Essex Partnership University
NHS Foundation Trust

RECORDS MANAGEMENT POLICY

POLICY REFERENCE NUMBER	CP9
VERSION NUMBER	3
KEY CHANGES FROM PREVIOUS VERSION	Removed all reference to creating paper files Updated processes
AUTHOR	Records Manager
CONSULTATION	Information Governance Steering Sub Committee Quality Committee
IMPLEMENTATION DATE	August 2017
AMENDMENT DATE(S)	August 2018
LAST REVIEW DATE	December 2021
NEXT REVIEW DATE	December 2024
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB- COMMITTEE	October 2021
RATIFIED BY QUALITY COMMITTEE	December 2021
COPYRIGHT	

OPERATIONAL POLICY SUMMARY

The purpose of this policy is to set out the overall aims and objectives of the Trust in the effective management of its records.

Effective records management is one element of information governance. There are records management standards in the Information Governance Toolkit and the achievement of Toolkit standards forms part of the overall Care Quality Commission assessment for the Trust.

The Trust monitors the implementation of and compliance with this operational policy in the following ways;

The Clinical Audit Department will include clinical/healthcare records audit as part of the annual programme as supported by the Service Leads. The clinical audits will be supported by the Clinical Audit Department with tool development, analysis and reporting. The clinical audit reports will be presented within the service Quality and Safety meetings to address any initial actions, escalating any issues and concerns via the reporting structures

SCOPE

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

RECORDS MANAGEMENT POLICY

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

RECORDS MANAGEMENT POLICY

ASSURANCE STATEMENT

This policy aims to ensure that the Trust has a systematic and planned approach to the management of records, from the moment they are created to their ultimate disposal, which ensures that the organisation can control both the quality and quantity of the information that it generates; can maintain that information in a manner that effectively serves its needs, those of government, the law and of the citizen; and can dispose of the information efficiently when it is no longer required.

The principles of this policy apply equally to all records whether created paper, electronically or digitally, and includes both medical and corporate records, as the concern is the records content or information and not the medium of delivery.

1.0 INTRODUCTION

1.1 The purpose of this policy is to set out the overall aims and objectives of the Trust in the effective management of its records.

1.2 Effective records management is one element of information governance. There are records management standards in the Information Governance Toolkit and the achievement of Toolkit standards forms part of the overall Care Quality Commission assessment for the Trust.

1.3 The adoption of corporate procedures, practices and standards is essential to ensure effective records management is consistently applied throughout the Trust in a systematic and sustainable manner.

1.4 Recent legislation, particularly the Freedom of Information Act 2000, has a significant effect on records management in public authorities. The Trust must ensure that records management policies and procedures are fully compliant with legislation and with Government policy on the management of information.

1.5 In line with Information Governance Alliance Guidance 2016, The National Archives' Records Management Standards and Guidance, the policy statement for the Trust is that it is committed to adopting:

1.6 The new data protection legislation came into effect in May 2018. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 replaces the Data Protection Act 1998. Many of the main concepts and principles are much the same as those in the Data Protection Act 1998. The following regulations have been introduced. The right to be informed/right of access/rights of automated decision making and profiling.

The right to rectification -

This gives individuals the right to have incorrect personal data rectified or completed if incomplete.

The right to erasure -

This gives individuals the right to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.

The right to restrict processing -

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

The right to data portability -

This will allow a requester to ask for a copy of personal data in an electronic format.

The right to object -

This gives individuals the right to object to the processing of their personal data in certain circumstances

The Trust has one calendar month to respond to all of these requests.

2.0 DUTIES

2.1 The Information Governance Steering Sub Committee (IGSSC) is responsible for approving the content of this policy and monitoring its compliance and effectiveness.

2.2 The Quality Committee is responsible for noting the approval of this policy.

2.3 The Chief Executive with delegated responsibility to the Director of ITT and Senior Managers (defined as Band 8 or above) – are personally accountable for records management within the organisation. The following Directors have specific responsibility for ensuring compliance and that adequate procedures and good practice are in place within their area of responsibility

(a) Clinical/health records (Executive Medical Director/Director of ITT)

(b) Personnel and Administrative records (Executive Director of People and Culture)

(c) Commercial/business records (Executive Chief Finance Officer / Deputy Chief Executive)

2.4 The Chief Executive has delegated responsibility for Caldicott issues to the Executive Medical Director, who has responsibility for reflecting patients' interests regarding the use of patient identifiable information, together with ensuring that patient identifiable information is shared in an appropriate and secure manner.

2.5 The Data Protection Officer is responsible for the development, implementation, compliance, monitoring and review of the data protection legislation, including providing guidance on records management issues, and ensuring that related policies and procedures conform to the latest legislation and NHS guides on data protection, patient confidentiality, information security and rights of access to information.

