MRI/Ultra-Sound/ X-Ray (including film) and scans
- Clinical Photographs, slides, and other images
- Departmental patient records held in ANY format
- Diaries and Index cards which contain/hold information about patients

ALL of the above constitute part of a patient's health record if it has been collected/created for the care or treatment of the patient and must be treated as such.

If any of the above has been collected/created for any other purpose e.g. research etc., the consent of the patient must be obtained and the information must be stored, secured, used, protected, retained and disposed of in line with Trust Policies and NHS guidance.

3. What is a 'Health record'?

A 'health record' is defined in Access to Health Records Act 1990 as follows:

A record which—
(a)consists of information relating to the physical or mental health of an individual who can be identified from that information, or from that and other information in the possession of the holder of the record; and
(b) Has been made by or on behalf of a health professional in connection with the care of that individual;

4. Duties and responsibilities:

4.1 **Xerox**:

The Trust has a contract in place with Xerox to provide the following services to the Trust (this is not a definitive list):

- Secure offsite storage of archived patient's legacy paper Health Records
- Secure offsite storage of Corporate Records
- Retrieval and scanning of archived legacy paper Health Records from offsite storage
- Retrieval and scanning of paper legacy Health Records held on site (in preparation for planned patient activity)
- Printing and delivery of Day Forward Event Packs for planned admissions and clinic attendance where it has been agreed
- Collection, transportation and scanning of Event Packs within agreed time frame following outpatient attendance and inpatient discharge
- Scanning of A&E cards & Fracture Packs

- Secure destruction of Health Records as and when approved by the Trust

Whilst Xerox are contracted to provide the Trust's Health Records Management Service, ultimate responsibility for these services sit firmly with the Trust.

Xerox compliance with their contract with the Trust is monitored by the Trust's Health Records Working Group – see section 4.7.

4.2 **Chief Executive Officer (CEO) -** has overall accountability for the management of all records within the Trust.

4.3 **Medical Director** and **Chief Nurse -** have responsibility for the clinical content of health records.

4.4 **Chief Digital Information officer** (**CDIO) -** has overall responsibility for the administration and management of Health
Records, including storage, availability, maintenance and security. They are also responsible for the management and monitoring of the Trust's contract with Xerox – see also Health Records Working Group below.

4.5 **Senior Information Risk Owner (SIRO)**
The SIRO takes overall ownership of the Trust's Information Risk Policy, acts as a champion for information risk on the Board, providing advice on the content of the Trust's Statement of Control in regard to information risk.

4.6 **Caldicott Guardian** is responsible for:

- Safeguarding the confidentiality of patient information
- Agreeing to the sharing, use and protection of patient identifiable information by Trust staff and across organisational boundaries
- Providing advice and where necessary resolving patient confidentiality issues, acting in the best interests of the patient
- Ensuring that the Trust achieves the highest score in the Confidentiality standards within the Information Governance Toolkit, thus maintaining the eight principles of the Data Protection Act 2018 and the Caldicott Principles.

4.7 **Chief Clinical Information officer CCIO** and **Chief Nursing Information Officer (CNIO):**
Key Clinical leader in supporting the adaptation, compliance and safe use of digital health records

4.8 **e-Health Records Lead**:

Is responsible for overall development and maintenance of health records management throughout the Trust, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

4.9 **Head of IG and Data Protection Officer**

The Head of IG encompasses the role of the Data Protection Officer (DPO) which is a leadership role required by the General Data Protection Regulations (GDPR). Data Protection Officers are responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements

The controller and the processor need to involve the DPO fully and at the earliest point in all issues which relate to the protection of personal data. A Consultative and Advisory Role to include the following:-

- Monitor Trust Compliance with GDPR
- Provide advice on DPIA's including the need to undertake one
- Investigate and report to the ICO all breaches within 72 hours (if a person's right is infringed)
- Undertake record keeping functions
- Independent and cannot be instructed to the output of advice

4.10 **Health Records Working Group (HRWG)**
The HRWG meet on a quarterly basis. The group is made up of Trust managers and clinicians and is chaired by the CCIO/Caldicott Guardian. This group is responsible for:

- Governing the structure of the Health Records and the critical artefacts within.
- Overseeing and supervising the maintenance of the Health Record system throughout the Trust
- Monitoring the management of the Xerox contract through the presentation of Key Performance Indicators which are linked to the requirements of the contracted service
- The containment of risk through the development of robust policies, procedures and audit in compliance with NHSLA and other required standards, legislative and NHS requirements including the IG Toolkit Health Record standards.
- Monitoring compliance with this policy

