CLINICAL RECORD KEEPING POLICY

Adults and Children

Version:	1.0
Consultation Groups	Community Nursing Team Leads/Managers Clinical Policies Review and Alignment Committee
Approved By	Nursing Development Steering Group
Ratified By:	Quality Committee
Date ratified:	14th October 2020
Name and Job Title of author:	Caroline Ogunsola Professional Development Lead Nurse for Community Services
Executive Director Lead:	Ruth Bradley – Director of Nursing
Implementation Date:	October 2020
Last Review Date:	
Next Review Date	October 2023

Services	Applicable
Trust wide	√
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0		Caroline Ogunsola		

Members of the Community Services Clinical Polices Alignment Group are:

- Caroline Ogunsola – Professional Development Nurse for Community Services - Convener
- Dupe Fagbenro - Community Services Pharmacist – Bedfordshire
- Nike Bademosi – Clinical Lead – Tower Hamlets
- Fiona Davies – Clinical Lead – Tower Hamlets
- Chantal Riviera – Clinical Lead Newham
- Shilpa Matta Kambo – Clinical Lead – Newham (Physiotherapist)
- Victoria Stone – Locality Manager - Bedfordshire
- Georgina Amparado – Molina – Clinical Lead Tower hamlets
- Charity Okoli – Directorate Pharmacist – Newham
- Sharon Eplett – Locality Manger – Bedfordshire
- Davinder Kaur – Clinical Lead - Tower Hamlets (OT)
- Vikramsingh Totaram – Diabetes Nurse Specialist

1.0 INTRODUCTION

East London NHS Foundation Trust (referred to as the Trust in this document) depends on the records it holds in order to operate efficiently and account for its actions. The Trust has a statutory obligation to maintain accurate records of its activities and make arrangements for their safe keeping and or secure disposal.

1.1 All records created in the course of business of the Trust, both clinical and corporate records, of whatever format and medium are public records under the terms of the Public Records Acts 1958.

1.2 Clinical information is vital to the NHS and for the delivery of high quality evidence-based care on a day-to-day basis. Clinical records are a valuable resource because of the information they contain. Such information is only usable if it is correctly recorded in the first place, regularly updated, and is easily accessible when needed.

1.3 East London NHS Foundation Trust is committed to a systematic and planned approach to the management of clinical records, controlling both the quality and quantity of information generated, maintaining and storing records so that they serve the purpose for which they are generated and that all records are effectively controlled and maintained from creation to destruction.

1.4 Rationale:

The rationale for this policy is to promote consistency in providing accurate, timely, relevant clinical records that reflects the delivery of safe and coordinated care involving the patient, carer and family.

All clinical and administrative staff creating or contributing to the patients' or service users' records will provide an accurate, contemporaneous and timely health record which can:

- Determine and or demonstrate accountability and responsibility;
- Facilitate clinical decision making;
- Improve patient care through clear communication of the assessment, treatment and care planning rationale;
- Promote and facilitate continuity of care
- Reflect and demonstrate consistent approach to partnership working;
- Support in the investigation of incidents, complaints or legal proceedings.

1.5 Clinical Information Assurance Statement

The Trust is registered with the Care Quality Commission (CQC) which sets the standards of care expected of all NHS Trusts.
This policy is related to, and incorporates a range of best practice and relevant legislative requirements to outline the organisation's expectations for record keeping standards, both paper and electronic, and uphold our obligation including the following:

- Records Management: NHS Code of Practice 2016
- Relevant professional bodies
- Data Protection Act 1998
- General Data Protection Regulation 2018
- Information Governance Toolkit
- Caldicott Principles
- Access to Clinical Records 1990

- Common Law Duty of Confidentiality
- Human Rights Act 1998
- Freedom of Information Act 2000

The standards within this policy will:

- Maximise patient safety and quality of care by advocating accurate and contemporaneous record keeping.
- Promote patient involvement in the planning and recording of their care
- Ensure compliance with best practice across the Trust
- Facilitate nurses, allied health professionals and medical staff to meet their respective professional records keeping standards
- Provide a framework for non-professional staff to comply with Trust record keeping requirements
- Enable the management of clinical and corporate risk
- Underpin the record keeping audit of health records in the Trust to monitor compliance with expected standards
- Allow for information sharing and communication across and between the patient, clinical teams and partner organisations

To achieve these, clinical records must be timely with accurate, factual, concise and up to date accounts of the assessment and treatment, plan of care and evaluation of individual patients.

Accountability – records are adequate to account fully and transparently for all actions and decisions, in particular to:

- Provide rationale for clinical decisions
- Protect legal and other rights of staff or those affected by those actions
- Facilitate audit or examination by internal or external reviewers
- Provide credible and authoritative evidence
- Facilitate research and evidence based practice

Interpretation – the content of the record can be interpreted; i.e. clear and concise; identification of staff who created or added to the record and when; an objective account of care and how the record is related to other records.

Quality – records are complete and accurate and reliably represent the information that was actually used in, or created by, the delivery of care, and its integrity and authenticity can be demonstrated.

Staff training aim to ensure that all staff are aware of their responsibility for record keeping and where applicable are conversant and compliant in their professional responsibilities, standards and guidance. Good clinical record keeping is an integral and vital part of professional practice which contributes to support:

- Clinical care and continuity of care, including the assessment and management of clinical risks.
- Day to day hospital and community teams and their business which underpin delivery of care.
- Evidence based clinical practice
- The decision-making process

The record must also:

- Meet legal requirements
- Assist clinical and other audits
- Support improvements in clinical and social care practice

- Ensure information is available, whenever and wherever there is a justified need, and in whatever media it is required
- Promote patient involvement in their care

1.6 This policy outlines East London NHS Foundation Trust (the Trust) standards to underpin the provision of quality health care records, in all formats to mandate the way in which information is recorded, managed and used.

1.7 In services that use an electronic patient record, a secondary care record may also be in use. The secondary care record is for storing information that cannot be stored on the electronic patient record. Detailed guidance and standards for using the Trust's electronic patient record are included in the relevant Standard Operating Procedures.

2.0 Professional Record Keeping Core Standards

- All Healthcare Practitioners have a duty to keep up to date with, and adhere to, relevant legislation, case law, Professional Bodies and professional standards, national and local policies relating to information governance and record keeping standards.

- Health Practitioners are **accountable** for ensuring that they are aware of and know how to use information systems, for example electronic patient record systems EMIS / SYSTMONE/RIO/CERNER MILLENIUM or any other clinical system used by the team in accordance with local Trust policy and procedures.