2.6 The Head of Electronic Systems & Information Governance and the Records Manager is responsible for records management within the Trust and for monitoring compliance and effectiveness of this policy. They are the responsible officer of this policy.

2.7 It is the responsibility of all staff including contractors and third parties to comply with this policy in carrying out their duties within the Trust and for bringing any areas of non-compliance or queries on its application to the attention of their line manager.

2.8 The Information Governance Steering Sub Committee (IGSSC) is a multi-disciplinary committee that is responsible for overseeing records management and advising on local policies relating to retention, archiving or disposal of sensitive, personal health / social care or corporate records, and ensuring that adequate resources are available to meet the Trust's obligations and that policies and procedures are adhered to.

3.0 DEFINITIONS

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

- Information Governance Alliance – Records Management Code of Practice for Health and Social Care Records 2016
- Care Quality Commission – outcome 21
- The Freedom of Information Act 2000
- Data Protection Act 2018
- Lord Chancellor's code of practice on the Management of Records issue under section 46 of the Freedom of Information Act 2000
- Public Records Act: 1958 and 1967

3.2 The Trust creates, receives and maintains records and information covering a wide range of activities, subjects and actions. Records and information may relate to patients, staff, financial transactions, strategic planning, daily operations, policies and procedures.

3.3 It is likely staff will receive requests for information and/or copies of records from patients, external institutions or members of the public. For example:

- A patient may request to see his/her patient records
- Relatives of a patient may request to see his/her records
- A member of the public may request to see a copy of a Trust policy document
- A research organisation might request some statistics on hospital admissions
- A member of staff may request to see what is written about them in an appraisal

3.4 Requests may be received for both confidential and non-confidential information

3.5 A record is: any information held on any format e.g. electronic systems, paper, CD, microfilm including (Health and Social Care records and Corporate records)

Written	For the purposes of this policy the term 'written' denotes a tangible copy; which must be printed matter from the Trust's electronic system, typed documentation or hand written documents.
The unified health and social care record	A completely unified health and social care record that comprises all of the demographic, social care and clinical care information for a patient/service user's care pathway. If paper, there may be more than one volume comprising the unified health and social care record for a patient/service user.

The subsidiary record	A health and social care record that is maintained in parallel to the unified health and social care record, when there is more than one mental health service being delivered to a patient/service user and the records are in a paper format.
The electronic unified health and social care record system	The complete and identifiable health and social care record for a patient/service user held in electronic form; which provides 24 hour access to authorised practitioners and staff.
Social care record	A record created and held by social services staff.
Person identifiable	Containing any information from which a person will be identified – for example: patient/service user or carer's name, initials, address (including postcode), date of birth etc.

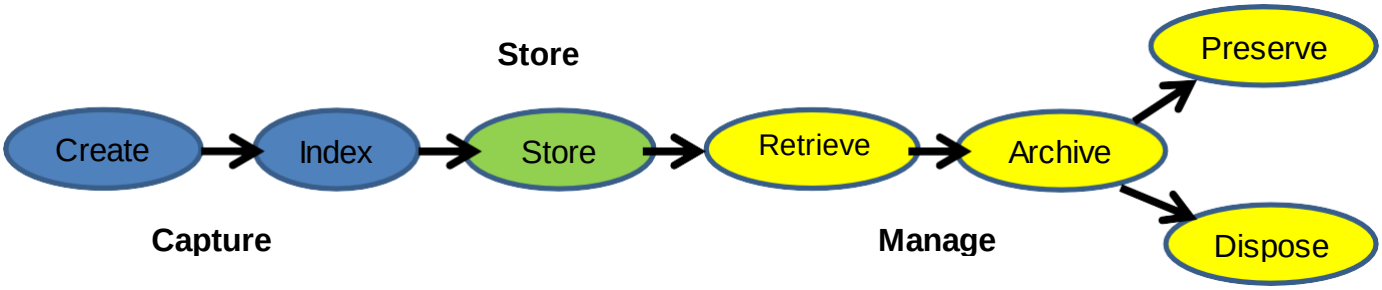
4.0 PRINCIPLES

- To support the guidelines contained in the Information Governance Alliance – Records Management Code of Practice for Health and Social Care Records 2016
- To identify the way in which the management of records in the Trust is currently structured.
- To support Information Governance - covering the Data Protection Act 2018 and Freedom of Information Act 2000.
- Accountability – to ensure accurate records are maintained for legal, audit or examination purposes.
- To provide documented retention and disposal schedules to include provision for permanent preservation of archival records.