4.11 **General Managers and Department/Ward Managers/Heads** are responsible for ensuring that:

- Staff working in their area/ward/department understand and comply with this policy and those referenced within it
- Investigate all breaches of confidentiality ensuring lessons learned are implemented and corrective training arranged as appropriate

4.12 **Information Asset Owner & Information Asset Administrators (IAO's & IAA's)**
Many IAO's are General Managers are Information Asset Owners who are responsible for Departmental IT systems used within their Divisions which contain patient identifiable data. These responsibilities include:

- Ensuring a Privacy Impact Assessment is performed on ALL new IT Systems procured by their Division that will process or store personal identifiable data – see the Trust's Information Governance Policy
- Management and monitoring of the contract for the system including any Service Level Agreement or support contract in place
- Identifying IT Security risk associated with the system through the completion of regular Security Assessments
- Reporting and mitigation of identified risks
- Providing access to the system on a need to know basis
- Management of leavers and starters

- The control and management of information flows from the system
- Data Quality of the information held on the system
- Management and risk assessment of upgrades and system improvements
- Monitoring user access to identify any inappropriate access

The Trust's IT Department is the IAO and IAA for the Trust's key systems, which constitute the Trust's Electronic Patient Record (ePR) which currently include:

Application Name	**What is used for**
i.PM	Patient administration system
ICE	Results & Reporting system incl. inpatient discharge letters
External ICE access	Results & Reporting system incl. inpatient discharge letters for GP & Community systems
Clinical Portal	View only electronic shared record system which feeds from various other system. Still under project
Nervecentre	Observations and Bed Management system including ePMA – Still under project
BigHand	Digital dictation system for outpatients
Evolve and Mediviewer	Electronic Document and Record Management System
Extramed	Patient flow
Infoflex	Cancer monitoring system
EDT Hub	Electronic Document transfer system used for electronic sending of letters to GPs and Community
Symphony	Urgent and emergency care system, incl. ED discharge letters
HICSS Endoscopy	Procedures recording and reporting tool for GI, Bronchoscopy and cystoscopy procedures
CRIS	Radiology information system used for radiology appointment and results
Carestream PACS	Picture Archiving Communication System used to store radiology images/studies
VNA	Vendor Neutral Archiving for storing PACS images
NBSS	National Breast Screening System for Breast Screening appointments and results
Sectra PACS	Medical Imaging system for storing images and radiology workflow
Winpath Enterprise	Laboratory information management system

Chemocare	Chemotherapy electronic prescribing system
NHS eReferrals Service (CAB)	Patient appointment booking via GP
CMIS	Maternity system
Dawn AC	Anticoagulant system
Bank Manager	Reporting system for Blood transfusion
Diamond.net	Diabetes system
Auditbase	Audiology system
Tomcat CVIS	Cardiology system
ICNet	Infection control system
Dash	Orthopaedics appointment system – receives patient demographics from i.PM
Medchart EPMA	Electronic Prescribing Management system for drugs administration
Tomcat(CVIS)	Cardiac care system
Viper	Clinical Portal
Metavision	Critical Care System

4.13 **All Staff**

Irrespective of grade or role (clinical, management or administrative), ALL staff are responsible for ensuring that:

- They understand and comply with this policy and those referenced within it
- The records they create or add information to are correct and up to date
- Speak to their line manager in relation to concerns over inaccuracies
- They keep records up-to-date by making accurate and timely entries
- Ensure that all information is legible so that it can easily be read and reproduced when required
- That they are familiar with the Guidelines of good practice for records and record keeping
- They are aware of the processes and procedures in relation to Event Packs and scanned records
- They comply with the requirements of the Data Protection Act 2018, The General Data Protection Regulations, the Common Law duty of Confidentiality, Caldicott Principles (see appendix C & D)

4.14 **EHR Users** – some EHR users have particular responsibilities. Staff MUST ensure they are aware of these responsibilities and ensure they comply with them – see appendix A.

4.15 **Personal/Professional Integrity**

All health care professionals have a legal duty of care; record keeping should be able to demonstrate:

- A full account of all assessments and the care planned and provided.
- Relevant information about the condition of the patient or client at any given time and the measures taken to respond to their needs.

- Evidence that the duty of care has been understood and honoured and that all reasonable steps to care for the patient has been taken.

Professionals are accountable for ensuring that any duties, which they delegate to those members of the multi-disciplinary health care team who are not registered practitioners, are undertaken to a reasonable standard. For instance, if a professional delegates record keeping to pre-registration students or to assistants, they must ensure that they are adequately supervised and that they are competent to perform the task and work to locally agreed protocols.

