NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL POLICY

Health Records

Policy Number:	**IT06**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint SIRO/Information Governance Group**
Approved By:	**Executive Director of Finance**
Date Ratified:	**July 2020**
Next Review Date (by):	**July 2022**
Version Number:	**2020 – Version 1.7**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Information Governance Officer**

TRUST-WIDE NON-CLINICAL POLICY

2020 – Version 1.7

Striving for perfect care and a just culture

TRUST-WIDE NON-CLINICAL POLICY

Health Records

Further information about this document:

Document name	**Health Records Policy and Procedure - IT06**
Document summary	This Policy is issued as a framework to support Information Governance and effective health records management. This document is presented in a standard structure and format. It will be made available in appropriate, alternative languages and formats on request.
Author(s) Contact(s) for further information about this document	**Geoff Springer** **Information Governance Officer** **Telephone: 0151 478 6899** **Email: Geoff.springer@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the Trust's website	**Mersey Care NHS Foundation Trust** **V7 Building** **Kings Business Park** **Prescot** **Merseyside** **L34 1PJ** **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** Corporate Data Quality **IT14** Data Protection Policy **HR32** Supporting trans*non binary and non-gender employees and people who use our services Policy
This document can be made available in a range of alternative formats including various languages, large print and braille etc	
Copyright © Mersey Care NHS Trust, 2015. All Rights Reserved	

Version Control:

		Version History:
Version 1.4	Approved by Health records sub-Committee	September 2016
Version 1.5	Approved by Health records sub-Committee	September 2017
Version 1.6	Approved by Health records & Data Quality Working Group	May 2018
Version 1.7	Executive Director of Finance	June 2020

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 adults, including:

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child / 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 / 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 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, sex, race, religion and belief (or lack thereof), sexual orientation, gender reassignment, pregnancy and maternity and marital and civil partnership status. The Equality Act also requires regard to socio-economic factors.

The Trust is committed to promoting and advancing equality and removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those that do not 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

1 Purpose and Rationale

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 and CD's

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 requirements e.g. Mental Health Services and Community Services data set.

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. Scope

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 health records policy.

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.

2.3 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.

2.4 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 Appendix 1 –* ***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 General Data Protection Regulation 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.

3 Outcome Focused Aims and Objectives

3.1 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.

3.1.2 This policy is intended to be a comprehensive guide to all staff involved in handling service users health records in electronic or manual media. Should you have any queries regarding a particular issue, or anything not documented within this policy, please contact the Information Governance Officer for further details.

3.1.3 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.

3.1.4 To ensure quality, continuity of operational services and to meet with the statutory legislation within the General Data Protection Regulation, 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.

3.2 Audit

3.2.1 An annual audit is undertaken to ensure compliance with the NHS Resolution and Information Governance standards on record-keeping. The formal report of the Annual Health Records audit is reviewed by the Health Records and Data Quality Working Group, the minutes of which are reported to the Joint SIRO/Information Governance Group who monitor progress against the action plan.

3.3 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 clinical records must be inputted into the relevant clinical information system ideally within 24 hours of the patient/service user being seen. All assessments/web forms relating to CPA documentation should be on the clinical information system within 3 days.

3.4 Legal Obligations

3.4.1 The Trust must comply with the following legislation guidelines:

- **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).** This 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 1 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.
- **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.
- **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.
- **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.
- **General Data Protection Regulation (GDPR) – May 2018** controls how personal information is being used by organisations, businesses or the government. Everyone who is responsible for using data has to follow the General Data Protection Regulation 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'.
- **Data Protection Act 2018-** this was introduced alongside GDPR and is UK law. The Data Protection Act 2018 controls how personal information is being used by organisations, business or the government. Everyone is responsible for using personal data must follow the principles of the Act, using personal information fairly, lawfully and transparently.
- **Freedom of Information Act 2000** provides the public with access to recorded information held by the Trust in varying formats, but excluding personal information. A request for information must be made in writing and the Trust has a duty to comply with the request within twenty working days.
- **Access to Health records Act 1990** - legislation issued by the Department of Health - outlines the rights of access to deceased patient health records by specified persons.
- **Access to Medical Reports Act 1988** – legislation 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.