5.0 RECORDS PROCEDURES

5.1 Records Management Lifecycle

Records lifecycle in records management refers to the following stages of a records "life span": from its creation to its preservation (in an archive) or disposal.



5.2 Records Creation

5.2.1 The content of a record will primarily be determined by the purpose for which it is being created, for example a personnel file will contain information about an

employee relating to things like employment history etc., a patient's medical file will contain information about diagnosis and treatment.

5.2.2 Records of business activity should be complete enough to:

- Facilitate an audit or examination of the business
- Protect the legal and other rights of The Trust, its patients and any other person affected by its actions
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

5.3 Records Storage Off-site

5.3.1 Offsite storage is managed by external contractors, they offer active storage, semi-active storage and deep storage. Requests for records to be sent offsite and or retrieval must go through email - epunft.essex.records@nhs.net

5.3.2 Records archived with the external contractors should be fully indexed and referenced to the box and should be sent with a review/destroy date (in line with The Trust retention schedule) clearly identified.

5.4 Records management / keeping

5.4.1 The importance of good record management cannot be underestimated. It ensures that:

- All records created are of the highest quality; are accurate, clear and relevant and meet required standards of data quality
- Records are always accessible, and staff in the organisation are able to work with maximum efficiency without having to waste time hunting for information
- There is an "audit trail" which enables any record entry to be traced to a named individual at a given date-time with the secure knowledge that all alterations can be similarly traced
- Those needing to read records at a later date can see what has been done, or not done, and why
- Any decisions made can be justified or reconsidered at a later date

5.4.2 In addition, the Trust recognises the need to manage records properly to:

- Support patient care and continuity of care
- Support day to day business which underpins delivery of care;
- Support evidence based clinical practice;
- Support sound administrative and managerial decision making, as part of the knowledge base for NHS services;

- Meet legal requirements, including requests from patients under access to health records legislation;
- Assist health and other audits; and
- Support improvements in clinical effectiveness through research and also support archival functions by taking account of the historical

importance of material and the needs of future research.

Record Keeping

5.4.3 High quality record keeping is one of the main components of Clinical Governance and we must ensure that health and social care records made by staff within the Trust are of consistent quality. This will be achieved by:

- Establishing and maintaining consistent standards of record keeping throughout the Trust
- Ensure all clinical records comply with professional standards and those of accreditation bodies i.e. GMC, NMC
- Ensure that record keeping meet legal obligations
- Ensure that the Clinical Governance requirement for effective monitoring of clinical care and high quality record keeping are met
- Meet Information Governance Toolkit Standards
- Support evidence based clinical practice and improvements in clinical effectiveness
- Ensure that the requirements under the Research Governance Framework for effective monitoring of research related record keeping are met

Legal Obligation and Good Practice

5.4.4 Although the primary purpose of health records is to facilitate continuity of care and to act as a tool of communication, good records allow a clear picture of events to be obtained which is vital for legal or evidential reasons. Records must be objective and worthy of independent scrutiny – in the event of an investigation their content can be critical.

5.4.5 The approach to record keeping which courts of law adopt tends to be that 'if it is not recorded, it has not been done'

Documentation and Professional Accountability

5.4.6 All healthcare practitioners and staff involved in clinical care or undertaking research are professionally accountable for keeping clear, legible, accurate and contemporaneous clinical records which record all the relevant clinical findings, any decisions made, information given to patients and any drugs or other treatment prescribed.

5.4.7 All clinicians have both a professional and a legal duty of care to patients. All professional organisations will expect that high quality standards of care including record keeping are maintained. Record keeping standards are an indication of professional practice.

5.4.8 A health record should inform any clinician who has a responsibility for the patient of all the key features which might influence the treatment proposed. It should also provide a contemporaneous and clear record of the patient's treatment and related features. A good record speaks volumes about the care a patient has received, and has a vital role in minimising clinical risk.

5.4.9 Good record keeping safeguards both patients and professionals from unsafe practice through the inaccurate recording or misunderstanding of health record information.

5.4.10 For clinical records the purpose is to facilitate care, treatment and support of a patient or patient/service user. Therefore, these records should:
("be typed" means directly into an electronic system using the appropriate forms)

- Include demographic, clinical and social care information
- A record of assessment of risks and needs
- Evaluations of care and treatment
- Progress under CPA or other care plan arrangements
- Results of biochemical and other tests if any
- Prescription and administration of medication if any
- The recording of detention under the Mental Health Act 1983 as amended by the Mental Health Act 2007 if any
- Identify who has been responsible for which aspects of care and treatment
- Identify when care and treatment was given.