In an inpatient setting, a qualified person must clearly countersign any entry made by an unqualified person each day. In circumstances where a patient is receiving a regular, on-going package of care and is being monitored by an unqualified member of staff, providing the patient's condition does not change, entries may be countersigned at a minimum of every six weeks. Entries made by unqualified staff should be checked and signed by qualified staff to record a review and evaluation of patient care. An example entry may read "On-going care package reviewed today and previous entries by unqualified staff checked".

Professionals are accountable for the consequences of entries made by unqualified members of staff.

4.16 **Responsibilities of Third Parties**

Where a non NHS agency or individual is contracted to carry out NHS functions, the contract must draw attention to obligations on confidentiality and to restrictions on the use of personal information, including those specified by the Data Protection Act 2018.

The contract must require that patient information is treated and stored according to specified security standards, and is used only for purposes consistent with the terms of the contract.

The contract should also make reference to the requirements laid out in the Freedom of Information Act 2000. Action that will be taken in the event of confidence being breached (e.g. termination of contract) should be specified.

All Health Records created by a third party on behalf of the Trust remain the property of the Trust.

5. Record Keeping Standards

The code of practice is a guide to the standards of practice required in the management of NHS records, based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each type of record. Its purpose requires the Trust to have effective procedures in place for the compilation, completion, use, storage, retrieval and disposal of records together with procedures for regular monitoring. To achieve this, the following issues in respect of patient records are primary:-

- Compilation
- Legibility
- Completion
- Amalgamation
- Patient-held records/computerised records
- Binding

- Linking with X-rays, test results etc.
- Storage
- Security
- Access for patients
- Copying
- Retrieval
- Availability
- Retention and Destruction
- Confidentiality
- Admission/Discharge

Health Records are valuable because of the information they contain, but that information is only useful and usable if it is correctly and legibly recorded in the first place, is then kept up to date and is easily accessible when needed.

Good records management is essential for:

- Providing high quality patient care
- Continuity of care
- Effective communication and dissemination of information between members of multi-disciplinary health care teams
- An accurate account of continuous assessment, treatment and evaluation reflected in a care plan
- The ability to detect problems, such as changes in the patient's condition, at an early stage
- Clinical liability
- Disputes or legal action

It is therefore important to ensure:

- Important and relevant information is recorded and completed
- It is legible, written in black ink, and can be easily read and reproduced when required.
- Information/records are easily accessible and kept up-to-date

The following must be followed to ensure quality records are created from the moment the patient is registered:

- The patient's demographic details must be checked at every opportunity and the relevant IT system updated
- An entry should be made in every inpatient record every 48 hours as a minimum
- Every significant intervention should be recorded
- Every significant conversation with the patient, relative(s) or other healthcare professional should be recorded
- The discharge policy must be followed
- All entries must be: named, timed, dated, designated, signed, and be legible
- Correction fluid must not be used in paper records
- Any change must be named, signed, designated, dated and timed
- Notes made in retrospect must be clearly marked as such, named signed, designated, dated and timed
- If a change to the record is required, the original should be struck through with a single line, signed, dated, designated and timed leaving the original entry visible