- **NHS Resolution Standards** - a special health authority that handles negligence claims made against NHS organisations and work to improve risk management practices in the NHS.
- **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.
- **Nursing and Midwifery Council (2015) The Code: Professional Standards and Behaviour for Nurses and Midwives** explains what they expect from nurses and midwives in relation to good record keeping.
- **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.

3.5 RECORD CREATION

3.5.1 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 General Data Protection Regulation – Subject Access Requests
- 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. PROCESS

4.1 RECORD KEEPING

4.1.1 Divisional 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 Information Governance Officer.

4.1.2 Non-compliance with Trust standards could result in employees being subject to HR01 Disciplinary Policy or HR11 Supporting Improvement Policy.

4.1.3 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 (Please contact the Information Governance Team for more information regarding abbreviations)
- 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

b) For those few areas where it is still required to use manual health records

- Entries should be written in black ink 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.

c) 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)

d) 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.

e) 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.

f) Cutting/Copying and Pasting Information

- Staff should avoid cutting/copying 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, e.g. "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.

g) 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.

4.1.4 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 REGISTRATION

4.2.1 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 that 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.

4.2.2 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.

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

4.2.4 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.

4.2.5 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.

4.2.6 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.

4.2.7 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 relevant clinical information system supportive documentation.

4.2.8 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.

4.3 AVOIDING THE RISK OF DUPLICATION OF CLINICAL RECORDS

4.3.1 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.

4.3.2 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. (Please see contact the IG Team for further advice)

4.4 Gender Realignment/Transgender

4.4.1 Recording of information within the health records should be done in conjunction with HR32(Support Trans* Non Binary and Non Gender Employees who use our Service) but the particular points below should be adhered to:-

- If a Service User is referred into the Trust and is going through the process of gender realignment their records will be formulated in the details they are living in currently.
- Should a Service User already be in receipt of Trust services and wishes to have their gender details changed they should make a direct request to the clinical team who will formally record this as appropriate to the request.
- If a Service User has undergone gender realignment they can request to have the whole of their clinical records changed/ closed. Services can request to see the Gender Recognition Certificate prior to closing/creating a new health record.

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 2**. Specific staff based within the Divisions have been trained in the processes involved in retrieving health records.

4.5.2 Retrieving Health records from another Division

If a member of staff from one Division or Service requires information contained in a clinical information system 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 in confidential waste bins

4.6 SCANNING OF DOCUMENTATION INTO ELECTRONIC HEALTH RECORDS

4.6.1 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.

4.6.2 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.

4.6.3 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/RIO.

4.6.4 The staff member undertaking the scanning should quality assure the scanned image against the original, e.g. check page reverse/side annotations.

4.7 Validation of Entries and Countersigning

4.7.1 Staff, regardless of designation, who make an entry into a patient care record, must take personal accountability for good record-keeping. They must keep clear, accurate, timely and complete records of the care they provide to their patients to support communication, continuity and decision-making. This includes all forms of patient records, i.e. anything that is documented about a patient and their care and treatment.

The validation of entries within an electronic health record is equivalent to signing an entry in a paper care record. Validation attaches an electronic signature to the entry and demonstrates that the author is satisfied with the content and accuracy of the entry. All entries must be contemporaneous (made in the patient's record as soon as possible after the contact and before the member of staff goes off duty) and validated/signed off. Entries that are not validated/signed off will not be deemed complete.
(If it is not possible to make the entry within 24-hours, a retrospective entry must be completed)

4.8 Delegation of Record Keeping and Countersigning

4.8.1 Record-keeping can be delegated to health care assistants (HCAs), nursing associates, assistant practitioners (APs) and nursing students so that they can document the care they provide and take personal accountability for the content and quality of the records. However, they must be deemed as wholly competent in the complete provision of care, which includes record-keeping and that it is in the best interest of the patient. The supervising practitioner retains professional accountability for the appropriateness of the delegation of the task.

4.8.2 HCAs, nursing associates, APs and nursing students deemed wholly competent can validate their own entries made on the electronic health record

once they are satisfied with the accuracy and completeness of the entry. Those not deemed to be competent in record- keeping must not make entries into a patient's care record.