- All Health Practitioners are **accountable** for entries they make to a patient record and must ensure that all entries made are clearly identifiable and each entry must be checked for accuracy prior to signing (written or electronic equivalent) in accordance with local Trust policy.

- All health records must comply with local policies and procedures, throughout the lifecycle of the record to include management, retention, review and disposal.

- Handwriting must be legible and written in black ink to enable legible photocopying or scanning of documents if required.

- Health records must be accurate and written in such a way that the meaning is clear and unambiguous (paper and electronic).

- Health records must demonstrate a full account of the assessment made and the care planned and provided; and actions taken including information shared with other health professionals.

- All entries must be recorded at the time of event or as soon as possible after an event has occurred (contemporaneous), within 24 hours.
- All entries must identify any risks or problems that have arisen and the steps taken to deal with them, so that colleagues who use the records have all the information they need.

- All healthcare professionals must complete records accurately without any falsification, taking immediate and appropriate action if you are aware that someone has not kept to these requirements.

- Health records must not include abbreviations or jargon, meaningless phrases, irrelevant speculation or offensive subjective statements, irrelevant personal opinions regarding the patient.

- If the date and time differs from that of when the records are written, this must be clearly noted in the record, and rationale given.

- All entries must be recorded, wherever possible, with the involvement of the patient/ client or their carer and written in language that the patient can understand.

- Health records must demonstrate any risks identified and/ or problems that have arisen and the action taken to rectify them.

- Every service user must have a Next of Kin (NOK) recorded in the records.

- Any corrections in handwritten records must be clear, dated and signed. For electronic records – follow the procedure in the appropriate standard operating procedure or handbook.

- Health Records must never be falsified.

- Health Practitioners must develop communication and information sharing skills with other professionals and providers of care as accurate records are relied on at key communication points, especially during handover, referral and in shared care.

- Legal requirements and local policies regarding confidentiality of health records must always be followed .

- Health Practitioners remain professionally accountable for ensuring that any duties delegated to non-registered practitioners are undertaken to a reasonable standard.

- The care delivered by non-registered practitioners (including students) will need to be overseen by a registered healthcare professional on a regular basis (determined locally based on the complexity and needs of the patients and their family) alongside a comprehensive review of the clinical records.

- Health records held on any form of media must be protected by appropriate levels of security, for example, locked records room, lockable trolleys and smartcard access

2.1 Who does this policy apply to?

This policy applies to all staff who are engaged in contact and delivery of clinical care to patients and refers to all information, in any media (but particularly paper and electronic), both active and inactive, that is recorded in relation to care provided to an individual.

This Policy must be read by all employees of the Trust, both permanent and temporary (e.g. bank, agency, locum, those on secondment and on honorary contracts). It also applies to anyone contracted by the Trust, who, in the course of their work are required to access clinical records normally restricted to directly employed staff, and to students and trainees on placements. The policy should be issued as part of induction programme for all new staff.

2.2 Definitions:

- **Health Record -** The Data Protection Act 1998 describes the health record as "consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual".

- **Paper Record -** Any of the following documents which record aspects of care of a patient or client can be required as evidence before a Court of Law or before any regulatory body:- e.g. Diaries**,** Incident forms**,** Attendance books, handover books, messages relating to the care of a patient and Clinic lists. This list is not exhaustive

- **Electronic Record -** The Electronic Patient Record is a secure, real-time, point-of-care, patient centric information resource. Electronic Patient Record (EPR) is an official health record for an individual that can be shared among multiple departments and agencies e.g. EMIS/ RIO/SYSTMONE/CERNER MILLENIUM. This may include "data", and is wider than just non-identifiable data used in business processes. This also includes all electronic information relating to a specific patient; e.g. activity; contracts; demographic information; care plans; assessments; carers/significant others

- **Contemporaneous -** Means records should be written at the time of or as close to the event described in the record.

- **Confidentiality -** All staff have a duty to protect the confidentiality of the patient record. Access to a patients records and the information contained in them must only be for an appropriate reason and by appropriate staff. See Standards of Conduct and Disciplinary Policy (HRP1) and Code of Conduct guidance for further details.

- **Caldicott Guardian -** The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information by safeguarding the confidentiality of patient information.

- **Access -** Means the opportunity or right to see records, under The Data Protection Act 1998, patients have the right to access their health records, subject to certain safeguards. See Access to Medical records policy for more details.

- **Being open (duty of candour) -** A culture of openness within the Trust ensures communication is open, honest and occurs as soon as possible following an incident, or when a poor outcome has been experienced. It encompasses the communication between healthcare organisations, healthcare teams, and patients, their families and carers, and ensures that the Trust supports staff in Being Open.

- **Records Lifecycle -** This 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. Refer to Records management Code of Practice for Health and Social Care (2016) for information on lifespan of records

- **Audit -** Audit provides a method for systematically reflection on and reviewing of practice to ensure compliance with current standards

- **NHS Number -** The NHS number is the only national unique patient identifier in operation in the NHS at this time. A ten digit number assigned to every individual registered with the NHS in England

- **Tracking -** Creating, capturing and maintaining information about the secure movement and use of records

- **People/User/Client/Patient -** These terms can be used interchangeably to represent users of services.

2.3 Duties / Responsibilities:

a. Chief Executive:
The Chief Executive has overall responsibility for Records Management within the Trust. The Trust has a responsibility for ensuring that it corporately meets its legal responsibilities that affect the safe management of health records, this responsibility is delegated to the Chief Information Officer. Each arm of the business (physical and mental health) takes responsibility which includes the on-going review, maintenance and upkeep of clinical documentation (both paper and electronic) and associated policies and procedures.

b. Trust Board
The Trust Board have overall responsibility for ensuring that the Trust delivers high quality services that are efficient and effective.
The Trust Board is made up of the Chair, Chief Executive, Executive Directors, and Non-Executive Directors. The Trust Board oversee the running of the Trust, make the decisions that shape future direction, monitor performance and ensure clear accountability.

c. Quality Committee
The primary function of the Quality Committee is to provide assurance to the Board of overall compliance with all statutory and regulatory obligations and ensure the effective management of Incidents, Complaints, Claims and Inquests and subsequent dissemination of lessons learnt, this includes the quality of health records. This group formally approves Trust Policies and the Information Governance Group reports to this committee.

d. Caldicott Guardian
The Caldicott Guardian within the Trust is the Chief Medical Officer. A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
The Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

This main role is to give advice when there is any uncertainty in the transfer of patient and service user information, seeking to clarify the purpose of the transfer, that it is justified; absolutely necessary; transferring only the minimum required; on a need to know basis and complying with the Data Protection Act 1998.

