Mersey Care NHS
NHS Foundation Trust

TRUST-WIDE SERVCE BASED POLICY DOCUMENT

Health Records Policy and Procedures

Policy Number:	IT06
Scope of this Document:	All Staff
Recommending Committee:	Health Records Sub-Committee
Approving Committee:	Executive Committee
Date Ratified:	November 2016
Next Review Date (by):	December 2018
Version Number:	2016 – version 1.4
Lead Executive Director:	Executive Director of Finance
Lead Author(s):	Information Governance Officer/Trust Health Records Manager

TRUST-WIDE SERVCE BASED POLICY

2016 – Version 1.4

Quality, recovery and wellbeing at the heart of everything we do

TRUST-WIDE SERVICE BASED POLICY

Health Records Policy and Procedures

Further information about this document:

Document name	**Health Records Policy and Procedure**
Document summary	This Policy is issued as a framework to support Information Governance. This document is presented in a standard structure and format. It will be made available in appropriate, alternative languages and formats on request. (IT06)
Author(s) Contact(s) for further information about this document	**Gina Kelly** **Information Governance Officer/Trust Health Records Manager** **Telephone: 0151 471 2351** **Email: gina.kelly@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **V7 Building,** **Kings Business Park** **Prescot** **Liverpool** **L34 1PJ** **Your Space Extranet:** **http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IT02** IM&T Security Policy **IT10** Confidentiality and Information Sharing Policy **IT11** **IT14** Data Protection Act Policy
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Version 1.4	Approved by Health Records sub-Committee	September 2016

SUPPORTING STATEMENTS – this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

CONTENTS Page

1. EXECUTIVE SUMMARY

1.1 This policy defines a structure to ensure adequate Health Records are maintained and that all aspects of Health Records, in any format or media type, from their creation all the way through their life cycle to their eventual disposal, are controlled effectively to comply with legal, operational and information needs. For the purposes of this policy the Health Record is the legal document relating to an individual service user regardless of the format this is available in, e.g. - paper, Epex, PACIS, Carenotes, microfiche or WinDIP.

1.2 Implementation of and adherence to this policy will ensure:-

- Health Records are available and can be accessed when needed
- Health Records are concise and unambiguous
- Health Records can be trusted
- Health Records can be maintained through time
- Health Records are secure
- Health Records are retained and disposed of appropriately
- Staff are trained and aware of their responsibilities for record-keeping and record management

1.3 This policy is applicable to all staff working for, or with, Mersey Care NHS Foundation Trust (the trust) who records, handles, stores or otherwise comes across service user information.

1.4 This policy has replaced previous trust policies:- IT07 policy, Retention, destruction of Health Records; IT08 policy, Safeguarding Health Records; IT09 policy, Filing within Health Records.

1.5 This policy should be read in conjunction with:-

- Guidance on Record Keeping standards from Health Care Professionals relevant professional body, e.g. Nursing and Midwifery Council (NMC)
- IT02 policy – IM&T Security
- IT10 policy – Confidentiality and Data Sharing
- IT11 policy - Data Quality
- IT14 policy – Data Protection Act
- SD21 policy - Care Programme Approach
- HR32 policy - Gender Realignment Support Policy
- Guidance and training information on relevant Clinical Information systems packages, e.g. Epex, PACIS, WinDip

2. INTRODUCTION

2.1 Rationale

2.1.1 In the context of this policy, a Health Record is anything which contains information in direct relation to the clinical history, diagnosis, treatment or review of a service user which has been created or gathered as a result of the work of NHS employees:-

- Service user Health Records (electronic or paper based)
- Microfiche, scanned or digitalised Health Records
- Audio and videotapes, cassettes, photographs

2.1.2 Accurate and effective record keeping is fundamental to high quality patient care and enables effective communication with other professionals involved in a service user's care, thereby contributing to the reduction of risk. In addition accurate and effective record keeping is essential for the organisation to comply with the multiple statutory dataset reporting.

2.1.3 The content of the Health Record is strictly confidential and should be used in accordance with this policy. The Health Record is a legal document and it is therefore imperative that good practice is followed at all times.

2.2 Scope

2.2.1 All staff, including those staff who are seconded Social Care staff, or staff who are part of Informatics Merseyside, are responsible for any records which they create or use. It is the responsibility of **all** staff involved in handling/usage of Health Records to comply with this policy.

2.2.2 Everyone working for or with the NHS who records, handles, stores or otherwise comes across service user information has a personal common law duty of confidence to service users/patients and to his/her employer. The duty of confidence continues even after the death of the service user, or after an employee, or contractor, has left the NHS.