If a student/staff member does not have access rights to the electronic health record to make an entry, two options are available:

- the student/staff member must write up their entry in Microsoft Word, including their full name, designation, date and time of the entry. The supervising practitioner will then either:
    - copy the entry into the electronic health record as a clinical entry, stating that they have done this on the person's behalf and then validate the entry or
    - upload the Microsoft word document to the electronic health record and associate this document to a clinical entry, stating that they have done this on the person's behalf, and then validate the entry
- the supervising practitioner will make an entry into the electronic health record stating who made the observation/completed the assessment/gave the care/was also present e.g. 'wound dressing renewed by nursing student [PERSON'S NAME] of [UNIVERSITY'S NAME] University'. The entry must then be validated. This will likely be used for students with the Trust on short-term placements.

Please note a registered nurse must not countersign records unless they have witnessed or can validate the activity as having taken place.

See the Royal College of Nursing's Principles of Accountability and Delegation for further guidance (www.rcn.org.uk/accountability-and-delegation).

4.9 RIGHT TO RECTIFICATION

4.9.1 The General Data Protection Regulation includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. This is referred to as "the Right to Rectification".

4.9.2 An individual can make a request for rectification, verbally or in writing, to anyone within the Trust – the Trust has one calendar month to respond to a request.

4.9.3 The Trust must take reasonable steps to satisfy itself that the data is accurate and to rectify the data if necessary. Consideration should take into account the arguments and evidence provided by the data subject.

4.9.4 If the data subject disputes an opinion recorded within their clinical record as long as the record shows clearly that the information is a clinical opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

4.9.5 After considering the individual arguments and evidence provided, if the Trust considers that the data is correct and therefore will not rectify the data, they must inform the data subject and explain why it believes the data is accurate. (Please speak to the IG Team for further advice)

4.10 STORAGE OF HEALTH RECORDS

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

4.11 Storing Non-Paper Records

4.11.1 Microfiche - 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's Information Governance Officer.

4.11.2 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 the Public Records Act 1958/1967.

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

4.11.4 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.

4.11.5 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 Trust's computer hard or shared drives. Print-offs 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.

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

4.12.1 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.

4.12.2 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.

4.12.3 Paper 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.

412.4 Information contained within the health record must not be revealed to any unauthorised persons.

4.12.5 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.

4.12.6 The incident must be reported immediately to the relevant line manager. The Information Governance Officer and Data Protection Officer should also be advised of the incident.

4.12.7 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 10*.

4.13 HEALTH RECORDS IN TRANSIT

4.13.1 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?

4.13.2 Postal options must be considered if health records are to be sent in external mail e.g. Special Delivery, Signed for First Class

4.13.3 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. 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.

4.13.4 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.

4.13.5 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

4.13.6 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.

4.13.7 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.***

4.14 RETENTION/DESTRUCTION OF HEALTH RECORDS

4.14.1 The NHS Retention/Disposal Schedule **MUST** be adhered to in relation to all health records and is set out in Appendix 1 The Trust employs social care staff and therefore create health and social care records.

4.14.2 The destruction of health records is an irreversible act, however the cost of keeping records can be high. 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.

4.14.3 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 Data Protection Officer and Caldicott Guardian and an agreement is reached with both the Health Records and Data Quality Working Group Joint SIRO/Information Governance Group 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.

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

4.15.1 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.

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

4.15.3 Once a health record has been identified for destruction this should then be disposed of in accordance with guidance documented in 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.

4.15.4 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 General Data Protection Regulation. 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.

4.15.5 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 1

4.15.6 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.

4.16 Marking Health Records for Permanent Preservation

4.16.1 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.

4.16.2 If the Caldicott Guardian is in agreement the clinician must document clearly the reason for permanent preservation within the health record.

5 TRAINING

5.1 Training

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 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**.

6 DUTIES & RESPONSIBILITIES

6.1 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.

6.2 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.

6.3 Data Protection Officer

The Data Protection Officer (DPO) role carries set duties as specified within the General Data Protection Regulation. The DPO assists the Trust to monitor internal compliance, inform and advise on our data protection obligations. The DPO must be independent and an expert in data protection.

6.4 Senior Information Risk Owner (SIRO)

The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board.

6.5 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.

6.6 Data Protection Officer

It is the responsibility of the Data Protection Officer 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 Data Protection Officer is the recognised professional lead within the Trust to advise staff on records management issues.

6.7 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.

6.8 Joint SIRO/Information Governance Group

The Joint SIRO/Information Governance Group ensures the Trust operates within the Information Governance framework and reports to the Executive Committee.