e. The SIRO (Senior Information Risk Owner)

The SIRO for the Trust is the Chief Information Officer and have the responsibility for the safe-keeping of all Trust records. The SIRO owns the Trusts overall information risk policy and risk assessment process ensuring we have a robust incident reporting process for information risks. The SIRO reports to the Trust Board and provides advice on the content of the Trust's Statement of Internal Control in respect to information risk

f. Information Governance Group

The Information Governance Group reports to the Quality Committee. In particular, the duties will include the review and monitoring of the:

- Trust's compliance with the Information governance processes
- Information Governance risks and to escalate them when appropriate to the Quality Committee
- Information Governance guidance which is relevant to the Trust and escalate when appropriate to the Quality Committee.

g. Record Keeping and Care Planning Workstream:

All clinical staff are accountable for their own actions and omissions. This includes record keeping performance as detailed within this policy, the relevant competencies and Professional Codes of conduct. The Quality Assurance Group (QAG) in each Directorate will constantly seek assurance that this process is compliant within their areas of responsibility and the monitoring of this process is undertaken by the Community Health Services Clinical Policies Review and Alignment committee.

h. Trust Records Manager

- Ensuring that the Trust complies with various frameworks, working collaboratively clinical leaders
- Ensure that the requirements of this policy meet the external standards set out in the Care Quality Commission, NHS Litigation Authority and Information Governance Toolkit. This will be monitored by the Records and Care Planning Workstream, with regular reports to the Information Governance Group
- Overall responsibility for the Access to Records Requests received by the organisation ensuring compliance with the requirements of the Data Protection Act 1998 and the General Data Protection Regulation 2018.
- Promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.
- Overall responsibility for the development and implementation of record management practices throughout the organisation.
- In collaboration with clinical leads, responsibility for the development of procedural documents and procedures that outline expected standards for managing the quality of health records within the organisation e.g SOP
- In collaboration with clinical leads, responsibility for the development and delivery of record keeping training in line with the Trust Standards and requirements

i. Directorate Leads have responsibility for:

- Ensuring that the standard of record keeping within their Directorate complies with Trust Standards
- Have responsibility for managing identified risks in relation to record keeping standards in the service at Directorate Quality Assurance Group
- The overall responsibility for monitoring staff record keeping training within the service in accordance with the Trust requirement.

- The overall responsibility for monitoring and implementation of action plans to improve quality of health records as required

j. Service Leads must:

- ensure that all relevant staff in the service are compliant with this policy
- ensure that all relevant staff comply with Trust procedural documents and procedures that outline expected standards for managing the quality of health records
- Have responsibility for identifying and managing any risks in relation to record keeping standards in their service
- Ensure that their service complies with Trust record keeping audits cycle
- Have responsibility for implementing recommended actions for the service following record keeping audits
- Must ensure that all relevant staff in the service attend training as outlined in the Trust Training Matrix

k. The Clinical lead/manager is responsible for ensuring that:

- All relevant staff in their locality/ team are aware of and compliant with this policy
- All relevant staff comply with Trust procedures that outline expected standards for managing the quality of health records
- Any risks in relation to record keeping standards in the service are identified and managed.

- All relevant staff in teams attend training as outlined in the Trust Training Matrix and that their team comply with Trust record keeping audits

- All actions from record keeping audits are implemented accordingly.

- Carry out audits and spot checks as and when necessary and as laid out in this policy.

- Report to Service Lead / Manager on issues affecting prompt recording of care delivered.

- Keep a record of staff signature in a secured place.

l. The Practice Development Team:

- Provide training and updates for all staff as and when required
- Keep a record of staff trained
- Share record of staff trained with L & D department so as to add to staff's profile on OLM
- Liaise with the clinical leads to monitor and maintain standards
- Provide support and supervision for staff currently not meeting the set standards until proficient
- Provide report and themes on all actions taken when required
- Share non-compliant concerns with the Service lead.

m. Team Leader is responsible for:

- Identifying staff who are not meeting set standards and provide necessary support for them in supervision. This can be done on three occasions
- Where staff is not meeting standards after three supervision meetings, then discuss with clinical lead and refer to the Practice development team.

- Ensuring that staff are booked onto Clinical system training as soon as they start in their new role, completing the induction booklet to confirm that this is done.
- Providing appropriate support for staff to enable them to familiarise themselves with various risk tools e.g. Waterlow score, SSKIN Bundle, CP-DAT etc.
- Liaising with the Clinical lead to ensure that new staff members are booked onto Clinical system training, and have the necessary tools to enable mobile working e.g. iPad
- Check staff records during supervision to ensure compliance
- Carry out local record audits and peer review monthly
- Carry out Record audit quarterly in line with Trust audit cycle.
- Work with the Practice development team to support staff as and when necessary.

n. Individual Employees (all staff) are responsible for:

- Their actions, inactions and omissions.
- Reading, understanding and complying with this policy and Trust procedural documents that outline expected standards for record keeping
- Attending training to keep up to date with best practice
- Reporting clinical incidents and near misses
- Cooperating and working positively with the practice development team if referred.
- Keeping up to date with relevant legislation relating to information governance and record keeping.
- complying with the common law duty of confidentiality; that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.
- Developing and updating personalised care plans
- Complete clinical risk assessment tools such as SSKIN, Waterlow, and CP-DAT etc. on EMIS/RIO/SYSTMONE/CERNER MILLENIUM according to professional responsibilities.
- Overseeing the quality of delegated care and related record keeping practice
- Demonstrating that the healthcare record is evidenced based.
- Providing a copy of a personalised care plan, where appropriate
- Safeguarding of confidential information held as paper records (in a structured filing system) and electronically (on computers and within information systems).
- Using agreed entry formats in their local area e.g. use of **S**ubjective, **O**bjective, **A**nalysis and **P**lan **"SOAP"** acronym in structuring entries in some community services. This format organises the documentation in such a way that it can be accurate, clear and concise. EMIS also prompts this documentation on progress notes and all are expected to make entries in this way.