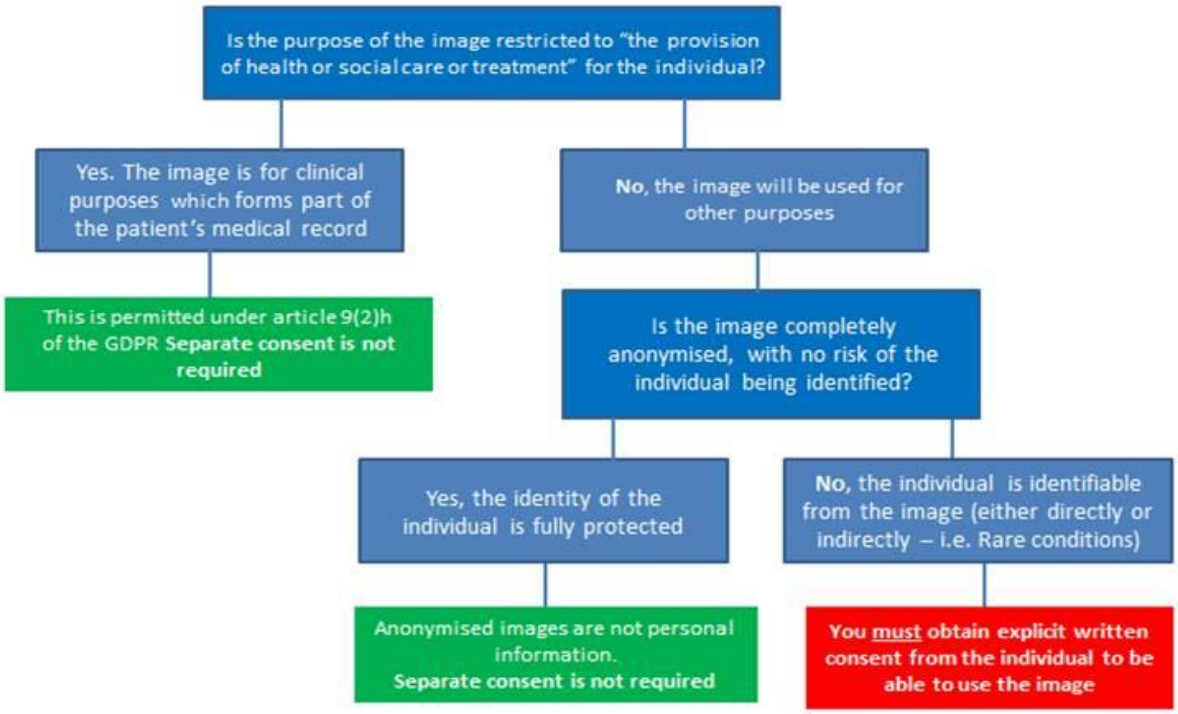
- An Electronic Discharge Letter (EDL) MUST be completed upon discharge. A copy must be given to the patient and a copy sent to the GP within 48 hours. The EDL MUST be a complete and accurate record of:
    - diagnosis and treatment
    - medication
    - follow up arrangements
    - comorbidities
- If an inpatient dies, the Event Pack or A&E attendance card MUST be passed to the bereavement office for the completion of a death certificate.
- Event Packs MUST be released following inpatient discharge, outpatient clinic attendance or A&E attendance to ensure they are available for Xerox to scan and make available on the EDRMS system – all staff are required to follow the agreed processes set up for their ward or department.
- Event Packs MUST be made available to the Trust's Clinical Coding Department to ensure activity can be coded in a timely manner – all staff are required to follow the agreed processes set up for their ward or department.

6. Maternity Records – Held by the Expectant Woman

The Trust currently supports the use of Maternity Records held by the expectant woman. These records are issued at the time of booking. Upon delivery this record must be returned to the Trust to be filed in the Maternity Record.

7. Images and Consent

Images made for clinical purposes form part of a patient's medical record, and therefore the processing of this information is legally permitted under Article 9(2)(h) of the GDPR. Separate consent is not required for this purpose; however staff should always ensure that patients are aware of the reason(s) for the image, and that it will be retained within their medical record. Images obtained for clinical purposes should not be used for any other purpose without explicit consent.



8. Adoption Records

Current adoption legislation requires that all adopted patients are given a new NHS number, and that all previous medical information relating to the patient is put into a newly created medical record. Any information relating to the identity or whereabouts of the birth parents should not be included in the new record. Whilst changing or omitting information from medical records would usually be contrary to ethical and professional guidance, this is not the case for the records of adopted patients and there is a legal requirement that it takes place.

9. Process for registering a patient gender re-assignment

Patients may request to change gender on their patient record at any time and do not need to have undergone any form of gender reassignment treatment in order to do so. When a patient changes gender, the current process on NHS systems requires that they are given a new NHS number and must be registered as a new patient at their practice. All previous medical information relating to the patient needs to be transferred into a newly created medical record. When the patient informs the practice that they wish to register their new gender on the clinical system, the practice must inform the patient that this will involve a new NHS number being issued for them. Subsequent changes to gender would involve a new NHS number. Please confirm this has been discussed with the patient when notifying PCSE.

10. The Data Protection act 2018 and General Data Protection Regulations

The General Data Protection Regulation (GDPR) was published by the European Union (EU) and this forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA18)

The Data Protection Act 2018 is the fundamental legal requirement that applies to all organisations and individuals processing data of a personal nature.

The Act applies to living individuals and gives those individuals a number of important rights to ensure that Patient Identifiable Data (PID) is processed lawfully. It regulates the manner in which information can be collected, used and stored, and so is of prime importance. The Act does not cover PID relating to deceased individuals. However, the NHS and the Trust applies the same level of confidentiality to this PID as if it were in relation to a living individual.