6.9 Health records & Data Quality Working Group

The Health records & Data Quality Working Group is comprised of multi-disciplinary staff from services provided within the Trust involved in promoting a high standard of Records Management and Data Quality to assist with the diagnosis/treatment and continuity of service user care. Also as part of the annual health records audit the contents of the audit tool is agreed by the group, the findings are approved and the development and delivery of any subsequent action plans are also the responsibility of the group.

The Working Group meets on a bi-monthly basis and minutes from the Health records & Data Quality Working Group will be tabled and reviewed by the Joint SIRO/Information Governance Group.

6.10 Divisional Health records Manager

The responsibility for health 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. This system must also been in line with national records keeping standards.

6.11 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.

7 CONSULTATION PROCESS

This policy has been developed by the Trust's Information Governance Officer, Executive Director of Finance, Joint Chief Information Officer , Joint Chief Clinical Officer and the Director of Informatics & Performance Improvement. The policy has also been reviewed by Clinical Leads for Allied Health Professionals/Psychology Staff/Social Care Staff and Nursing Staff,

Clinical information systems staff, and members of the Health records & Data Quality Working Group Committee and the Joint SIRO/Information Governance Group.

8 MONITORING

System for the Monitoring of Corporate Health records	
Monitoring of compliance with this policy will be undertaken by:	Information Governance Officer
Monitoring will be performed:	On an annual basis
Monitoring will be undertaken by means of:	Audit to comply with requirements of NHS RESOLUTION standards, Information Governance standards and compliance of this policy.
Should shortfalls be identified the following actions will be taken:	The Health Records & Data Quality Working Group will consider the outcomes of the review and make recommendations for change to the Divisions, the Executive Committee and the Joint SIRO Group/Information Governance Group.
The results of monitoring will be reported to:	The Executive Committee, the Joint SIRO/Information Group and if required, the Audit Committee.
Resultant actions plans will be progressed and monitored through:	The Health Records & Data Quality Working Group.

APPENDIX 1 - Retention Schedule (2016)

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Care Records with standard retention periods				
Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Adult social care records	End of care or client last seen	8 years	Review and if no longer needed destroy	
Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Electronic Patient Records System (EPR) NB: The IGA is undertaking further work to refine the rules for record retention and to specify requirements for EPR systems	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.
General Dental Services records	Discharge or patient last seen	10 Years	Review and if no longer needed destroy	General Dental Services records
Record Type	**Retention**	**Retention**	**Action at end of**	**Notes**

	start	period	retention period	
GP Patient records	Death of patient	10 years after death - see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: • Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated • Where a patient is known to have emigrated records may be reviewed and destroyed after 10 years • If the patient comes back within the 100 years,
Mental Health records	Discharge or patient last seen	20 years or 8 years after the patient has died	Review and if no longer needed destroy	Covers records made where the person has been cared for under the Mental Health Act 1983 as amended by the Mental Health Act 2007. This includes psychology records. Retention solely for any persons who have been sectioned under the Mental Health Act 1983 must be considerably longer than 20 years where the case may be ongoing. Very mild forms of adult mental health treated in a community setting where a full recovery is made may consider treating as an adult records and keep for 8 years after discharge. All must be reviewed prior to destruction taking into account any serious incident retentions.
Obstetric records, maternity records and antenatal and post natal records	Discharge or patient last seen	25 years	Review and if no longer needed destroy	For the purposes of record keeping these records are to be considered as much a record of the child as that of the mother.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Care Records with Non-Standard Retention Periods				
Cancer/Oncology - the oncology records of any patient	Diagnosis of Cancer	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of any cancer must be retained in case of future reoccurrence. Where the oncology records are in a main patient file the entire file must be retained. Retention is applicable to primary acute patient record of the cancer diagnosis and treatment only. If this is part of a wider patient record then the entire record may be retained. Any oncology records must be reviewed prior to destruction taking into account any potential long term research value which may require consent or anonymisation of the record.
Contraception, sexual health, Family Planning and Genito-Urinary Medicine (GUM)	Discharge or patient last seen	8 or 10 years (see Notes)	Review and if no longer needed destroy	Basic retention requirement is 8 years unless there is an implant or device inserted, in which case it is 10 years. All must be reviewed prior to destruction taking into account any serious incident retentions. If this is a record of a child, treat as a child record as above.
HFEA records of treatment provided in licenced treatment centres		3, 10, 30, or 50 years	Review and if no longer needed destroy	Retention periods are set out in the HFEA guidance at: http://www.hfea.gov.uk/docs/General_directions_0012.pdf
Medical record of a patient with Creutzfeldt-Jakob Disease (CJD)	Diagnosis	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of CJD must be retained. Where the CJD records are in a main patient file the entire file must be retained. All must be reviewed prior to destruction taking into account any serious incident retentions.
Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care. The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Births, Deaths & Adoption Records				
Birth Notification to Child Health	Receipt by Child health department	25 years	Review and if no longer needed destroy	Treat as a part of the child's health record if not already stored within health record such as the health visiting record.
NHS Medicals for Adoption Records	Creation	8 years or 25th birthday	Review and consider transfer to a Place of Deposit	The health reports will feed into the primary record held by the local authority children's services. This means that the adoption records held in the NHS relate to reports that are already kept in another file which is kept for 100 years by the appropriate agency and local authority.
Record Type	**Retention start**	**Retention period**	**Action at end of retention period**	**Notes**
Pharmacy The IGA are conducting further work to expand this section which will be updated in the near future. As an interim measure you can view a list of Pharmacy records and their associated retention periods and actions by clicking on this link to the NHS East and South East Specialist Pharmacy Services retention schedule.				
Information relating to controlled drugs	Creation	See Notes	Review and if no longer needed destroy	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) guide can be found at the link (subscription required): http://www.rpharms.com/support/mep.asp Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years. NHS BSA will hold primary data for 20 years and then review. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see: http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/
Pharmacy prescription records. See also Information relating to controlled drugs.	Discharge or patient last seen	2 Years	Review and if no longer needed destroy	There will also be an entry in the patient record and a record held by the NHS Business Services Authority. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see:

				http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-
Record Type	**Retention start**	**Retention period**	**Action at end of retention period**	**Notes**
Pathology				
Pathology Reports/Information about specimens and samples	Specimen or sample is destroyed	See Notes	Review and consider transfer to a Place of Deposit	This Code is concerned with the information about a specimen or sample. The length of storage of the clinical material will drive the length of time the information about it is to be kept. For more details please see: https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition-.html Retention of samples for clinical purposes can be for as long as there is a clinical need to hold the specimen or sample. Reports should be stored on the patient file. It is common for pathologists to hold duplicate reports. For clinical purposes this is 8 years after the patient is discharged for an adult or until a child's 25th birthday whichever is the longer. After 20 years for adult records there must be an appraisal as to the historical importance of the information and a decision made as to whether they should be destroyed of kept for archival value.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Event & Transaction Records				
Blood bank register	Creation	30 Years minimum	Review and consider transfer to a Place of Deposit	
Clinical Diaries	End of the year to which they relate	2 years	Review and if no longer needed destroy	Diaries of clinical activity & visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.
General Ophthalmic Services patient records related to NHS financial transactions	Discharge or patient last seen	6 Years	Review and if no longer needed destroy	General Ophthalmic Services patient records related to NHS financial transactions
Operating theatre records	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	If transferred to a Place of Deposit the duty of confidence continues to apply and can only be used for research if the patient has consented or the record is anonymised.
Patient Property Books	End of the year to which they relate	2 years	Review and if no longer needed destroy	
Referrals not accepted	Date of rejection.	2 years as an ephemeral record	Review and if no longer needed destroy	The rejected referral to the service should also be kept on the originating service file.
Requests for funding for care not accepted	Date of rejection	2 years as an ephemeral record	Review and if no longer needed destroy	
Screening, including cervical screening, information where no cancer/illness detected is detected	Creation	10 years	Review and if no longer needed destroy	Where cancer is detected see 2 Cancer / Oncology. For child screening treat as a child health record and retain until 25th birthday or 10 years after the child has been screened whichever is the longer.
Smoking cessation	Closure of 12 week quit period	2 years	Review and if no longer needed destroy	
Transplantation Records	Creation	30 Years	Review and consider transfer to a Place of	See guidance at: https://www.hta.gov.uk/codes-practice

			Deposit	
Ward handover sheet	Date of handover	2 years	Review and if no longer needed destroy	This retention relates to the ward. The individual sheets held by staff must be destroyed confidentially at the end of the shift.
Notifiable disease book	Creation	6 years	Review and if no longer needed destroy	

APPENDIX 2 – Contact Addresses

Local Division
Divisional Support Services Manager
V7 Building
Kings Business Park
Prescot
L34 1PJ

Secure Division
Health Records Lead
Ashworth Hospital
Maghull
L31 1HW

Contact Telephone Number: 0151 471 2629

Community Division
Health Records Manager
Burlington House
Crosby Road North
Liverpool L22 OQB

Contact Telephone Number: 0151 295 3163

Corporate Division
Human Resources
V7 Building
Kings Business Park
Liverpool

Contact Telephone Number: 0151 479 3881

Corporate Division
Occupational Health Department/Staff Support
Switch House
North Perimeter Road
Bootle
Liverpool
L30 7PT

Contact Telephone Number: 0151 471 2451

Appendix 3

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
Code of Practice on Confidentiality Information 2014
General Data Protection Regulation 2018
Date Protection Act 2018
Freedom of Information Act 2000
NHS Resolution
Data Security Protection Toolkit Standards 2018
NMC (2015) The Code: Professional Standards and Behaviour for Nurses and Midwives
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

Equality and Human Rights Analysis

Title: Health Records Policy and Procedure
Area covered: All health records across the Trust

What are the intended outcomes of this work?
Who will be affected? All staff, including those staff who are seconded Social Care staff, or staff who are part of Informatics Merseyside are all responsible for the records which they create or use.

Evidence
What evidence have you considered? As part of the policy review human rights analyisis check has been undertaken. There has been no evidence provided to consider concerning in relation to Equality and Human Rights.
Disability (including learning disability) There has been no evidence provided to review in terms of the policy having any effect on disability.
Sex There has been no evidence provided to review in terms of the policy having any effect on sex.
Race There has been no evidence provided to review in terms of the policy having any effect

on race.
Age There has been no evidence provided to review in terms of the policy having any effect on age.
Gender reassignment (including transgender) This is an area where the policy may be used in a positive way to enable service user's to get their records altered in accordance with their circumstances. The policy follows the general legal principles relating to gender reassignment.
Sexual orientation There has been no evidence provided to review in terms of the policy having any effect on a person's sexual orientation.
Religion or belief There has been no evidence provided to review in terms of the policy having any effect on a person's religion or religious beliefs.
Pregnancy and maternity There has been no evidence provided to review in terms of the policy having any effect on pregnancy or staff on maternity leave.
Carers There has been no evidence provided to review in terms of the policy having any effect on carers.
Other identified groups The policy works hand in hand with policy the Trust's policy *HR32* – Supporting *trans* non binary and non-gender employees and people who use our service.* This In turn offers this particular group of staff the correct service in relation to record keeping.
Cross Cutting – *Not Applicable*

Human Rights	**Is there an impact? No** **How this right could be protected? N/A**
Right to life (Article 2)	**N/A**

Right of freedom from inhuman and degrading treatment (Article 3)	**N/A**
Right to liberty (Article 5)	**N/A**
Right to a fair trial (Article 6)	**N/A**
Right to private and family life (Article 8)	**N/A**
Right of freedom of religion or belief (Article 9)	**N/A**
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	**N/A**
Right freedom from discrimination (Article 14)	**N/A**

Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.*
The Information Governance Team has previously taken legal advice on the development and the implementation of this policy because of its complexity.

Summary of Analysis *This highlights specific areas which indicate whether the whole of the document supports the Trust to meet general duties of the Equality Act 2010*
Eliminate discrimination, harassment and victimisation *The policy strives to eliminate discrimination treating everyone's health records in the same*

way. It also lays out clearly how health records must be treated and respected therefore supporting the Trust in meeting the general duties of the Equality Act 2010.

Advance equality of opportunity

N/A

Promote good relations between groups

The policy has a provision in it for minority groups, under certain circumstances, to get their health records altered. This in turn promotes good relations and is in line with current legislation.

What is the overall impact?

Good, no adverse effects noted.

Addressing the impact on equalities

N/A

Action planning for improvement – N/A

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different*

groups as the policy is implemented (or pilot activity progresses)

- *Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives.*

For the record **Name of persons who carried out this assessment:** Geoff Springer
Date assessment completed: 11th June 2020
Name of responsible Director: Neil Smith
Date assessment was signed: 11th June 2020