Each letter of the "**SOAP"** acronym and expected content and actions are explained below:

SUBJECTIVE:

- This must include anything that the patient and/or you said during your visit.
- A summary is needed of key points - not every single word.
- Document reason for visit/ purpose of the session
- Document consent- how was this gained (verbally, non-verbally, best interests)
- How patient is feeling physically or mentally (e.g. mood/ pain) ideally this must be reported in patients own words

- Any relevant information provided by patient or carer (e.g. History or background information provided)
- Document who else was present during the session
- Any goals/priorities or concerns identified by patient or carer

OBJECTIVE:

- This is a Statement of what actually happened during the session including:
- Names of assessment tools and scores and measures/grading
- Any procedures or activities carried out e.g. dressings
- What did the patient do? e.g. mobility - Include any tests performed: range of movement, neuro, mobility, transfers etc.
- Any support provided to patient to carry out an intervention
- Basic vital signs and observations e.g. blood pressure, Spirometry test, pulse rate, respiratory rate etc.
- Advice and information provided by staff
- If several activities or issues are covered on the visit, this should be divided into subheadings

ANALYSIS:

- What is your analysis of the subjective and objective notes:
- What is your clinical opinion in summary, document key findings - If there are there any changes in presentation what might be the reason for this? e.g. is the situation stable/ improving/ deteriorating?
- Assessment of the situation, the session, and the client, regardless of how obvious it might be based on the subjective/objective.
- What was the outcome of your assessment and what does it mean in the context of your intervention (progress/lack of progress).
- Is the care plan meeting the patient's needs? If not what changes are recommended?
- Progress against a goal
- Any Risks identified
- What factors explain the patient's presentation?

PLAN:

- What is the plan for future? This includes treatment. e.g. further antibiotics, further dressings needed etc.
- Date/ day or frequency of next visit
- Need for discussion with other staff/supervisor
- Any reports or alerts that need to be completed
- Any specific changes to care plan and who will do this and when by
- Any onward referrals or joint visit required
- Risk management plan
- Discharge plans
- When is the next follow up/review? Date and time as much as possible
- What is the direction of the intervention?
- Any onward referrals.
- It is very important that clinicians follow up any promises made in the plan and document this clearly when completed.

All staff with authorised access to clinical information have a duty to keep clinical information confidential, secure and in line with the standards and procedures as set out in this and related Trust policies; professional standards and Codes of Practice; NHS Codes of Practice and Data Protection Legislation.

The Trust monitors the usage and access of accounts on electronic records systems such as EMIS/RIO/SYSTMONE/CERNER MILLENIUM.

Any unauthorised use of clinical information e.g. searching for information about a friend, neighbour, relative etc. or any use of information outside of a "legitimate professional relationship" may lead to immediate disciplinary action. The Trust views such breach of confidentiality seriously.

2.4 BANK & AGENCY CLINICAL AND NON-CLINICAL STAFF

All temporary clinical and non-clinical staff, including bank, agency nurses, locum doctors and other agency allied health professionals are subject to the same accountability and responsibilities in relation to the clinical record keeping and management standards in this Policy. The Trust provides agency and bank staff instant access to clinical records held on EMIS/RIO/SYSTMONE/CERNER MILLENIUM after a period of training.

2.5 TRAINING:

Training Requirements

- All new Staff should access a face to face Record keeping training either via web or classroom.
- All new staff are expected to access necessary training on electronic records within the first week of starting in post.
- A programme of clinical record keeping training courses will be available for clinical staff, as part of their continuing professional development requirements.
- All staff will be required to complete an e-assessment on record keeping principles every year on OLM.
- The completion of a record keeping self-assessment competency (Appendix …..) is required by all Health Care Professionals and this should be accessed for discussion during each employee's appraisal; and for professional regulatory body's revalidation evidence.
- During staff monthly supervision, the line manager should check three clinical record entries made by the staff member and establish any areas of good practice and areas for further improvement. This should be documented as part of the supervision record, and any relevant issues addressed accordingly following the Trust's policies and guidelines.
- Where staff is consistently non-compliant, a referral must be made to the Practice development team for support and further supervision until proficient.

3.0 CLINICAL RECORD CREATION AND MANAGEMENT

This section describes the organisation's standards to ensure that information contained within the health record is correctly recorded, regularly updated, legible, factual, and easily accessible. If it has not been written / recorded, it has not happened. Professional Regulatory Bodies also require registered staff to adhere to current professional record keeping standards as required by the following: -

- General Medical Council
- Health and Care Professions Council
- Nursing and Midwifery Council
- General Pharmaceutical Council

The important activity of making and keeping records is essential. These standards are to assist healthcare professionals to fulfil the expectations of the Trust and to promote the best

interests of patients. Health care professionals will promote respect, privacy, dignity and independence by placing the needs, wishes, preferences and decisions of people who use services at the centre of assessment, planning and delivery of care, treatment and support.

This includes discussion on risks and benefits, while balancing the need for preference and choice with safety and effectiveness**.** All staff must refer to and comply with the relevant Standard Operating Procedure for the electronic system they are accessing. Deviation from the Trust Policies and Procedures may lead to disciplinary action under HR guidance.
A percentage of clinical records will be audited by the Trust in each directorate during the year to ensure that standards within this policy are maintained.

3.1 Basic Record Keeping Standards:

- All paper records must be identified with the patient's full name and date of birth and NHS number.
- All records need to demonstrate accurate chronology of the patient's progress. If handwritten, it should be completed in black ink/typed for all entries, do not use pencil, as must be readable on any photocopies and with black ink
- Records should be dated and timed; the 24 hour clock should be used.
- Entries should be contemporaneous and made within 24 hours of event. If the time of recording varies significantly from the time of event, this must also be noted.
- Records should be accurately signed (validated) with the full names printed alongside each entry along with the designation. If electronic entries they need to be attributable to the author, including designation.
- When using paper records, staff must follow local procedures for signature management, and managers should always keep signature specimens in a safe and locked cupboard. Please see Appendix 3 for Signature specimen template.
- All clinical records must comply with the standards for record keeping set out in this policy**.** (Links to professional body websites to be added – NMC. HCPC. GMC. GPhC etc.)
- Diaries (paper and electronic) must not be used for recording clinical information.
- Any notes made during an unplanned visit, or in an emergency, must be transferred to the clinical record as soon as possible within 24 hours of event. Refer to Procedure for the Management of Personal Information for further guidance.
- The retention, archiving and destruction of clinical records will be managed via the Trust's **Retention, Review & Disposal Schedule; Archiving Guidelines and Procedure.**

3.2 When using RiO / EMIS/SYSTMONE /CERNER MILLENIUM:

- All staff have validation rights, including pre-registration students who will be working with a mentor that will monitor their records.
- All progress note entries must be validated by the originator.
- No entries should be deleted from the clinical records system because deletion of records on clinical systems such as EMIS/SYSTMONE/RIO/CERNER MILLENIUM could lead to harmful effect on patients.
- However, where deletion happens accidentally, this must be reported to the team leader or the shift co-ordinator who will advise the Electronic Clinical System team immediately.