And also be:

- Be factual, consistent and accurate
- Where paper exists - be written in black ink, with the exception of pharmacy which will be in green for verification purposes.
- Be typed / written as soon as possible after the event has occurred, providing current information on the care and condition of the patient/service user (if the date and time differs from that of when the records are written up, this should be clearly noted under the signature, printed name and position/grade.
- Be typed / written clearly, legibly and in such a manner they cannot be erased (electronic records once saved cannot be erased) Where paper exists erasers, liquid paper, or any other correction fluids should not be used to cancel errors.
- A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment. In electronic records the above principle is applicable for use within the continuation sheets.
- Be accurately dated, timed and signed electronically in line with both Information Governance and ITT policies and procedures The use of abbreviations should be kept to a minimum
- Be typed / written, wherever possible, with the involvement of the patient/service user or carer and in terms that can be understood by all
- Be contemporaneous and continuous, with electronic records all documents saved will be in a time line effect.
- Documents must be inputted into the electronic system as soon as possible and saved. Printed documents and / or hand written documents must be scanned within a 24 hour period. (Weekends and bank holidays will be the exception)

5.4.11 Records must not contain:

- Information that is not relevant to the patient/service user to whom the record/s pertains
- Opinions that are not professionally based
- More than one copy of any document, although duplicate letters should be retained if they are date-stamped as being received by different people.

5.4.12 Good Record Keeping Ensures That:

- Staff can work with maximum efficiency without having to waste time searching for information
- Any record entry or alteration can be traced back to a named individual at a given date/time
- Those caring for the patient after you can see what has been done, and still needs to be done and the reasons for this
- Any decisions made can be justified or reconsidered at a later date if the situation changes

5.4.13 Relevant and Useful

- Identifying problems that have arisen and the action taken to rectify them and expected outcomes
- Providing evidence of the care planned, the decisions made, the care delivery and the information shared
- Providing evidence of actions agreed with the patient/service/user (including consent to treatment and/or consent to share information)

5.4.14 And Including

- Clinical observations: examinations, tests, diagnoses, prognoses, prescriptions, other treatments
- Relevant disclosures by the patient/service user (likely to understanding cause or effecting cure/treatment)
- Facts presented to the patient/service user
- Correspondence from the patient/patient/service user or other parties
- Patient/service user to write an account of their illness in their records, ensuring this is on a separate sheet of paper, their name is clearly identified as the author, it is dated and signed.

5.4.15 Patient/Service user Records Should Not Include

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subject statements
- Personal opinions regarding the patient/service user (restrict to professional judgements on clinical matters)
- The name(s) of third parties involved in a serious incident. The name should be included on the separate incident form for cross referencing
- Detailed correspondence generated from legal papers and complaints

5.4.16 Litigation and Complaints and Data Protection requests

5.4.16.1 Correspondence generated from patient/service user litigation and complaints must not, under any circumstances, be filed within the clinical records. These documents are not relevant to clinical care and are often restricted from disclosure, unlike the clinical record itself.

5.4.16.2 However, when a report is generated to assist in a legal case, this may be relevant to clinical decision making, or documents pertaining to the formal admission of patients under the Mental Health Act 1983, and may be filed within the clinical record.

5.4.17 Health Record Keeping Standards

5.4.17.1 The Trust audits against standards and requirements set by national, professional and accreditation bodies.

5.4.17.2 The Trust recognizes that there are two main areas in developing standards for clinical records and they are in generic and professional quality.

5.4.17.3 Generic quality is concerned with the basic content and structure of the record. Professional quality relates to the value of the record as an effective communication tool.

This above is a statement of good-practice principles, and is not intended as a comprehensive list of standards.

5.5 Record Creation/Registration/Architecture

5.5.1 This is the complete record of each individual patient/service user.

5.5.2 Records are created to ensure that all information is available within the Trust:

- To support the care process and continuity of care
- To support the day-to-day business, which underpins delivery of care
- To support evidence based practice
- To support sound administrative and managerial decision making
- To meet legal requirements, including requests from patient/service users and staff under the Data Protection Act 2018 and Access to Health Records (pertaining to deceased individuals only)
- To assist in health and other audits
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of media and the needs of future research
- Whenever and wherever there is a justified need for information, and in whatever media it is required

Registration

5.5.3 In order to ensure records can be identified and retrieved when required it is necessary to allocate a unique number via a registration system to records.

5.5.4 The types of records, which are most likely to be placed on a registration system, include:

- Clinical / Health and Social Care records
- Personnel records
- Financial records/papers
- Performance monitoring
- Policy papers (reports, correspondence, etc.)
- Minutes, circulated papers etc. of meetings
- Papers relating to the preparation of legislation
- Complaints papers and correspondence
- Research and development papers

5.5.5 All records created within Mental Health Mobius (South) Paris (North) Community Services (SystmOne), IAPT (IAPTUS), Health and Justice (Excelicare) and substance misuse (Theseus) are directly created within the electronic systems. Therefore the unique identifier is allocated automatically

5.5.6 The electronic records systems already have established agreed document structures. Any changes required to these structures would need to go to the relevant project boards for a decision.