This Act applies to all personally identifiable information held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays etc. Appropriate security measures must be taken against unauthorised access, alteration, disclosure or destruction and accidental loss or destruction.

The Act dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence, investigated in line with the Trust Disciplinary policy and could be potentially prosecuted.

Every person working for, or within the NHS, who records, uses, stores or otherwise processes patient information has a personal common law duty of confidence. This is in addition to the Terms and Conditions of their contract with the Trust and the requirements enforced by any professional body they may be registered with e.g. GMC, GDMC, NMC etc.

Together they are a framework of rights and requirements which are designed to safeguard PID of all UK and \EU Citizens, regardless of which country it is being processed in. This framework balances the legitimate needs of the Trust to collect and process PID to enable it to function, against Data Subjects rights.

GDPR and DPA18 are complex pieces of legislation which are explained further in the Information Governance Policy

Patient information, including Event packs MUST never be taken off the Trust site unless it is part of an agreed process e.g. for Trust clinics held off site.

Users of IT systems containing patient information must never share their password with others.

Original records **must never** be sent outside the hospital, unless:

- They are for use at a Trust led Outpatient Clinic or community visit

Or

- A patient is being transferred to another hospital as a ‘blue light’ emergency, and the consent of either the Manager of the Day or 555 Bleep holder (if out of hours) has been obtained. *A ‘blue light’ emergency is defined as when the decision to transfer a patient is made and the ambulance is outside the Trust ready to transport the patient within 10 minutes*.

Or

- The original records are being taken by the Coroner at their request

Please note: Patient information must NOT be faxed unless it is the only option available and that the decision to do so can be justified and evidenced. The Trust's process for secure faxing MUST ALWAYS be followed.

Step 1 - ensure you use a Safe Haven front sheet (available on the Intranet Document or IG Department zones).....
Step 2 - call the recipient to let them know you are sending them a fax and to double check the fax number. (Do not rely on number that have been programmed into machines unless you are 100% sure that number is still correct).
Step 3 - ask the recipient to confirm they have received the fax, or call them back to make sure they have received it. (Do not rely on fax receipts).

11. Patient Access

Patients have a legal right to access their health record. Access to Health Records falls under the Data protection Act 2018 and applies to records relating to the physical or mental health of an identifiable individual, which have been made by a Health Care Professional in connection with their care and treatment. This does not relate to the deceased which must be dealt with under the Access to Health Records Act 1990.

PLEASE NOTE - There are legal deadlines, which the Trust MUST meet when dealing with subject access requests. Please act upon requests immediately by forwarding them on to the Information Governance department.

Please refer to Section 12 within the Information Governance Policy

Inappropriate Access

Unlawful disclosure or misuse of personal data (including staff accessing their own personal health records or the records of colleagues, family or friends without authorisation) is a breach of Trust policy and may constitute a criminal offence.

Users are granted access to Health Records to enable them to perform their contracted duties ONLY. Staff wishing to view their own records MUST follow the Subject Access Request process noted in section 12 of the Information Governance Policy

The Trust's Information Governance Manager performs regular audit trail audits of key IT systems to identify any inappropriate access to a patient's Health Records.

12. Safe Sharing and Transportation of Patient Information

To ensure the risk of breaching patient confidentiality is mitigated when sharing and/or transporting patient information it is important that the Trust's Information Governance Policy & Procedures MUST be complied with.

Options for the safe sharing and transportation of patient information from a patient's Evolve record are covered in appendix B.

13. Patient Document Tracking (PDT)

Patient Document Tracking (PDT) is the electronic method of tracking inpatient Event Packs on i.PM.

All staff are responsible for tracking these Event Packs in and out of their ward/department/area/location on i.PM. It is essential that this is done to ensure they can be located when needed at any given time.

Outpatient Event Packs MUST NOT leave the clinic area after the clinic session. This MUST remain in the agreed location for collecting and scanning by Xerox staff.

14. Subject Access Requests and Access to Health Records Requests

Access to Health Records falls under the Data protection Act 2018 including GDPR and applies to records relating to the physical or mental health of an identifiable individual, which have been made by a Health Care Professional in connection with their care and treatment. This does not relate to the deceased which must be dealt with under the Access to Health Records Act 1990.