2.2.3 The responsibility for the safeguarding of the Health Record and the information contained within the Health Record rests with the individual/individuals involved in the handling of the Health Record.

2.2.4 Personal information (e.g. about a service user) processed/kept for any purpose should not be kept for longer than is necessary for that purpose *see Section 11* – ***Retention/Destruction of Health Records***. Service user information may not be passed on to others without the service user's consent except as permitted under Schedule 2 and 3 of the Data Protection Act 1998 or, where applicable, under the common

law where there is an overriding public interest. Further guidance on safeguarding service user information can be found within the NHS Code of Confidentiality and the Trust's Confidentiality Policy (IT10) available via the trust website:
www.merseycare.nhs.uk/Who_we_are/Policies_and_Procedures/IT10

2.3 Legal Obligations

2.3.1 The trust must comply with, but not limited to, the following legislation and guidelines:

2.3.2 **Records Management Code of Practice for Health and Social Care (2016)** This document was published by the Information Governance Alliance for the Department of Health in Summer 2016 and replaces **Records Management: NHS Code of Practice Part 1 & 2 (2006, 2009).** It is a guide to the required standards of practice in the management of records. It is based on current legal requirements and professional best practice. Appendix 3 sets out the minimum periods for which the various records created within the NHS should be retained. It provides information and advice about all records commonly found within NHS organisations.

2.3.3 **Public Records Act 1958/1967** places responsibility for the management of public records on (government) departments. The records management department advises other government departments on good record keeping and promotes the effective and efficient management of records across government.

2.3.4 **Guide to Confidentiality in Health & Social Care 2013** published by the Health & Social Care Information Centre as a guide to good practice to enable staff to use their professional judgement confidently in the best interests of individuals.

2.3.5 **Code of Practice on Confidential Information 2014** published by the Health & Social Care Information Centre as a guide to good practice for organisations collecting, analysing,publishing or otherwise disseminating confidential information.

2.3.6 **Data Protection Act 1998** controls how personal information is being used by organisations, businesses or the government. Everyone who is responsible for using data has to follow the data protection principles *(please refer to policy IT14 for further information).* Thus, with the exception of anonymised information, most if not all NHS information concerning service users, whether held electronically or on paper, will fall within the scope of the 'Act'.

2.3.7 **Access to Health Records Act 1990** - guidance issued by the Department of Health - outlines the rights of access to deceased patient health records by specified persons.

2.3.8 **Access to Medical Reports Act 1988** - guidance issued by the Department of Health - outlines the right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes.

2.3.9 **NHS Litigation Authority Risk Management Standards** - a special health authority that handles negligence claims made against NHS organisations and work to improve risk management practices in the NHS.

2.3.10 **Information Governance Standards** outline the way organisations "process" or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records. The standards provide a way for employees to deal consistently with the many different rules about how information in handled.

2.3.11 **Freedom of Information Act 2000** provides public access to recorded information held by public authorities. Recorded information includes printed documents, computer files, letters, emails, photographs and sound or video recordings.

2.3.12 **Nursing and Midwifery Council (2009) Record Keeping: Guidance for Nurses and Midwives** explains what they expect from nurses and midwives in relation to good record keeping.

2.3.13 **Academy of Medical Royal Colleges: Standards for the Clinical Structure and Content of Patient Records (2013)** describes standards for the structure and content of health records, contain a list of clinical record headings and a description of the information that should be recorded under each heading.

2.4 Principles

2.4.1 It is the responsibility of all Senior Managers/Clinical Staff within the trust to ensure that staff within their remit who have any involvement with Health Records are made aware of, and fully understand, the content of the Health Records Policy. From July 2008 the responsibility for Record keeping has been incorporated into relevant staffs Contracts of Employment and included within Job Descriptions.

2.4.2 This policy is intended to be a comprehensive guide to all staff involved in handling service users Health Records in electronic or manual media.

2.4.3 Should you have any queries regarding a particular issue, or anything not documented within this policy, please contact the Health Records Manager for the Trust.

3. POLICY

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

3.2 To ensure quality, continuity of operational services and to meet with the statutory legislation within the Data Protection Act, all records should be accurate and up to date. The trust expects that entries into service user's Health Records are made at the same time as the events you are recording or as soon as possible afterwards – *see Section 4.1 Record Keeping*.

3.3 Minimum Standards for Health Records

The trust is undergoing changes to the Clinical Information Systems used within the organisation. It is acknowledged that the changes across all areas will take some time. In the interim, we are seeking to attain the minimum NHS Litigation Authority (NHSLA) and Information Governance recommended standards in respect of Health Records.

3.4 Audit

An annual audit (**Appendix 1**) is undertaken to ensure compliance with the NHSLA and Information Governance standards on record-keeping. The formal report of the annual Health Records audit is reviewed by the Health Records Committee, the Minutes of which are reported to the Executive Committee who monitor progress against the action plan.

3.5 Care Programme Approach (CPA)

3.3.1 The trust is obliged to ensure that information in respect of service users receiving secondary care services is captured, recorded and monitored irrespective of whether service users are on new CPA or not. CPA documentation is available within electronic Health Records. This information is also required for such purposes as the Mental Health Services Dataset.

3.3.2 It is important for all staff to be aware that whether information is recorded electronically or manually it must comply with the trust standards in respect of Record Keeping. All assessments/web forms related to CPA documentation should be on the clinical information system within 3 working days.

4. PROCEDURES

4.1 RECORD KEEPING

Divisions (Divisions) specific procedures should be developed to ensure data quality for electronic and any manual records. These procedures should be circulated to all staff involved in recording the information. Procedures should be regularly reviewed and updated in conjunction with the Trust's Health Records Manager and also contain the implementation date and author. See **Appendix 2** for specific procedures.

4.1.1 Basic Standards for Record-Keeping

The purpose of a clinical record is to facilitate the delivery of care, management of treatment and support of an individual service user. The following standards are a minimum requirement expected within the trust:-

a) Service User Health Records should:

- Be factual, consistent and accurate
- Be input/scanned (if electronic Health Record)/ written (if manual Health Record) as soon as is practicably possible after an event has occurred, providing current information on the care and condition of the service user - **if the date and time differs from that of when the records are written up, this should be clearly noted in the record** – *NB audit trails are performed on electronic entries made into Health Records*
- Be written legibly, concisely and in such a manner they cannot be misinterpreted
- Be accurately dated, timed and signed with the name and position/grade written alongside the first entry
- The use of abbreviations should be kept to a minimum
- Be written, wherever possible, with the involvement of the service user and carer and in terms that the service user or carer will be able to understand
- **For those few areas where it is still required to use manual Health Records *(further guidance issued to new junior doctors at their induction is attached to this policy) Guidance A***
- Entries should be written in black ink and include the service users name, date of birth, health record number, NHS number, the date and venue of consultation, the names and designation of those healthcare professionals present and the entry should be signed and dated with name and designation printed legibly
- Be consecutive
- Erasers, liquid paper, or any other obliterating agents 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.

- Be bound and stored so that loss of documentation is minimised.
- For guidance on "missing" health records please see **Appendix 3**.

b) Be relevant and useful

- Identifying problems that have arisen and the action taken to rectify them
- Providing evidence of the care planned, the decisions made, the care delivered and the information shared
- Providing evidence of actions discussed with the service user (including, but not limited to, consent to treatment and/or consent to share)

c) And include

- Clinical observations: examinations, tests, diagnoses, prognoses, prescriptions, other treatments
- Relevant disclosures by the service user – pertinent to understanding cause or effecting cure/treatment.
- Facts presented to the service user.
- Correspondence from the service user or other parties.

d) Contemporaneous notes

Information recorded about the service user should be written at the time of the event, or as soon afterwards that is practicably possible, to provide a chronological and accurate record of events. This is vitally important as it captures the reality of the events within which the service user's care was delivered and can be used in any legal proceedings. It is important that healthcare professionals ensure that contemporaneous notes are made at the time of the service user's consultation and reflect the care given or omitted and the rationale for these decisions.

NB – *completion of all assessments/web forms, e.g. CPA and HoNOS documentation must be on the clinical information system within 3 working days.*

e) Copying and Pasting Information

- Staff should avoid cutting and pasting sections of information within one part of the electronic health record to another part of the health record
- External emails – record receiving an email, who this is from (include organisation and job title) and the date it was received then document relevant clinical information within

quotations, eg “ultrasound of the kidneys showed degenerative changes”

- Internal emails – do not copy and paste any part of an internal email without first gaining the consent of the sender; information copied should be relevant clinical information only relating to the health and wellbeing of the service user.

f) Service User Health Records should not include

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subject statements
- Personal opinions regarding the service user (restrict to professional judgements on clinical matters)
- The name(s) of third parties involved in a serious incident, however initials only could be used. The name should be included on a separate incident form for cross referencing
- Entries written in the style of text language, e.g. “l8r”
- Correspondence generated from legal papers and complaints.

4.1.2 Filing of legal papers and complaints

Correspondence generated from legal cases and complaints must not, under any circumstances, be filed within the clinical record. These papers are not relevant to clinical care and are often non-disclosable, unlike the clinical record. However, when a report is generated to assist in a legal case, this may be relevant to clinical decision making and this report should be filed within the clinical record.

4.2 RECORD CREATION

4.2.1 Complete and well structured Health Records enable Health and Social Care staff to access relevant information contained in the Health Record quickly as recommended in “Setting the Record Straight” Audit Commission 1995. In addition well structured records assist the trust meet its legal obligations under the Data Protection Act 1998 in respect of Subject Access rights for individuals.

4.2.2 Health Records are created to ensure that information is available within the trust:-

- To support the care process and continuity of care
- To support 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 service users under the Data Protection Act 1998 – Subject Access legislation
- To assist clinical 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 material and the needs of future research
- Whenever and wherever there is a justified need for information, and in whatever media it is required

4.3 REGISTRATION

4.3.1 Registration of a service user within the trust is made by the collection of service user data which is maintained within an index system. Registration of service users at the trust is made by designated authorised staff who have been trained in Registration functionality on the electronic Clinical Information Systems and assessed by the clinical trainers to ensure they are competent before being allowed access to the "live" systems.

4.3.2 The *NHS Number* is the only national unique patient identifier in operation in the NHS. The trust must ensure that service user records, both paper and electronic, have an NHS Number stored on them as early as possible in the episode of care. Staff should be routinely using the NHS Number as part of the provision of care, to link the service user to their care record, to communicate within and between organisations and ensure service user awareness of the NHS Number.

4.3.3 Each service user is allocated at registration the trust's unique identifier which is numerical – which could have an alphabetical prefix.

4.3.4 The registration details or index of service users within the trust are currently held by means of electronic Clinical Information Systems. The allocation of the trust's unique identifier enables Health Records to be identified and retrieved efficiently.

4.3.5 Authorised staff will be given access to computer systems via the application of a User Identifier. Individual staff must be responsible for the security and maintenance of their own individual password. Audit trails can then be performed on data access within the system. The registration process entails keying into the electronic Clinical Information Systems minimum demographic details e.g. the service user's name, date of birth or NHS number if known to establish whether the service user has previously been in contact with any of the trust Services or not. Upon receipt of a referral, if the NHS number is not readily available staff are expected to check against the National Summary Care Record for the NHS number for clarification of the individual's information. Authorised trust staff are trained and granted authorised access to the National Summary Care Record in order to trace and obtain missing NHS Numbers. Additional functionalities are available to assist checks at the registration stage e.g. soundex or the ability to search under a date of birth.

4.3.6 If the service user has previously attended the trust, then the unique identification previously allocated must be used to record the new contact – ensuring that all demographic details are checked. Where manual records are still in use a new front registration form is printed from the electronic Clinical Information Systems, which has been updated, and filed at the front of the existing records.

4.3.7 If the service user has **NOT** had any previous contact with the trust then **ALL** the demographic fields, as appropriate, must be completed on the Clinical Information Systems by the authorised staff. The system will automatically generate a unique registration number for that service user. Detailed procedure notes are provided in **Appendix 4**.

4.3.8 With the development of electronic Health Records, there will be a need to identify every item to be stored within the Health Record, which is service user related, with the relevant NHS number to provide the necessary links through all electronic records.

4.4 AVOIDING THE RISK OF DUPLICATION OF CLINICAL RECORDS

4.4.1 It is of paramount importance that duplicate records are not created as this poses a risk to the Service User. There are some instances where Service Users may give false names and addresses and these may be difficult to detect. It is therefore essential that all Service Users are asked at the initial point of contact whether they have ever received treatment within any of Mersey Care NHS Foundation Trust services (it is important to be specific and name the areas to avoid confusion). A thorough check of the Registration systems should be made. Further checks may be made against the Summary Care Record to ensure the correct match.

4.4.2 Upon identification of a duplicate or incorrectly merged records then the procedure for the management of duplications or incorrectly merged records must be adhered to. See **Appendix 5.**

4.5 RETRIEVAL OF RECORDS

4.5.1 Requests for retrieval of records should be made to designated areas within each Division as set out in **Appendix 6**. Specific staff based within the Divisions have been trained in the processes involved in retrieving Health Records. *See Section 8 for further information.*

4.5.2 Retrieving Health Records from another Division

If a member of staff from one Division or Service requires information contained on WinDip from another Division or Service, permission must be sought from the hosting Divisional management team prior to information being released.

4.5.3 Reprinting

In some instances a reprint may be required of information held on electronic Clinical Information Systems - if reprinting is conducted reprints must be made on yellow paper, to indicate that the information is already held electronically. If reprints have been produced and the information is no longer required then the copies must be securely disposed of adhering to the local arrangements, e.g. “Shred-It” confidential bins. Any Division/Service that reprints documentation to be given to another Division/Service should follow the guidance in sections 7 and 9 of this policy.

5. SCANNING OF DOCUMENTATION INTO ELECTRONIC HEALTH RECORDS

5.1 Any document, relevant to the care and treatment of a service user, that would previously have been filed into a manual Health Record should be put into the electronic Health Record using locally based scanners. Please refer to relevant guidance prior to scanning, e.g. Epex.

5.2 Staff who have the responsibility for scanning documentation onto clinical systems must ensure they do this as soon as is practicably possible in a timely manner so that this information is readily accessible.

5.3 Any documentation scanned into the electronic Health Record held on WinDip, should contain the unique identifier which must be cross referenced with electronic Clinical Information System e.g. Epex/PACIS.

6 COUNTERSIGNING

6.1 When a practitioner signs a care record, they are signing to confirm that it is an accurate account of any communication, planning, intervention or outcomes related to the care of an individual service user.

6.2 This requirement includes Assistant Practitioners, Health Care Assistants who have completed an NVQ or equivalent, OT assistants, Psychology Assistants, trainee psychologists and any non-professionally affiliated practitioners deemed competent by their supervisor. All entries must adhere to the required standards described within this policy.

6.3 The supervisor must be satisfied that the person to whom any task is delegated is competent to carry out the intervention or procedure *and* the recording of it. Supervision sessions should be a forum to discuss these competencies and duties.

6.4 All student Nurses **must** have their entries countersigned by a qualified practitioner.

6.5 For further guidance please see **Appendix 7**

7 STORAGE OF HEALTH RECORDS

7.1 Equipment and systems should ensure that the risk of loss or damage of documentation is minimised.

7.2 Storing Non-Paper Records

7.2.1. Microfiche Health Records are held across different sites within the Trust. This is a widely recognised system for storing archived material. Documents stored on microfiche are available and can be accessed or reprinted as necessary. For further information please contact the Trust Health Records Manager.

7.2.2. Photograph and film collections Assembled by medical and other staff through their work within the Trust, should be regarded as Public Records and subject to these guidelines.

Note that the provisions of the Data Protection Act 1998 on registration of records and restriction of disclosure, relate to photographs of identifiable individuals as well as to other personal records.

Film should be stored in dust-free metal cans and placed horizontally on metal shelves. Microform, sound recordings and video-tape should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

7.2.3 Compact Discs that contain digitalised service user Health Records must be held in secure fireproof locked boxes. Backup copies of the discs should be retained in a fireproof safe at a different location from the service. Discs must not be removed from the department where they are stored and access will only be made to authorised staff involved with the service user. Data from the discs must not be downloaded onto any of the trusts computer hard or shared drives. Print-off's of service user information should only be made to assist with continuity of service user care or to enable the trust to comply with the legislative framework. Copies of individual service user's records may only be permitted to assist with continuity of service user care or to enable the trust to comply with the legislative framework.

8 Safeguarding the Health Records and the Information it contains against Loss, Damage or use by unauthorised persons

8.1 The confidential nature of Health Records cannot be overstressed and must always be borne in mind by those who have to handle such records. Authorised staff will be given access to computer systems via the application of a User Identifier. Individual staff must be responsible for the security and maintenance of their own individual password. Audit trails can then be performed on data access within the system.

8.2 Health Records must not be left in a position where service users, or unauthorised persons can obtain access to them, whether they are on computer screens or any other format e.g in hard copy. It is also essential that the individuals involved in handling the Health Records are responsible for ensuring that the Health Record is safeguarded against loss, damage or use by unauthorised persons.

8.3 Health Records must be tracked out by means of the manual tracer card / electronic tracking systems. This must include the date health records have been taken/sent somewhere and the destination.

8.4 Information contained within the Health Record must not be revealed to any unauthorised persons.

8.5 Upon an incident occurring in relation to loss, damage or unauthorised access an adverse incident form must be completed and a formal investigation launched into the incident.

8.6 The incident must be reported immediately to the relevant line Manager and the Health Records Manager should be advised of the incident. The line Manager should also advise the Information Governance Manager and Risk Management Department of the incident.

8.7 The trust Health & Social Care original records should not be sent off Trust premises e.g. to other NHS or associated organisations. If a request has been received from another NHS organisation for the Health Records then a copy (printed or photocopied) of the original records should be made and sent *see section 9*.

9 HEALTH RECORDS IN TRANSIT

9.1 When choosing options staff should consider the following:-

- Will the records be protected from damage, unauthorised access or theft?
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?

- Does the mail provider offer 'track and trace' options and is a signature required upon delivery?
- Have I used the correct envelope/packaging?

9.2 Postal options must be considered if Health Records are to be sent in external mail e.g. Signed for First Class, Special Delivery

- **Signed for First Class** has replaced Recorded Delivery and is for a letter or parcel that is to be signed for by the person that is receiving it. If an item is for Signed for First Class this should be marked on the envelope and taken to the post office to enable the relevant documentation to be completed.

- **Special Delivery** has replaced Registered Delivery and is the recommended method of posting copy Health Records. It is signed for as with Signed for First Class and there is a 9am delivery (which is more expensive) or a Next Day Delivery (this is the more popular of the two). Items sent Special Delivery can be insured.

9.2.1 With Special Delivery there is a Track and Trace service which can be accessed by using the internet or telephone. This will advise you of the various stages the letter/package has been signed for and at what time.

9.2.2 Consideration needs to be given to the volume of copy Health Records as it may be more appropriate to use an approved secure Courier Service, eg DHL, UPS

9.3 Care should be taken when addressing envelopes/packages containing Personal Identifiable Information. The envelope should be clearly marked "Private and Confidential – Addressee only" with the address written in full, cross referencing the details with the relevant correspondence to ensure the accuracy of the address. It is recommended that staff use "double wrapping" for added security of the information being posted.

9.4 If the decision has been made to send Personal Identifiable Information external to the organisation via electronic mail it is imperative that staff have a robust system in place to ensure that the recipient's email address is confirmed as accurate. Staff should then only send Personal Identifiable Information via secure encrypted email. ***Please refer to IM&T policy IT02, SS03 Internet and Email Security Standard before sending an encrypted email.***

10 RETENTION/DESTRUCTION OF HEALTH RECORDS

10.1 The NHS Retention/Disposal Schedule **MUST** be adhered to in relation to all Health Records and is set out in **Appendix 8**. The trust employs Social Care staff and therefore create Health and Social Care

Records. The Trust has adopted the statutory retention periods for Mental Health Records as detailed in the Information Governance Alliance Records Management Code of Practice for Health and Social Care as this has been established to be the longer statutory record retention period.

10.2 The Destruction of Health Records is an irreversible act, however the cost of keeping health records can be high. The trust has adopted the Retention/Destruction schedule detailed in the Information Governance Alliance Records Management Code of Practice for Health and Social Care.

10.3 Retention periods reflect minimum requirements of clinical need. Personal Health Records may be required as evidence in legal actions; the minimum retention periods take account of this requirement. Before any destruction takes place, ensure that:-

- There is consultation with the Trust's Health Records Manager and Caldicott Guardian and an agreement is reached with both the Health Records sub-Committee and Information Governance & Caldicott Committee and any course of action must be clearly minuted.
- Any other local clinical need must be considered, and
- The value of the records for long-term research purposes has been assessed, in consultation with an appropriate place of deposit.

10.4 Definition of disposal and destruction (applied to health records)

Disposal may include one or more of the following: the transfer of selected records to an archive facility; transfer from one application to another, paper to scanned electronic record.

Destruction is the process of eliminating or deleting records beyond any possible reconstruction.

10.5 Once a Health Record has been identified for destruction this should then be disposed of in accordance with guidance documented in the the Information Governance Alliance Records Management Code of Practice for Health and Social Care. Miniaturised or electronic collections are subject to the same NHS Retention/Disposal legislative requirements as hard-copy Health Records. This may involve a variety of approved options which range from transfer of documentation to the Depository at the Public Records Office, shredding, pulping or incineration. If an outside agency is contracted to undertake the disposal of records then it is vital that a data processor contract is established which sets out the parameters of the outside agency's work as the data controller retains full responsibility for the actions of the data processor.

10.6 Therefore the contract must require the data processor to comply with obligations equivalent to those imposed on the data controller by the Seventh Principle of the Data Protection Act 1998. The contractor must

produce written certification of confidential destruction. It is vital however, to ensure that confidentiality is maintained at every stage whichever method is selected.

10.7 Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will involve shredding, pulping or incineration. When Health Records are destroyed a record should be kept of the service user's name, a description of the Record, the date the Record was destroyed. Specific details of the NHS Retention/Disposal Schedule are documented in *Appendix 8*.

10.8 Each Division **MUST** identify designated staff who will be responsible for keeping a record of all checking, retention and a log itemising each record selected for destruction **MUST** be maintained electronically *see Appendix 3.*

10.9 Marking Health Records for Permanent Preservation

In exceptional circumstances Health Records may require permanent preservation – the clinician who is seeking this course of action should gain approval for permanent preservation from the Caldicott Guardian.

10.10 If the Caldicott Guardian is in agreement the clinician must document clearly the reason for permanent preservation within the Health Record.

11 TRAINING

11.1 Training in respect of good Record Keeping and standards to adhere to are included as part of the trust Corporate Essential Mandatory e-learning platform. The Information Governance Toolkit has e-learning training materials with mandatory modules around confidentiality and additional modules specific to job roles. In addition bespoke sessions on "Recording Information" (half day workshops) are offered to staff across the trust. The training requirements for the Health Records Policy & Procedures can be found in the Corporate Training Needs Analysis which is an appendage to the trust's Learning & Development Policy **HR28**.

12 DUTIES & RESPONSIBILITES

Chief Executive

The Chief Executive has overall responsibility for records management within the Trust. As the accountable officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to

support service delivery and continuity. Record management is key to this as it will ensure appropriate and accurate information is available as required.

Caldicott Guardian
The Trust's Caldicott Guardian, who is the Medical Director, has a particular responsibility for reflecting service user's interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is only shared in an appropriate and secure manner.

Head of Information Governance / Information Governance & Caldicott Committee
The Head of Information Governance is responsible for ensuring that the trust is working within the legal framework of the Data Protection Act, Freedom of Information Act, the Information Governance Alliance Records Management Code of Practice for Health and Social Care, NHS Code of Practice for Confidentiality, Information Governance Toolkit Standards. The Information Governance & Caldicott Committee ensures the trust operates within the Information Governance framework and monitors compliance with this policy.

Senior Information Risk Owner (SIRO)
The SIRO is the Executive Director for Finance/Deputy Chief Executive who is responsible the organisation's Information Risk Policy and acts as advocate for information risk on the Board.

Information Asset Owner
Information Asset Owners are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.

Health Records Manager (Trust)
It is the responsibility of the Health Records Manager to ensure that this policy is implemented and that the records management system and robust data quality processes are developed, co-ordinated and monitored. The Health Records Manager is the recognised professional lead within the trust to advise staff on records management issues.

Chief Clinical Information Officer
The role of the Chief Clinical Information Officer (CCIO) is required to support the strategic aims of the Trust taking particular responsibility for ensuring clinical adoption and engagement in use of technology, driving continuous clinical process improvement focused on patient outcomes and efficiency and developing clinical information that supports and enhances organisation reform.

Information Governance Committee

The Information Governance Committee ensures the Trust operates within the Information Governance framework and reports to the Executive Committee.

Health Records Sub-Committee
The Health Records Sub-Committee is comprised of multi-disciplinary staff from services provided within the trust involved in promoting a high standard of Records Management to assist with the diagnosis/treatment and continuity of service user care. The Sub-Committee meets on a quarterly basis and minutes from the Health Records Sub-Committee will be tabled and reviewed by the Executive Committee.

Director of Informatics and Performance Improvement
The Director of Informatics and Performance Improvement is responsible for the Trusts Health Record Manager and their annual programme of work, clinical information systems and the reporting of management information.

Local Managers
The responsibility for local records management is devolved to the relevant directors and managers. Heads of Departments, other units and business functions within the trust have overall responsibility for the management of records generated by their activities, e.g. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policy.

Health Records Managers (Local)
The Health Records Managers have direct responsibility for the daily management of Health Records functions within their service and work within the boundaries of trust Health Records Policy, Health Record Procedures, Local procedures and Statutory legislative framework, NHS Litigation Authority Standards and Information Governance Standards.

All staff
All trust staff *(this includes permanent, temporary, bank and agency workers)*, whether clinical, social care or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the trust and manage those records in keeping with this policy and with any guidance subsequently produced.

Compliance with the content of this policy will be monitored by the Health Records Manager and the findings presented to the Health Records Committee by way of an annual report.

13 DEVELOPMENT & CONSULTATION PROCESS

This policy has been developed by the Trust's Health Records Manager, Head of Information Governance, Executive Director of Finance, Director of Informatics & Performance Improvement. The policy has also been reviewed

by the Health Records Sub-Committee and the Information Governance & Caldicott Committee.

14 MONITORING

System for the Monitoring of Corporate Health Records Policy and Procedures	
Monitoring of compliance with this policy will be undertaken by:	Trust Health Records Manager
Monitoring will be performed:	On an annual basis
Monitoring will be undertaken by means of:	Audit to comply with requirements of NHSLA standards, Information Governance standards and compliance of this policy.
Should shortfalls be identified the following actions will be taken:	The Health Records Sub-Committee will consider the outcomes of the review and make recommendations for change to the Divisions, the Executive Committee and Information Governance & Caldicott/SIRO Committee.
The results of monitoring will be reported to:	The Executive Committee, the Information Governance & Caldicott/SIRO Committee and, if required, the Audit Committee.
Resultant actions plans will be progressed and monitored through:	The Health Records Sub-Committee.

15 REFERENCE DOCUMENTS

Records Management Code of Practice for Health and Social Care, 2016 – Information Governance Alliance
NHS Code of Practice – Records Management 2006, 2009
Public Records Act 1958/1967
NHS Code of Confidentiality 2003
Data Protection Act 1998
Freedom of Information Act 2000
NHSLA Risk Management Standards
NHSLA – Clinical Record Keeping Standards
Information Governance Standards
NMC–Guidelines for Records and Record Keeping
Mental Health & Learning Disabilities Minimum Data Set
"Setting the Record Straight" – Audit Commission 1995
Standards for the clinical structure and content of patient records – Academy of Medical Royal Colleges, July 2013

16. BIBLIOGRAPHY - No Bibliography

17. GLOSSARY - No glossary terms

18. IMPLEMENTATION PLAN

18. IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Co-ordination of implementation How will the implementation plan be co-ordinated and by whom? *Clear co-ordination is essential to monitor and sustain progress against the implementation plan and resolve any further issues that may arise.*	The implementation plan will be co-ordinated by the Trust Health Records Manager. The plan will include distribution of the policy in accordance with the guidance in Policy and Procedure for the Development, Ratification, Distribution and Reviewing Policies and Procedures. Lead clinical staff across both Divisions will receive a copy of this Policy (IT06) via email requesting dissemination to all their clinical and administrative staff.	December 2016
Engaging staff Who is affected directly or indirectly by the policy? Are the most influential staff involved in the implementation? *Engaging staff and developing strong working relationships will provide a solid foundation for changes to be made.*	This policy is applicable to all staff working for, or with, Mersey Care NHS Foundation Trust (the trust) who records, handles, stores or otherwise comes across service user information.	
Involving service users and carers Is there a need to provide information to service users and carers regarding this policy? Are there service users, carers, representatives or local organisations who could contribute to the implementation? *Involving service users and carers will ensure that any actions taken are in the best interest of services users and carers and that they are better informed about their care.*	There is no need to provide service users and carers with a copy of the policy. However, it is available if requested. Service Users and Carers will not be involved in implementing the procedure.	

18. IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Communicating What are the key messages to communicate to the different stakeholders? How will these messages be communicated? *Effective communication will ensure that all those affected by the policy are kept informed thus smoothing the way for any changes. Promoting achievements can also provide encouragement to those involved.*	Key messages are: - this policy applies to everyone working for or with NHS Health and Social Care Records - applies to electronic or paper based format - basic national standards of Record Keeping - safeguarding information contained in electronic/paper based Health Records All staff will be able to access the policy via their manager or the Trust website.	
Training What are the training needs related to this policy? Are people available with the skills to deliver the training? *All stakeholders need time to reflect on what the policy means to their current practice and key groups may need specific training to be able to deliver the policy.*	Regular updates for all staff on Good Management of Records as a minimum standard Training will be facilitated by Trust Health Records Manager.	
Resources Have the financial impacts of any changes been established? Is it possible to set up processes to re-invest any savings? Are other resources required to enable the implementation of the policy eg. increased staffing, new documentation? *Identification of resource impacts is essential at the start of the process to ensure action can be taken to addess issues which may arise at a later stage.*	There are no additional financial implications arising from the implementation of this procedure.	

18. IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Securing and sustaining change Have the likely barriers to change and realistic ways to overcome them been identified? Who needs to change and how do you plan to approach them? Have arrangements been made with service managers to enable staff to attend briefing and training sessions? Are arrangements in place to ensure the induction of new staff reflects the policy? *Initial barriers to implementation need to be addressed as well as those that may affect the on-going success of the policy*	Consideration of potential barriers was discussed during the development of the procedure.	
Evaluating What are the main changes in practice that should be seen from the policy? How might these changes be evaluated? How will lessons learnt from the implementation of this policy be fed back into the organisation? *Evaluating and demonstrating the benefits of new policy is essential to promote the achievements of those involved and justifying changes that have been made.*	Increased awareness of basic national record keeping standards Annual clinical record keeping audit	
Other considerations		