5.6 Accessing Records/Security/Confidentiality

5.6.1 Access to and use of records containing person identifiable material is governed by the Data Protection Act 2018, the Access to Health Records Act 1990 and Caldicott Principles.

5.6.2 Confidentiality levels bind all Trust staff. Managers must therefore ensure that all staff are trained in data protection and are aware of the implications should confidentiality be breached. The impact of a breach of confidentiality could be any of the following:

- Threat to personal safety or privacy
- Embarrassment for the Trust
- Legal obligation
- Financial loss
- Disruption of activities

Staff do not have an automatic right to look at their own health records or those of colleagues, friends and family, they too must follow this procedure, failure to do so will be considered an Information Governance breach and may lead to disciplinary action.

5.6.3 The Trust is committed to multi-disciplinary working procedures and this requires all key professionals to work together and share information to the benefit of the patient/client. Patients/clients have an expectation that information held relating to them is confidential and held securely and will be available to facilitate and inform their care and to assure their safety and that no unauthorised person will be allowed deliberate or inadvertent access to the

confidential information contained in the unified health and social care record or subsidiary record.

Accessibility to Health and Social Care Records Process

Within the clinical capacity if the need to transfer clinical records between clinical environments is essential to the provision of appropriate care and treatment. The record must be transported as little as possible, but when it is necessary, it must be by the most secure means available. It is essential that the required Directorates have in place appropriate mechanisms and protocols to ensure the secure transfer of clinical records.

5.6.4 Records can be accessed 24 hours per day, 7 days per week, via the Trust's electronic patient records systems. HIE is available to staff to improve patient care and decision making by facilitating the safe sharing of patient records and vital information, which is both easily accessible and relevant. Reducing the time and removing challenges that can be faced by clinical staff when retrieving patient information. However if paper files do exist then the following applies:-

- 9.00am – 5.00pm, Monday to Friday –contact to be made with the epunft.essex.records@nhs.net to retrieve the relevant record from offsite storage providers
- Bank Holidays and Weekends – as above
- Electronic paper based records are available at the desk top 24-7. Authorised staff have access to the electronic system. Each ward and team has been given guest log in access if additional access is required both during hours and out of hours. For detailed instructions on electronic retrieval please refer to procedure CPG9(d)

5.6.5 Records stored offsite are retrieved on a daily basis and are delivered within 24 hours to a designated location.

- 9.00am– 5.00pm, Requests for records are sent to delegated records staff who liaise with the offsite storage provider. Records are returned to a designated location and then forwarded on to the original requester. All records are tracked both at the offsite storage provider and on the Trust's internal catalogue
- 5.00pm – 9.00am plus Bank Holidays and weekends, notes required urgently and in cases of extreme emergency, may be retrieved through the contact centre who will liaise with the designated out of hours staff. The Service level agreement with the offsite storage provider allows records to be delivered within a 2-4 hour time frame. All records are tracked both at the offsite storage provider and on the Trust's internal catalogue

Subject Access Requests – Clinical Records

5.6.6 Under the Data Protection Act 2018, the following individuals are entitled to have access to their clinical records (subject to some safeguards and exceptions), regardless of when the record was created, providing consent and required documentation is received:

- The patient/service user
- A person authorised in writing to make an application on the patient/ service user's behalf
- A person with parental responsibility when the patient/patient/service user is a child
- A person appointed by the court to manage the patient//service user's affairs because of incapability

5.6.7 Solicitors needing access to the records will need the consent of the patient / service user prior to any access being granted

5.6.8 There are some exceptions where records can be shared without patient/service user consent:

- The Mental Health Act Commission when patient/service users are detained under Mental Health Act 1983 as amended by the Mental Health Act 2007
- The General Medical Council - if a doctor is under investigation
- The police - if someone is at serious risk or a serious crime has been committed
- The courts - in criminal or other legal cases, when a court order is made
- Child Protection staff - where there is concern over a child's welfare and safety (even if the child is not under our care). Staff have a duty to volunteer information before it is asked for if they suspect a child is at risk.
- he DVLA - if a patient/service user's illness might make it unsafe for them to drive.