The right of access is principally for the individual who is the subject of the record, but the individual may authorise another person, to make an application for access on his or her behalf in writing. Other instances where an application to another person's record may be granted are:

- An Authorised person on behalf of the patient, i.e. relatives, or where an individual is incapable of managing his or her own affairs.
- Parents (The child's rights to confidentiality have to be balanced against parental responsibility).
- Patient representative – A person you nominate to make healthcare decisions
- Executor of a will/Persons who may have a claim arising out of the patients estate

For further information, please refer to section 12 of The Information Governance Policy

Data Subjects have several rights, some of which are new. However, these will not apply to every individual, application will depend on what data/information it relates to and why it is being processed e.g. patients do not have the right to have their health record deleted, but they do have the right to have it corrected if it is incorrect.

1. Right to be informed
2. Right of access
3. Right to rectification (Correction)
4. Right to erasure ('right to be forgotten')
5. Right to restriction of processing
6. Right to data portability
7. Right to object

8. Right to know if we carry out Automated indecision-making and profiling

All of these rights are covered in detail in the Data subject and individual rights policy

There are legal deadlines which the Trust MUST meet when dealing with any of the above rights. Please refer all requests of this nature immediately to the Information Governance Department.

Requests from Solicitors who are acting on behalf of a patient, where the claim is against the Trust – Medico Legal must be referred to the Trust's Litigation Department.

15. One Patient One NHS Identifier and Hospital Number

It is imperative that every patient registered with the Trust has one "unique" NHS Number. This will also be matched with a locally unique hospital number.

Staff who identify any patient who may have more than one hospital number MUST report this to the IT Service Desk, and information will be assessed and rectified appropriately

Wherever possible and practicable the NHS Number should appear in all electronic systems which hold patient information, appear on each document and used as the primary identifier when sharing information between organisations.

16. Retention and Destruction of Health Records

16.1 Paper Records

A patient's paper health record can be destroyed if they meet the following criteria:

1. The patient has not attended the hospital as either an inpatient or outpatient in the last eight years
2. The patient has been deceased for eight years or more.

It will be destroyed under the instruction of the Chief Executive, or their designated officer, in accordance with the NHS Records management code of practice for Health and Social care 2021 and a certificate of confidential destruction will be provided.

Exceptions to these **retention** guidelines are listed below:

- ***Maternity records*** – documents may be destroyed 25 years after last attendance or 8 years after the death of a child (but not the mother).
- ***Paediatric records*** – records relating to children and young people may not be destroyed until the patient's 25th birthday or 26th birthday if the entry is made when the young person was 17 years of age or 8 years after the death of the patient, if sooner.
- ***Mental Health Records*** – records relating to mentally disordered patients within the meaning of the Mental Health Act 1959 may be destroyed 20 years after no further treatment is considered necessary or 8 years after the patient's death, if sooner.
- ***Oncology & Neurology records*** – 30 years. Also consider the need for permanent preservation for research purposes.
- ***Patients involved in a clinical trial or research*** – 5 to 30years after conclusion of trial or research depending on the subject. Advice may be sought from the Trust's Research & Development Manager who will be able to confirm the actual end date of any trial or research.
- ***Donor records (blood and tissue)*** – 30 years post transplantation

- **Records of patients with Genetic conditions** - 40 years
- ***X*-rays following official complaint or litigation** – 10years
- **Corneal Transplants** – 30 years post transplantation
- **Children or adults with activity where an ICD10 code for actual or suspected Non Accidental Injury has been used** – keep until advised otherwise.

All other records may be subject to differing lengths of retention as specified in the NHS Records management code of practice for Health and Social care 2021.), including (but not limited to) supplementary documents such as signatory books, off duty rotas, ward diaries, theatre registers etc. etc.

16.2. Electronic Records (including scanned records)

Ninety days after legacy paper records and Event Packs for current patients have been scanned they will be destroyed. The scanned record will then become the patients Electronic Health Record.

For ALL Electronic Health Records within our ePR systems the Trust interprets the useful life *"for the purpose of clinical decision making and care delivery"* to be until the patient is deceased. Electronic records will not be destroyed prior to notification of death, although may be moved out of active system storage into a lower tier of hierarchical electronic storage.

17. Process for Monitoring Compliance

This Policy will be reviewed periodically and amended to take into account changes in legislation and/or guidance by the e-Health Records Lead and submitted to the HRWG.

What is the standard/audit criteria	Time frame/ Format /how often	How/Method	Reviewed and action plan development by who/which group	Action Plans monitored by and how often
Incident Reporting	On-going	Datix(transition to Inphase)	e-Health Records Lead & General Managers	Bi-Monthly to Health Records Working Group
Health Record Audits. See Appendix E for Audit Proforma	Quarterly	Audit	Division/Specialty	Division/Specialty
Annual audit of the QA scanning process	Annually	10% of a day's scan throughput	Senior Information Risk Owner (SIRO)	Bi-monthly to Health Records Working Group

18. Training

Each department is responsible for ensuring that their staff are:

- made aware of the agreed processes and procedures within their ward/department/area, and,
- are given access and training for the IT systems required to enable them to perform their duties.