3.3 RECORD KEEPING BEST PRACTICE

To adhere to best practice of record keeping, the following should be observed:

- All records should be written as soon as possible after the event; within 24 hours of returning to work.
- Meaningless phrases and offensive subjective statements unrelated to the patient's care and associated observations should be avoided.
- In patients with complex needs, high clinical record entries are expected.
- You must use your professional judgement to decide what is relevant and should be recorded as you are accountable for your own actions and omissions.
- The use of abbreviations must be kept to a minimum, if using abbreviations; they must be universally accepted and written out in full at the beginning of each individual entry or can be pre-printed in the footer of the documentation in use by the service.
- Dictated and typed in records should include the name and position of the clinician, checked and corrected as necessary; dated and signed by the dictating clinician.
- Letters may be reviewed by clinicians electronically using encrypted NHS mail or shared network drives with restricted access. They may then be marked "dictated and checked electronically but not signed personally to avoid delay".
- Administrative staff may contribute to clinical records, depending on agreed local procedures, e.g. the process for taking and recording messages. Where the record is available to the administrator, messages may be recorded, along with action taken to convey the message to the relevant clinician who is then responsible for any consequent action.
- When completing a form on behalf of the patient, all sections of the forms must be completed. If they are not applicable they must be struck through with a single line and marked "not applicable". Forms on electronic systems must be completed according to the relevant standard operating procedure and/or Service Specific Guidance.
- Pre-carbonated forms must be completed with a black ball-point pen.
- A single line must be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the error. No erasers or corrective fluids (Tippex), or any other obliterating agents should be used to cancel errors; for electronic records – follow the procedure as written in the local Standard Operating procedure or handbook.

3.4 CLINICAL INFORMATION STANDARDS

Clinical Information will vary depending on clinical service provided, and if relevant must include:

- A record of initial assessment
- A record of investigations and results
- A record of medication prescribed, including benefits and potential side effects
- A record of treatment
- A management / care plan with goals that are specific and measurable.
- A record of the patient's comments and/or related expectations and goals related to their health and their perceptions of their anticipated treatment (which may influence treatment / management plan)
- Entries should be made following every intervention (whether direct or indirect) by the healthcare professionals and at any other time as necessary.

- An entry per shift should be made as a minimum for patients who are active and being cared for in an inpatient setting or on team caseload to facilitate safe handover. The entry should summarise clearly the main elements of the care given and interaction with the patient over the course of that shift.
- If “aides memoires” are used for shift handover – these should not contain any information not already recorded in the clinical record and should be confidentially destroyed at the end of handover.
- It is important for staff to make accurate and meaningful records of the care that has been given to patients.
- One important thing to do is making clear the date and time that an encounter or intervention happened.
- Most often while using electronic record system on the desktop or iPad, this happens automatically.
- Electronic record system marks the notes entry with the date and time that it was typed and saved. However, sometimes we might not be able to make an entry in the notes at the time of an encounter with a patient e.g. if there's an emergency we need to deal with, or (rarely) if clinical system is not available.
- If a staff member must make a notes entry later, this must be entered within 24 hours of the clinical encounter.
- If the date and time of the clinical encounter differs from that of when the records are written, this must be clearly noted in the record with reason stated.
- Electronic clincal systems keep a clear and unchangeable audit trail of the actual date and time that an entry is made, and the Trust can be reassured that notes are meaningful, accurate and legal record of the care given.

More information is available from your local Electronic Record System trainer.

3.5 PATIENT HELD RECORDS

Treatment related information given to patients or left in patients’ homes will vary according to clinical needs and can include:

- Personalised care plan / goals
- Risks and benefits of treatment and relevant options where applicable
- leaflets (including source, version control and year of production) and any other documentation
- Specific verbal advice and details of any discussion with patients /or authorised relatives and carers or representatives
- Differentiation between information given to patients and carers and any other authorised representatives.

3.5.1 When clinical records are left in the patient’s home, relevant records concerning the care of the patient should be returned to the base after treatment according to the local procedure. However some records are held by patients for integrated care purposes including goal setting (e.g. My Record of What matters to me). Such records are shared, and patients can write in it too. A brief summary should be kept at the patient’s home, and main entries recorded on the appropriate electronic patient record.

3.5.2 Where care or treatment is likely to be delivered over a sustained period of time, it is good practice to regularly archive elements (according to defined local procedure) of the patient held record that are no longer required or relevant to the episode of care.

3.5.3 If it is considered that there is a significant risk of the clinical record being lost if left in the home, then the summary should be left in the patient’s home and

the main record retained for secure storage at the base. In some directorates, staff leaves minimum records with patients, and the main entry is made on the electronic clinical system RIO/ EMIS/SYSTMONE/CERNER MILLENIUM.

3.5.4 A Personal Child Health Record (PCHR) commonly known as the "Red Book" is issued to children at birth. Although this remains NHS property, it is kept at the family (carers) home and normally retained by the young person or family when the child becomes an adult. Relevant information will also be recorded in the electronic record by the Practitioner. The "Red Book" is a clinical record and can be requested at any time.

3.6 Communicating with Service Users by e-mail & Social Media

This does not include Facebook, Tweeter, Instagram, Telegram and Snapchats. These media are <u>not</u> acceptable for clinical patient records keeping.

Therefore, before agreeing to communicate with the patient or their carer/s via e-mail or text, the risks must be discussed with them, and a disclaimer/consent signed.

If the patient lacks mental capacity to consent, the patient/carer must give valid consent on initial assessment; and ongoing consent to the procedure. This may be verbal or implied (Refer to the Trust's Consent to Treatment Policy and the Mental Capacity Act Policy).

Where an adult patient lacks mental capacity (temporarily or permanently) to give or withhold consent, no one else can give consent on their behalf unless there is an identified Lasting Power of Attorney in relation to concerning health and financial matters. Lasting Power of Attorney must be registered with the Court of protection and must have a valid documentation to show this.

However, treatment may be given if it is in the patients' best interest except where there is a valid evidence of advanced decision to refuse treatment.

Any e-mail communication with the patient/carer must be printed off and filed in the paper record / inpatient care record. This can also be kept as an attachment to EMIS/SYSTMONE/RIO / CERNER MILLENIUM; to ensure the exchange forms part of formal documentation and correspondence, and to maintain an audit trail of communications. See **Consent Form for Email or Text in Appendix.**

The Professional bodies e.g. Nursing & Midwifery Council set out some principles that can be applied to other kinds of online communication, such as personal websites and blogs, discussion boards and general content shared online, including text, photographs, images, video and audio files. Please see the Professional bodies guide on the use of Social media e.g. NMC Standard for the use of social media.