5.6.9 Under the Access to Health Records Act 1990, the following individuals are entitled to have access to the clinical records of deceased patients/service users:

- The personal representative of the deceased patient (e.g. the Executor of the Estate)
- Any person who may have a claim arising out of the patient's death

5.6.10 Patients/service users wishing to make subject access requests should be directed to the Trust's Records Manager using the following email address:- – epunft.accesstorecords@nhs.net

5.6.11 Under the terms of the same legislation, individuals also have a right to have their unified health and social care records amended if the records contain inaccuracies, misrepresentations or errors of fact. The Trust and its practitioners therefore have a duty to ensure that what is written in the unified health and social care record is accurate, to-the-point and as far as possible objective.

Subject Access Requests (Corporate Records)

5.6.12 Under the Data Protection Act 2018, members of staff are entitled to see their own personnel records. Staff wishing to request formal access to their records

should contact the Trust's Legal Department epunft.sar@nhs.net

Access to Corporate Records

5.6.13 The Freedom of Information Act (FOIA) 2000, which came into force in January 2005 was designed to ensure greater openness within the public sector, a commitment that is thoroughly supported by the Trust. The Act grants members of the public access to all types of recorded information that is held by the Trust.

5.6.14 The Trust has established efficient and effective procedures to ensure that requests for information under the terms of the FOIA are managed and actioned appropriately. Further information in relation to these procedures can be found within CP/ CPG25 – Freedom of Information 2000 Policy and Procedures.

5.6.15 Certain information may be exempt from disclosure, under one or more of the 23 exemptions. For example, the disclosure of personal or private information relating to an individual is forbidden under Section 40 – Personal Information.

5.6.16 Under the terms of the FOIA, the Trust has developed a publication scheme that is available via its website www.eput.nhs.uk. Any requests for information from the publication scheme must be forwarded to the Legal Team – epunft.foi@nhs.net

5.6.17 Any applications for information made under the FOIA, which have been received by staff must be forwarded immediately to the FOI team epunft.foi@nhs.net

5.7 Electronic Records Systems

The Trust is committed to reducing clinical risk to patient/service users by ensuring that their staff benefits from having as much information about them as possible prior to caring for them. To achieve this, the Trust has mandated the complete use of electronic systems for recording all patient/service user demographic, clinical and social care information.

5.7.1 From the point of a patient/service user's external referral being received, throughout the mental health and social care pathway to their discharge, all demographic, clinical and social care activity must be recorded on the electronic system.

5.7.2 The primary electronic system used by the Trust is Mobius (South) and Paris (North) for Mental Health, SystmOne for Community services, Theseus for substance misuse, Excelicare for Criminal Justice Team and IAPTUS for Therapy for You.

5.7.3 The use of information technology is increasing within the NHS generally and a large proportion of documents are now produced electronically. This change places new demands on the managing of records. For example, if an electronic document is to be produced as evidence in court cases it will only be accepted if assurances can be given that the Unified Electronic Patient Records System (UEPR) was not being misused and was operating properly at the time the record was produced.

Scanning/Access Control

5.7.4 For reasons of business efficiency, the Trust has undergone the transition of scanning archived health records into electronic records, which exist in paper form. All new patients/service users records are electronic from the point of contact with the Trust.

5.7.5 The UEPR will provide an authentication mechanism that controls access to its information and that validates each user attempting access at the start of each user session. Each user will enter a unique user-name and password in order to gain entry to the system.

Managing the Electronic Record

5.7.6 The Trust will monitor electronic records to ensure that:

- Records to be captured are being processed electronically if they do not appear in the paper record
- As far as possible, there is no duplication between the paper and electronic records
- A distinction is made between printed electronic records and those, which reside in the paper record
- An inventory is kept of all records that are scanned electronically

Standards for Electronic Records

5.7.7 The principles for electronic record keeping are the same as for paper records. In addition, when using electronic documentation, the Trust will ensure that the following procedures are in place, including:

- Physical/equipment security
- Access control
- User password management
- Computer virus control
- Data backup
- Computer network management
- Data and software exchange
- Validation
- Adequate training for all users

Security of Electronic Records

5.7.8 The Trust must implement and maintain an electronic records security program for office and storage areas. Any software or documentation required to maintain the functionality of the UEPR equipment must be located in a separate building. If records are stored on rewritable electronic media, the UEPR system must ensure that read/write privileges are controlled and that an audit trail of rewrites is maintained.

Maintenance of Electronic Records

5.7.9 The Trust should maintain all long-term and permanent backup and security

electronic recording media in a storage facility, either on-site or off-site, with the correct temperature and relative humidity controls (i.e. temperature below 70 degrees Fahrenheit, and humidity 30 to 40 percent).

5.7.10 The Trust should carry out an audit annually to read a statistical sample of all electronic media to identify any loss of information and to discover and correct the cause of data loss. The Trust should also consider the necessity to copy the media, after a specific agreed time period, and transfer onto tested and verified new media. This will ensure that enough 'memory core space' within the ERMS is available.