Appendix A
EDRMS Responsibilities

OUTPATIENT - Activity	Receptionist /Clinic Clerk	Clinic Nurses	Consultants	Secretaries	Xerox
Print out Event Packs for Walk In Patients	Y				
Print out additional smart forms where required	Y				
Ensure semi smart forms are available when necessary	Y				
Print out labels for outpatient appointments prior to the patient seeing the Consultant	Y				
Remove items from Event Packs that should not be scanned ie labels	Y			Y	
Print out header sheets where necessary ie for referrals	Y				
Print out the relevant header sheets for test results		Y			
Ensure all forms are filed behind the OP header sheet	Y			Y	
Ensure that all documents of size A5 & smaller are sellotaped on all 4 sides to A4 sized paper and attached to the correct header sheet paper ie test results		Y		Y	
To ensure all Event Packs are correctly filed prior to sending for scanning to Xerox	Y			Y	
Ensure all Event Packs are left with the Clinic Clerks or in an agreed secure location at the end of clinic		Y	Y		
Collect Event Packs from clinic areas					Y
To upload to Evolve external documentation which comes directly to the Consultant				Y	
To ensure all OP Event Packs are delivered to relevant areas					Y
To ensure Clinics have a supply of empty Event Packs for walk in patients	Y				Y

INPATIENT – Activity	Ward Clerk	Nurse	Xerox/Porters	Coding
Print out Event Packs for Emergency Admissions	Y	Y		
Ensure sufficient smart forms are in an Event Pack ie print out daily where necessary	Y	Y		
Ensure semi smart forms are available for clinical purposes when necessary	Y	Y		
Print out header sheets for non barcoded documents ie for Inpatient Correspondence	Y			
Ensure all forms are filed behind the Admission Episode Header Sheet (IH)	Y			
Ensure that all documents of size A5 & smaller are sellotaped on all 4 sides to A4 sized paper	Y			
Remove items from Event Packs that should not be scanned ie labels	Y			
Ensure all Event Packs are correctly filed before they leave the ward ie transfer or discharge	Y			
Ensure wards have a supply of empty Event Packs for emergency and long stay patients	Y		Y	
Collect Event Packs from wards			Y	

Appendix B

Secure Options for Sharing and Transporting Clinical Information

Section	Content
1	Introduction
2	Confidentiality
3	Option 1 – Export & Email
4	Option 2 – Export & NHS Secure File Transfer (SFT)
5	Option 3 – Requesting a DVD from Patient Services Team
6	Option 4 – Export and Transfer to DVD
7	Option 5 – Print & Post

1. Introduction

This guidance lists the secure options available when information from a patient's Health Record held in Trust Clinical Systems needs to be shared and transported to a recipient outside of the Trust.

2. Confidentiality

Sharing and transporting information inappropriately and in an unsecure manner could result in a breach of patient confidentiality and the Data Protection Act. When sharing and transporting patient information the following must be considered to ensure these risks are eliminated.

a) The information being provided must be no more than is required to serve the purpose.
b) It is the responsibility of the sender to ensure patient information being shared:
    - does not include information from another patient's record.
    - is only sent to the intended recipient using one of the options noted below.
c) The recipient of the information MUST either:
    - have a legitimate clinical relationship with the patient or,
    - have legal or statutory powers to request and receive patient information (please refer to the Trust's Information Sharing Policy), or,
    - provide proof of patient consent

If you have any questions please contact the Trust's IG Manager on 7928.

3. Option 1 – Export & Email:

Relevant documents can be "Exported" from Clinical Systems and sent by email.

When documents are exported from EDRMS they are automatically encrypted to NHS standard – you will be prompted to add a password to the exported documents.

For Example :Follow the EDRMS Instruction manual for creating a Summary Note and the one for Exporting Documents.

Check the Summary Note to ensure documents from other patients Health Records have not been filed in the wrong patient. If it does include documents from another patient's record

please log a call with the IT Service Desk to get these moved to the correct patient's record on EDRMS

Important…do *not* *send the password for the encrypted file in the same email as the file itself, but in the body of the email add the telephone number for the recipient to call to request the password, or send it in a separate email. Do not use the same password for all exported files*

4. **Option 2 – Export & NHS Secure File Transfer (SFT):**

The NHS SFT service has been established to support the secure transfer of large data files.