3.7 Communicating with Service Users by Text including WhatsApp, Viber, Imo etc:

- It is right to say that text messages are not given the same level of record keeping attention given to other forms of digital records as there are no archiving solution in place for the retention and oversight of text messages, which causes problems and significant risk when facing a regulatory examination, open records request, an investigation, e-discovery event or litigation.
- Emails, social media accounts and corporate websites are often monitored, but text messages must be brought into this perimeter to further reduce risks. Currently,

most Trusts do not monitor business text messages sent and received by their employees.

- Although texting is easy, concise, reliable and intuitive, where it is used for official Trust business communications, please note that it can present tremendous risk. Text messages is extremely accessible when an employee wants to communicate with their colleagues, patients, carers, or prospects in a time-crunched, connected society. Text messaging without proper governance is a major gap that can no longer be ignored.

- Sending text messages between mobile devices is now one of the keyways that employees connect with each other, patients, carers and other professionals therefore these records need to be maintained for completeness.

- Where texting communication is agreed between the patient and practitioner, the risks must be explained, and they must sign a consent form which will be filed in their electronic record). See draft consent form in Appendix…

- The Practitioner and patient must ensure the nature and content of text message/ email communication is always kept professional. This must be discussed between the practitioner and patient when completing the Patient Consent Form for Email and Text Message Communication. All email/text communication should be ceased if the terms within the consent form are breached.

- Practitioners engaging in text message communication must ensure the conversation is documented on the patient's electronic record.

- Text message communication can be 'quoted' word for word and typed in progress notes; emailed and uploaded as a document or via a screen capture which is then uploaded as an attachment.

- It is the practitioner's responsibility to be able to justify any exempted text message or email that has not been documented. All practitioners will be accountable to their professional body.

- If possible, services and staff should only send emails from generic team accounts (for example **diabetes@lgi.nhs.net** / **oncology@coch.nhs.uk**) and established corporate text messaging accounts. This ensures that patients / service users can be confident that the sender is legitimate.

- Use of generic accounts also ensures that emails and text messages can be accessed and actioned by multiple members of staff, providing cover in the event of absence.

- Practitioners must not use their personal phone to contact patients/services users. It would be advisable to use the email text messaging system.

- If there is a need for the practitioner to communicate via text message to any young person under the age of 18; an adult with parental responsibility must agree and sign the Text Message Communication consent form to approve this.

- The young person must be deemed **Fraser** competent (term originating in England and used in medical law to decide whether a child under 16 years of age is able to

consent to their own medical treatment, without the need for parental permission or knowledge) and must also be made aware of the terms within the consent form.

- Practitioners should not be communicating via text messages to any other person other than the consented patient, main carer or those who have parental responsibility.

- Text messages relating to Trust business are public records whether sent or received on a Trust or private mobile phone. However, text messages that are private are not automatically public records, even if sent on a work mobile phone. See **Consent Form for Email / Text.**

- Text messages must be kept in a searchable format that cannot be tampered with, destroyed, or otherwise disposed of by anyone on purpose, or accidentally.

- Text messages must be produced quickly for FOI or public records requests, and regulatory examinations.

- Therefore, **all text messages must be emailed to the sender's NHS email account** and attached to the electronic records of the patient on EMIS/SYSTMONE/RIO/CERNER MILLENIUM. This gives clear and consistent picture of events concerning the patient.

- Please note that Mobile phone Network providers do not keep records of text messages for long, and they are not obliged to provide records of them.

- The responsibility for retaining and producing requested text messages lies with the organisation that creates the records.

a. Risks of sending Text messages:

i. Legal risk

- Text messages can be requested as part of a litigation investigation or event, since texts are often considered relevant electronically stored information (ESI) within an organisation. Many courts compel the production of texts in civil litigation, if a mobile device is believed to possess relevant text messages.

- While other forms of electronic communication, including email, are relatively straightforward to collect, archive, and extract, text is different. Text messages can be emailed to your Trust official email account, and then saved as an attachment on the electronic clinical system.

- If a company's legal team cannot find and or produce text data in real-time, and respond quickly and completely when asked to search and produce specific text messages in an investigation, the Trust may face legal consequences related to missing records, or failure to produce requested data — and can be fined by the Information commissioners and or have to pay high legal fees.

ii. Reputational risk

The use of text messaging without the proper monitoring protections in place can leave the Trust susceptible and affect the reputation of the Trust.
Monitoring text messages and other electronic communications on a regular basis will enable steps to quickly assess potential threats, and mitigate actual problems when they occur.

When a company has access to these content types with a single comprehensive archiving solution, conversations can be monitored from a broader and more holistic perspective. For instance, conversation threads can be followed easily when a discussion starts on social media, moves to email, and concludes in text messages.

iii. **Regulation risk**

The Trust is regulated by the Care Quality Commission and as highly regulated industries, thus will retain and supervise text communications in the manner described in this policy.

Similarly, many organisations have seen recent rulings that reinforce how text messages are classified as business records. Essentially, any highly-regulated industry that has record keeping requirements for business communication must archive electronic messages, no matter what platform they are on—and that includes mobile devices.

3.8 PANDO MESSAGING SERVICE FOR NHS & LOCAL AUTHORITY STAFF

Pando is the new UK's most widely used clinical messaging platform that is approved by NHS Digital and listed in the NHS Apps Library.

Pando is the essential tool for teamwork and secure collaboration. It is designed to benefit anyone working in health and social care, working in a team, with a need to share sensitive information and images securely. Pando verifies the identity of all our users to make sure that information can be shared securely and with the right people.

a. Features

In comparison to other clinical messaging apps, Pando is made solely for health and social care workers and equips them with features specifically made for them. These include secure messaging, image capturing and patient lists. Each feature is being developed based on an existing problem our users are facing and is being thoroughly tested to make sure Pando serves their exact needs.

Pando is designed to provide a platform that is efficient, reliable, and supports a sustainable work-life balance. It is PIN protected and has no time limit on data storage, making sure that you can always access it when you need it.

b. Secure Messaging

Find and contact other professionals – search by name, role or hospital.

- Create groups with more than 100 colleagues.
- Individual and team messaging.

- Message people within your organisation or the wider region.
- Broadcast messaging to the entire staff to distribute critical information.

c. Forums

- Join an open forum dedicated to a particular conversation topic.
- Cross-organisation collaboration to share best practices.
- Fixed point of contact for staff at health & social care organisations.
- Search and join a forum or create a new one.
- Share & get information on current topics.

d. Image Capture & Export

- Take images with Pando, upload them from your device or export them from the app.
- Take pictures and organise them in your personal in-app gallery.
- Come back to images and attach them to a patient card or export them to your secure email.
- Keep track of your patient's progress and get instant advice from colleagues.
- Images are never stored on your personal device.

e. Patient Lists

- Keep your patient information stored securely and up to date.
- Manage your patients and keep track of your tasks.
- Assign patients to your colleagues and share updates instantly.
- Attach notes and images to a patient to record their progress.

f. Work-Life Balance

- Mark yourself unavailable when you are off work and let others know.
- Stop receiving notifications for 1 hour, 48 hours or indefinitely.
- Your network is informed whether you are available or not.
- Facilitate decision-making when working from home – but turn off when you need to.
- Separate your work and personal messages and switch off.

g. Communicating with professionals using Pando.

In practice some of our teams use Pando to communicate with other team members, not patients. However, they share patient information via Pando as it is safe to do so.

The Pando application is a secure communication and collaboration tool designed to benefit anyone working in health and social care, working in a team, with a need to share sensitive information and images securely. Pando verifies the identity of all their users to make sure that information can be shared securely and with the right people.

- Pando offers a variety of features that aim to help professionals share information immediately, including the following:
- Message individuals, teams or the entire staff
- Import, attach and securely send images (images are never stored on the device)
- Create task and patient lists – which you can attach images and notes to, and share with colleagues
- Pando communication is only used between professionals. When using the Pando application to share patient information, staff must ensure:
- Consent is gained before sharing information.
- Keep information confidential and only share with professionals within the application.

- Keep login details confidential.
- Adhere to the standards laid out in this policy.

An example of how Pando was used in patient care:
"Before transferring a critically ill child to the community, the team was able to engage a surgeon and an intensive care specialist for advice and devise a management plan, all through Pando. Ultimately an intubation was avoided, and the child was transferred to definitive care much sooner than if he was intubated at the time". – ***Team member in a team where Pando was effectively used for care coordination.***

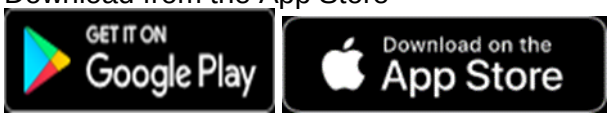
TO ACCESS PANDO:
Connect with your colleagues & share information securely. Free to use messaging service for NHS & Local Authority staff.

Step 1 - Download Pando from App Store Google Play or Apple App Store (See image below)

Step 2 - Sign up with your NHS or Trust email

Step 3 - Connect with your colleagues

Download from the App Store



3.9 Communicating with services users through Social Media

- All staff must use all forms of spoken, written and digital communication **(including** social media and networking sites) responsibly and with great professionalism.

3.10 Deceased patients:

- Once a patient has died, all information relating to the delivery of care prior to the death must be recorded on the record. The cause of death, if known, should also be recorded.
- In the event of a retrospective entry needing to be recorded, staff should raise this with their Manager, and follow local service specific guidance. Additional information may need to be recorded in the deceased patient records (e.g. bereavement follow-up) and staff should follow local service specific guidance.

3.11 Child Deaths

- Staff receiving information of a child's death should notify the Safeguarding Children's Single Point of Contact (SPOC). Staff should follow the Safeguarding Children's relevant policy.

- Details of the death notification should be recorded into the Electronic Patient Record within 24 hours of notification. SPOC can support and give advice on any recording.

3.12 Filing

- Each volume of the paper containing clinical record must have the agreed index and clear instructions regarding filing of documents. Refer to the appropriate local Standard Operating Procedure for details.

- All documentation in a paper record must be hole-punched and filed chronologically, according to the index.

- Folders with “back pockets”, or “plastic wallets” must not be used. “Post-it notes” must not be used. See Health Records Policy for more information

4.0 ARCHIVING OF RECORDS:

All clinical records must be properly archived according to local procedure to facilitate easy and prompt access to records as and when needed. For staff TUPE’d into ELFT e.g. Tower Hamlets Community health services, please contact your local Records officer for information about archiving pre ELFT days.

Please see Trust’s Health Records Policy and Records Retention guidance for more information; for advice of Freedom of Information request, please refer to the Trust’s Freedom of Information policy available on the intranet or contact the Trust’s Information Governance manager or your local Records officer.

4.1 Confidentiality & Information Security

- All clinical information, whether created and stored as an electronic or paper record, must be kept secure. Each individual staff member is responsible for the information that is in their care and disciplinary processes will be followed if information is inappropriately accessed or lost.

- Unavailable, mislaid or lost clinical records are a serious risk to the Trust and it is therefore vital that tracking/tracing procedures are always in place and followed.

- If however, clinical records are unavailable, mislaid or lost, it is vital that appropriate action is taken to manage the potential loss of the information. This must be treated as an incident and logged on Datix accordingly.

4.2 Management of Clinical Records of staff who are patients/service Users

Staff who are also patients and or service users through this policy are assured that:

- Only staff that have legitimate professional/clinical, administrative, managerial or reporting reason or relationship with the patient are authorised to access information held by the Trust on electronic or paper clinical records.
- Information contained in clinical records is confidential and must be handled in line with NHS Code of Confidentiality; i.e. all client information, in whatever format, must not normally be disclosed outside of the care team without the consent of the client.

  There are three exceptions to this:

- Where the relevant client has consented;
- Where there is a risk of serious harm and/or disclosure is in the public interest; or
- Where there is a legal duty, for example, a court case

Unauthorised access may contravene the Computer Misuse Act 1990, the Data Protection Act 1998 and other legislation that may result in prosecution and disciplinary proceedings. Experience has shown that storing staff records separately or failing to enter data electronically increases the risk of:

- Missed contacts or appointments;
- Failure to share information appropriately;
- An adverse incident not being dealt with appropriately.

Therefore, all clinical staff records (electronic or paper) should be kept in line with local procedures and practice and not be held in a different format or location.

Any member of staff or a relative of a member of staff who receives care from the Trust must be advised at the outset that:

- All staff working in the Trust has a legal duty to keep information obtained during an episode of care about a patient confidential.
- Anyone who receives information from the Trust is also under a legal duty to keep it confidential.
- The Trust needs to keep clinical records about the care and treatment provided to individual patients. Such records will be kept manually (in the form of case notes) and/or electronically (e.g. EMIS/RIO/SYSTMONE/CERNER MILLENIUM). They are vital in ensuring the provision of good quality and timely care, and useful for investigation purposes and continuity of care.
- Information about patient care may be shared with other professionals and services on a need to know basis and consent may be required as part of this process.
- **Staff must only login into the Trust's electronic patient record e.g. RIO/EMIS/SYSTMONE / CERNER MILLENIUM using their own access details** and must not share their login details with anyone else. This may be via a Smartcard, and staff must comply with the Registration Authority Policy.
- **Staff must not login to the Trust's electronic patient record using someone else's login details**, **or make entries in the electronic patient record via someone else's log-in or via someone else's Smartcard.**

- **Staff must not use their own log in details or Smartcard to record care provided by another staff member**.

- All staff should be aware that the Trust performs comprehensive electronic system access audit trails regularly, on a monthly basis.

- Abuse of Smartcards and/or logins is a serious issue, which will result in disciplinary action which could lead to dismissal.

Refer to Information Governance and IMT Security policy at
http://elftintranet/sites/common/Private/Community_View.aspx?id=406&pageid=4553&url=ObjectInContext.Show(new%20ObjectInContextUrl(2%2C58082%2C1%2Cnull%2C970%2Cundefined%2Cundefined%2Cundefined%2Cundefined%2Cundefined))%3B

Health Records Policy at:

http://elftintranet/sites/common/Private/Community_View.aspx?id=406&pageid=4553&url=ObjectInContext.Show(new%20ObjectInContextUrl(2%2C58940%2C1%2Cnull%2C970%2Cundefined%2Cundefined%2Cundefined%2Cundefined%2Cundefined))%3B

4. 3 Patient Opt-out

Patients have the right, under Section 10 of the Data Protection Act, to request to "opt-out" of having an electronic patient record. This decision is based on clinical risk assessment, and impact on the individual. Refer to the Trust's EPR Opt-out Procedure for detail and process.

5.0 ACCESS TO ELECTRONIC PATIENT RECORDS (EPRS)

In order to be given access to the Trusts EPR staff must be working in a role that requires access to clinical records.

Staff must have a legitimate reason for accessing an EPR. This includes:

- Recording clinical information
- Reading clinical information of clients referred to the clinician / team where there is a legitimate relationship with the client
- Reading clinical information about clients that present to the service without a referral
- Monitoring and auditing the completeness and quality of the record
- Undertaking reviews, gaining feedbacks and investigations
- Providing support, assistance and guidance to staff

Any unauthorised use, for example searching for information about a friend, neighbour, relative, famous person, accessing their own record etc, or the use of information that is not directly related to the provision of care to the client (i.e. legitimate relationship) will be referred to the appropriate manager for an investigation. If unauthorised use is proved, this will lead to disciplinary action being taken. Findings from investigations may also be referred to the relevant professional body.

5.1 Unqualified/non-registered staff using EPRs

All unqualified or non-registered clinical staff will have access to appropriate EPRs. The quality of their entries remains the responsibility of the Lead Clinician for the service, and clinical supervision should be used to ensure that the staff member has the competence to complete clinical records. For example, going through three clinical records entered by the staff member during one to one supervision and discussing the quality of the entries.

6.0 MONITORING AND AUDIT

Standards	Monitoring and Audit			
	Method	**By**	**Frequency**	**Reviewed by and actions arising followed up by**
Random audit of 6 home records per locality	Random visits / Peer review	Clinical leads	Monthly	Local QAG
Appropriate storage and documentation at all levels.	Audit of records including electronic record	Clinical Leads	Quarterly	Local QAG
Awareness and understanding of policy	Induction of New staff Launch and Induction Availability on intranet	Clinical Leads / Team leaders Caroline Ogunsola	As and when new staff are appointed Annually	Local QAG Report to Local Quality Assurance Group (QAG)
Peer review of records	Audit	Peers in each area	Quarterly	Assurance provided via the clinical lead at QAG Meeting

6.1 Management of Mental Health Act Documentation

This is specific to patients who are subject to the Mental Health Act and the process is administered by Mental Health Act Administrators. These records are not part of the clinical record but clear standards and procedures are required in order to comply with the CQC. See **Mental Health Act Documentation Procedure** for detail.

6.2 Subject Access Request – Access to Records

Under the Data Protection Act 1998 (DPA) and the General Data Protection Regulation 2018 individuals (data subjects, staff or patients) have the right to review and receive copies of their own records. See **Subject Access Requests and Disclosure of Personal Data Procedure** for details on how to manage a request.

6.3 Litigation and Complaints Documentation

Clinical records must not contain information (inc. correspondence, reports, statements emails) relating to complaints, critical incident reviews or litigation. This

includes inputting or uploading into electronic patient record systems on EMIS/RIO/ SYSTMONE / CERNER MILLENIUM. Information relating to these processes must be maintained in a separate file, according to the Records Management Code of Practice.

7.0 Policy Review

This policy will be reviewed in three years, or earlier if necessitated as a result of changes to legislation, Codes of Practice or National Standards.

Associated guidance, procedures and templates will be updated as required, and signed off by the Nursing Development Steering Group, and or the Information Governance Group (as required).

8.0 Associated Documents

Please refer to the Trust website including:

- The Public Records Act 1958 http://www.nationalarchives.gov.uk/
- NHS Code of Practice: Records Management 2016
- The Data Protection Act 1998 https://ico.org.uk/
- Access to Health Records Act 1990
- NHS Code of Practice: Confidentiality 2003
- NHS Health & Social Care Information Centre http://www.hscic.gov.uk/
- Information Governance Toolkit https://nww.igt.hscic.gov.uk/Home.aspx
- Care Quality Commission http://www.cqc.org.uk/
- Nursing & Midwifery Council http://www.nmc.org.uk/
- General Medical Council http://www.gmc-uk.org/
- Common Law Duty of Confidentiality
- The NHS Care Record Guarantee
- Human Rights Act 1998
- Freedom of Information Act 2000
- Caldicott Principles
- Care Quality Commission

References:

NHS England. 2016. Accessible Information Standard: Using email and text message for communicating with patients- guidance from the Information Governance team at NHS England. Available at https://www.england.nhs.uk/wp-content/uploads/2016/04/Using-email-and-text-messages-for-communicating-with-patients.pdf [Accessed on 19/09/19]

Appendix 1

Patient consent for email & text message

Appendix 2

Email and text message agreement f

Appendix 3

Signature specimen template .docx