Legal Admissibility

5.7.11 All scanned records will be copied and stored in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BS 10008-2020). This provides good practice guidance on the electronic creation, storage and retrieval of information, duty of care, audit trails, and records management requirements for electronically stored information. Non-compliance could have a major impact on information being accepted in a court of law.

5.7.12 In order to ensure that this need is met, records should be stored on network drives and not on individual hard drives (C:\ or any folder beginning with 'My'). The policy on encryption of memory sticks must also be adhered to when using this media**.**

5.8 Retention and Destruction Retention

5.8.1 The Public Records Act 1958 imposes a statutory duty of care upon all individuals who have direct responsibility for any such records. The Trust follows the Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016. These are recommended minimum retention times from the Information Governance Alliance, although where there is a business need, records may be retained for longer periods. Where this is the case the decision must be justifiable.

Retention of Electronic Records

5.8.2 The retention criteria for electronic records are the same as for paper records. This retention criterion will include provisions for:

- Scheduling the retention and disposal of all electronic records, with the approval of the Trust Electronic Records Group and / or the Information Governance Steering Committee
- Establishing procedures for regular recopying, reformatting and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorised life cycle

5.8.3 Electronic records must be destroyed in accordance with the Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016. At a minimum the Trust should ensure that electronic records scheduled for destruction are disposed of in a manner that ensures protection of sensitive personal information.

Selection of Paper-Based Records for Permanent Preservation

5.8.4 All NHS records, whether paper-based or electronic, are public records under the terms of the Public Records Act 1958.

5.8.5 Prior to the decision to destroy any paper-based record, the Trust will give consideration to the value of the content to future generations and may take into account any genetic implications. Records which are thought to be worthy of permanent preservation, should be referred to the Trust Electronic Records Group and / or the Information Governance Steering Committee for review, whereby arrangements for their deposit in a place appointed under the Public Records Act 1958 will be made.

Disposal, Destruction and Destroying

5.8.6 Disposal is defined as the point in a records lifecycle when they are either transferred to an archive facility or prepared for destroying.

5.8.7 Destroying is defined as where the records are no longer required to be kept due to statutory requirement or administrative need and they have no long- term historical or research value.

5.8.8 Destruction is defined as the definitive obliteration of a record beyond any possible reconstruction.

In conjunction with this policy please also refer to Storage, Retention and Destruction procedure CPG9(c) Electronic Records Procedure CPG9(d) and Secure Handling and Disposal of Confidential Waste procedure RMPG13(d)

5.8.9 All Clinical records contain sensitive and confidential information. It is vital that confidentiality is safeguarded at every stage of disposal and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will mean disposal as confidential waste, in confidential waste bags provided throughout the Trust or by use of confidential 'waste bins'. It is important to remember that the destruction of records is an irreversible act. It is important to note that 'recycling' bins do not provide a safe destruction method.

5.8.10 The Trust uses contract services for the transporting and destruction of certain records, namely clinical records. The Contract terms must include guarantees on security and confidentiality of information. Enquiries regarding this should be addressed to the Records Manager in the first instance. A register of records destroyed should be kept, recording what was destroyed, when and by whom.

5.8.11 Managers must ensure that corporate records held within their areas of responsibility that are no longer required for business use are reviewed as soon as practicable under the criteria set out in Information Governance Alliance Guidance for records.

5.8.12 Only the Head of Electronic Systems & Records / Records Manager has the authority to action records for destruction. Individual staff members are only permitted to destroy individual paperwork which includes duplicate reports, version controlled / draft documents and letters. Please always check with your

line manager prior to any destruction.

5.8.13 In line with the policy for the destruction of records, patient/service users with an identified diagnosis of one of the following will not be destroyed and marked as such:

- Huntington's Chorea F022
- Creuzfeldt-Jakob's Disease F021
- Pick's Disease F020
- Parkinson's Disease F023
- Human Immunodeficiency Virus F024

Specific Clinical Records Destruction

5.8.14 Please refer to storage, Retention and Destruction procedure CPG9(c) and Electronic Records procedure CPG9(d) for further guidance.

Destruction Process

5.8.15 All records are reviewed in accordance with both the Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016 or Trust procedure CPG9(c) Storage, Retention and Destruction of Records Procedure.

5.8.16 Individual departments all have the facility for local blue bin destruction which is then periodically collected and shredded with approved contractors.

5.8.17 The destruction of clinical/health records only takes place via the scanning department in conjunction with the Trust's Head of Electronic Systems/Records, once process as outlined in CPG9(d) Electronic Records Procedure has been followed. The Information Governance Steering Sub Committee has given prior authority for these records to be destroyed.

5.8.19 Specific destruction requests are made with the approved contractors for bulk destruction.

5.8.20 In all cases destruction certificates are obtained.

5.8.21 For records stored in offsite storage facilities (corporate only) a concise catalogue is kept with retention dates, these are looked at periodically. Any box numbers identified that require destruction are returned to the originating department for approval. Once this approval is received the Trust's Head of Electronic Systems/Records will instruct the offsite storage provider. Checks are made against each of the box numbers and once satisfied authorisation is given from the Trust to destroy. A destruction certificate is then obtained.

5.9 Storage

5.9.1 The Trust has a responsibility for ensuring the effective and efficient operation of all storage facilities within the organisation. This includes the safekeeping, accessibility and retention of records for as long as required, the transfer of those records selected for permanent preservation, and the timely destruction

of records no longer required.

5.9.2 All storage facilities should be in a suitable environment, which has easy access and appropriate safety to ensure the records are not damaged or destroyed.

Transportation

Please refer to the Trust's Transfer Transportation procedure CPG9f

Emergency request for records

5.9.3 There will be the need from time to time to request records in an emergency situation (unplanned admission, no records at outpatient clinics, serious incidents) and records will need to be transported accordingly and securely.

5.9.4 All emergency records requests will still need to be tracked using the methods as described in this policy.

5.9.5 Approved carrier methods can be used i.e. couriers, internal postal collections, external approved taxis, providing the records have been secured in the first instance.

5.9.6 Any request from third parties including Police, Solicitors and Courts should initially be on an original request form and after authorisation from the on call director out of hours or the Access to Records Team during normal office hours, copies only of the records can be shared. Under no circumstances can the original record be given out.

5.9.7 Records required for serious incidents will in the first instance be photocopied and scanned and then sent and secured within the health records departments and before any further action can be taken or shared.

5.10 Sharing and Disclosing Information

5.10.1 The Trust will ensure appropriate agreements are put in place to govern the sharing of identifiable information between organisations. Such sharing must be in line with the care of the patient and the rights of staff in accordance with the Data Protection Act 2018.

5.10.2 Where information is requested in line with the Freedom of Information Act 2000, it will be managed in accordance with the Freedom of Information 2000 policy and procedures.

5.10.3 Where information is requested in line with the Data Protection Act 2018 it will be dealt with in accordance with their statutory right under the 'subject access' regime.

5.10.4 Requests for an individual's health information will be dealt with in accordance with the Data Protection and Confidentiality policy and procedures.

6.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE

6.1 The Director of ITT is responsible for monitoring the implementation and effectiveness of this policy and related procedural guidelines.

6.2 Monitoring of the availability of Clinical Records will be undertaken by the Trust's Records Manager and any missing records will be reported to the Information Governance Steering Sub Committee in the format of a report for action to be agreed.

6.3 The quality of all written and electronic Clinical Records will be audited and co-ordinated by the Clinical Audit Department.

6.4 Audits will be undertaken using the Trust agreed audit tools

6.5 Results of all audits and monitoring will be presented to Quality & Safety meetings

6.6 All audit reports will contain the background information on what was audited and why, outcome data for each element of the audit tool and recommendations and action plans for improvements.

6.7 The Workforce, Development and Training Department will undertake monitoring of Training via OLM

7.0 POLICY REFERENCES / ASSOCIATED DOCUMENTATION

7.1 The Trust is bound by a number of legislations governing an individual's rights, access to information, and the safeguarding of personal information concerning its patients and staff from unauthorised access and disclosure.

Legislation

- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 1992
- Human Rights Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Computer Misuse Act 1990
- Access to Health Records Act 1990
- Copyright Designs and Patents Act 1988
- Children's Act 1998
- Public Records Act 1958
- NHS and Community care Act 1990
- Mental Health Act 1983 (revised 2007)
- Carers (Recognition & Service) Act 1995
- Patient/service users Access to Records Act 1987 and Regulations
- Adoption Act 1976
- Health Act 1999 (Section 31)

- Health and Social Care Act 2001
- Caldicott Review 2013
- BS10008 Legal Admissibility
- General Data Protection Regulations (GDPR)

7.2 BS10008 is the British Standard that outlines best practice for the implementation and operation of electronic information management systems, including the storage and transfer of information. It is designed to help verify and authenticate all information to avoid the legal pitfalls of information storage. BS10008 outlines best practice for transferring electronic information between systems and migrating paper records to digital files. It also gives guidance for managing the availability and accessibility of any records that could be required as legal evidence.

8.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES

Please read in conjunction with the following Trust's policies, procedures and relevant legislation and guidance:

- Access to Records Procedure
- Freedom of Information Policy
- Data Protection & Confidentiality Policy
- IM&T Security Policy
- Transportation policy

END