Linked to NHSmail it can handle transfers of up to 1GB in size and can, thus, reduce the need for the transfer of data using USB pens or CDs and DVDs. Files can be sent to any nhs.net user very quickly.

To use SFT you and the recipient/s must have an nhs.net email account.

If you do not have an nhs.net email account please log a call with the IT Service Desk who will set one up for you.

Instructions:

- Follow the EDRMS Instruction manual for creating a Summary Note and the one for Exporting Documents.
- Check the Summary Note to ensure documents from other patients Health Records have not been filed in the wrong patient. If it does please log a call with the IT Service Desk to get these moved to the correct patient's record on Evolve.
- Go to https://nww.sft.nhs.uk and follow the instruction.
- Communicate the password in an email or by telephone.

5. **Option 3 – Requesting a DVD from Patient Services Team (part of the Information Governance Department):**

Please note: This is NOT an "Urgent" service.

Instructions:

- Follow the Evolve Instruction manual for creating a Summary Note.
- Check the Summary Note to ensure documents from other patients Health Records have not been filed in the wrong patient. If it does include documents from another patient's record please log a call with the IT Service Desk to get these moved to the correct patient's record on Evolve.
- Complete the form "Evolve DVD Request" which can be found on the staff Intranet under "Information Governance Department" and send it to Patient Services Team or scan and email to patientservicesteam@ldh.nhs.uk

6. **Option 4 – Export and Transfer to DVD:**

For this option you will need a DVD writer (and the application it comes with). To purchase this please contact IT Service Desk for advice and assistance. You will also need a stock of DVD's (DVD-R), protective sleeves, a pen for writing on the DVD and a stock of bubble wrap envelopes – these can be purchased through the Trust's Purchasing system (currently Lyreco).

Instructions:

- Follow the EDRMS Instruction manual for creating a Summary Note and the one for Exporting Documents.
- Check the Summary Note to ensure documents from other patients Health Records have not been filed in the wrong patient. If it does include documents from another patient's record please log a call with the IT Service Desk to get these moved to the correct patient's record on Evolve.
- Insert DVD-R into your DVD Writer and follow the instructions for the application it came with.
- Write or stamp the Hospital name on the DVD. The date the DVD was created. Who it is being issued to. Any reference numbers and the patients NHS Number or name (**DO NOT** include the patients address).
- **Send the disk in a bubble wrap envelope using Recorded Deliver Post ONLY**.
- The password MUST NEVER be sent with the DVD. It MUST be sent in a separate letter using standard post, communicated by telephone or sent by email (does not need to be from your nhs.net email account).
- Ensure your communication with the receiver includes the following. This will help to ensure they are able to open and read the content of the DVD:

If you cannot open the folder on the CD please install a zip extractor such as 7zip found at the following link: http://www.7-zip.org/

If you experience difficulty opening the documents found on the disc please ensure you have the latest version of adobe PDF reader which can be found at the following link for free http://get.adobe.com/uk/reader/

Please note that these applications are not supported by the Trust, therefore we are unable to provide technical support following the installation of this software or accept any liability for any software download to your PC.

7. Option 5 – Print & Post:

Hard copies can be printed from Evolve and hand delivered or sent by post in line with the Trust's Information Governance Policy & Procedures.

PLEASE NOTE: If documents in an Event Pack are required they should be photocopied and the original kept in the Trust. Event packs or original documents from an Event Pack MUST NOT leave the Trust.

Appendix C

Principles of the Data Protection Act 2018

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.
Article 5(1) requires that personal data shall be:
1. Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
Article 5(2) adds that:
"The controller shall be responsible for, and be able to demonstrate compliance with, ('accountability')."

Appendix D

The Seven Caldicott principles

- ***Principle 1***
  Justify the purpose(s)
  Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

- ***Principle 2***
  Don't use patient-identifiable information unless it is absolutely necessary
  Patient-identifiable data items should not be used unless there is no alternative.

- ***Principle 3***
  Use the minimum necessary patient-identifiable information
  Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

- ***Principle 4***
  Access to patient-identifiable information should be on a strict need to know basis
  Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

- ***Principle 5***
  Everyone should be aware of their responsibilities
  Action should be taken to ensure that those handling patient-identifiable information, (both clinical and non-clinical staff) are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- ***Principle 6***
  Understand and comply with the law
  Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

- ***Principle 7***
  The duty to share information can be as important as the duty to protect patient confidentiality
  Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies