# Health Records Policy

| Version: | 2.1 |
|---|---|
| Ratified by: | Information Governance Steering Group |
| Date ratified: | March 2016 |
| Name of originator/author: | Head of Information Governance |
| Name of responsible committee/individual: | Information Governance Steering Group (IGSG) |
| Circulated to: | Members of IGSG<br><br>Associate Director of Mental health Law<br><br>RiO team |
| Date issued: | March 2016 |
| Review date: | March 2019 |
| Target audience: | All staff |

# Version Control Summary

| Version | Date | Author | Status | Comment |
|---|---|---|---|---|
| 1.0 | October 2011 | Head of Information Governance | Final | Condenses previous versions of the policies and procedures below into one document: Clinical records management procedures Health Record Keeping Policy Procedure for Health Record Archiving and Destruction |
| 1.1 | January 2012 | Head of Information Governance | Final | Incorporates NHSLA Level 3 requirements |
| 1.2 | March 2012 | Head of Information Governance | Final | Incorporates revised NHSLA Level 3 requirements published end January 2012 |
| 1.3 | May 2012 | Head of Information Governance | Final | Sets definitive timescales for entering information on to electronic record keeping systems |
| 1.4 | July 2012 | Head of Information Governance Clinical Records Development Manager | Final | Revised to reflect access / tracer card practice in locations without a dedicated Records Manager |
| 1.5 | August 2012 | Head of Information Governance | Final | Includes updated guidance on filing incident reports. Outlines clinical responsibility for ensuring new information about inpatients is seen and acted on |
| 1.6 | November 2012 | Clinical Records Development Manager | Final | Strengthened guidelines to address queries related to errors identified in the entries made in clinical records. Clarified guidance on electronic health records. |
| 1.7 | January 2014 | Head of Information Governance | Final | Revised guidance to transfer records from CAMHS to adult services |
| 2.0 | January 2016 | Associate director of Assurance | Final | Revised as the primary health record is now electronic. .Incorporates previous Clinical RiO policy |
| 2.1 | February 2016 | Head of Information Governance | Final | Revised validations section following IGSG/IMTAC review |

# Contents

## 1.0　　Introduction

High standards of record keeping underpin the delivery of high quality, evidence based healthcare. Records should be up to date, accurate and accessible when required.  This policy provides a framework for achieving high quality safe record keeping based on the principle that records are electronic.

## 2.0　　Purpose

The Data Protection Act 1998 summarises a health record as 'one which relates to the physical or mental health of an individual … made by or on behalf of a health professional in connection with the case of that individual. Thus with the exception of the anonymised information most if not all NHS information concerning patients whether held electronically or on paper will fall within the scope of the Act'.

This policy sets out the standards and processes required for maintaining high quality health record keeping standards for all service users.

The electronic record has replaced the paper record as the primary record for both community and mental health service users unless a service does not yet have access to an electronic clinical system.

## 3.0　　Duties

**All individuals**

All individuals must ensure confidentiality, integrity, accuracy and appropriate availability of records. All individuals are personally responsible for the records they create or use and will not be allowed access to RiO or any other electronic clinical system until they have completed training at this Trust.

All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty of confidentiality. Everyone accessing the health information of service users has a common law duty of confidentiality to both the service user and the Trust. Confidentiality extends even after the death of a service user.

Individuals should be aware that information recorded in a service user's record is legally binding. The record should therefore be non-judgemental and contain only information the individual would be willing to be accountable for in Court.

Any notes about a service user form part of the clinical record and should be uploaded to their clinical record e.g. during ward rounds, during CPA meetings, where Duty of Candour is invoked etc,

All teams should have an internal process for ensuring the relevant clinician / care worker is aware of all new documentation / correspondence relating to a service user.

All individuals should be familiar with their patient system crib sheets which guide the user through particular tasks.

Individuals should never share Smartcards. If information is accessed / added on behalf of another individual this should be made clear within the record. If an individual accesses the electronic record of a patient not under their direct care they will be prompted to state why they are accessing this information. This will be recorded and audited. Access without a legitimate reason may result in disciplinary action or dismissal and legal proceedings

**Line managers**

All ward, team or service managers, supported by the Head of Information Governance, are responsible for ensuring the principles set out in this policy are followed together with any local supporting procedures.

All line managers and supervisors must ensure that their staff, whether administrative or clinical, are adequately trained in the management of health records and apply the appropriate guidelines and crib sheet procedures.

Line managers will be responsible for authorising access to RiO and other systems requiring Smartcards through the Registration Authority (RA) who will issue smartcards on receipt of that authorisation.

**Clinicians**

Clinicians must ensure they adhere to the records management standards of their professional body in addition to the requirements of this policy.  Validation

All qualified staff are able to validate their own records.  The only exceptions to this are those staff with identified capability issues or students whose need for validation should be highlighted on the access application by line managers/supervisors.

**Local Records Managers**

Each directorate will have a local Records Manager under whose guidance designated staff will:

**For paper records**:

- Maintain safe and structured records management stores
- Ensure there is a process for the retrieval of case notes and update tracer cards.
- Organise the safe transportation of records from one location to another

**For all records**

- Deal with requests for access to health records within statutory time limits. In some services there are designated access to records leads. This is covered in detail in the Trust's Access to Records policy.

**Duty Senior Nurse**

Out of hours, the Duty Senior Nurse / Manager in charge is the only individual permitted to access a paper records store to retrieve case notes and update tracer cards. Out of hours the Duty Senior Nurse / Manager in charge must enter inpatient events on to the relevant electronic clinical recording system within four hours of the occurrence of the event

**Data Controller**

The Chief Executive is the Trust's Data Controller and has an overarching duty to make arrangements for the safety and integrity of the Trust's health records

**Data Protection Officer**

The Information Rights Manager is the Trust's registered Data Protection Officer and has responsibility for ensuring health records meet statutory requirements

**Caldicott Guardian**

The Medical Director is the Caldicott Guardian and has responsibility for matters relating to patient confidentiality.

**Service Directors as Information Asset Owners**

Service Directors are Information Asset Owners for the health records within their service and must ensure the quality, integrity and security of records in their directorates.

## 4.0    General principles

**Health records use**

Health records must be reliable, accurate and timely to support:

- Continuity of care
- Multi disciplinary working
- Defence in cases of litigation or complaints
- Evidence based clinical practice
- Administrative  and managerial decision making
- Legal requirements including requests for access to records
- Clinical audit and effectiveness
- Statutory and contractual reporting requirements

**Health records standards**

Health records must:

- Be factual, consistent and be written according to Trust policy and accepted professional standards

- Contain as a minimum the service user's name, date of birth and NHS number. Where the NHS number is not known it should be verified via SCR / PDS. To ensure continuing accuracy of records the service user's full name, address and key contact details (including GP) should be verified at each contact and differing records synchronised.

- Completed as soon as possible after the event. Services should check local CQUINS / KPIs adhering to any shorter timescales where required.  In particular, Trust timescales are:

  o Referrals within 24 hours of receipt

  o Outpatient / community entries within 24 hours of  event

  o Inpatient entries within four hours of occurrence  e.g. admission, discharge, transfer, AWOL, leave etc

o   Physical health forms within 24 hours

**Confidentiality**

Information in a service user's record must be held in complete confidence and only viewed by those directly involved in the provision of care or who are otherwise authorised by the Trust to do so. Unauthorised disclosure and misuse of information constitutes a breach of confidentiality and breach of this policy which may lead to disciplinary action, dismissal and legal action.

Information contained in a service user's record should only be accessed on a 'need to know' basis. Individuals are specifically not permitted to access the records of people they know via a work, social or family connection or in response to media interest.

The Trust will undertake regular and targeted audits to identify instances where confidentiality is breached and take action against any individual found to have inappropriately accessed a record.

Where copies of records are taken outside the Trust (i.e. to visit a service user) they should not be opened / looked at whilst on public transport

**Format**

Health records will be in a number of formats including emails, x rays, photographs, audio visual recordings. The same principles apply to all formats. Where paper copies are received note that the primary health record in the Trust is electronic. Paper copies should therefore routinely be scanned and held electronically unless the format makes this not possible.

**Records retention**

Records in any media (electronic or paper) must be retained according to the Trust's Record Retention and Disposal Schedule. This is based on the NHS Records Management Code of Practice.

Inactive records that have reached the minimum retention period should be reviewed annually to identify the need for extended retention or destruction. After review the list should be updated to show those identified for destruction and those identified for extended retention.

**Confidential waste**

All confidential waste must be securely destroyed. Waste material should be sent to the designated confidential destruction site or shredded. All waste paper baskets must be properly labelled to read 'No Confidential Waste'. In the absence of a shredder, confidential waste must be kept in a 'Confidential Bag' which should kept in secure location and send to the confidential destruction site

**Information sharing**

Generally, the following principles apply:

- Service users should complete a Permission to share form that clearly lists individuals and agencies they do not want information to be shared with. The form should be updated at regular intervals. They should also be given a copy

of the [Your records and you](#) leaflet that explains how their information is processed, and advised that in some circumstances it may not be possible to care for them if their information is not shared.

- 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.

- Explicit consent is required if identifiable service user information is used in any publication

- Where identifiable information is disclosed a record of the disclosure and the reasons for doing so should be recorded in the notes

- In circumstances where information is shared without the consent of the service user the Responsible Clinician should make this decision The Information Rights Manager, Associate Director of Assurance or Caldicott Guardian can also advise

- When a child or vulnerable adult is believed to be at risk then relevant information should be shared without delay. This requirement will always override all other confidentiality considerations. Conversely, if it is believed disclosure may compromise an individual's safety, or that it is not in the public interest to disclose, then the information should not be shared. Reasons must always be documented in the record.

**Mental Health Act documentation**

There are specific requirements regarding the receipt and scrutiny of documents under the Mental Health Act 1983:

- Receipt of section papers - only Mental Health Law staff and clinical staff at Band 5 or above (or equivalent) who have at least one year's experience at that level and have attended the relevant Trust training are authorised to formally receive section papers and scrutinise them

- Leave periods - the granting of leave and the conditions attached to it should be recorded in the notes and on the Trust's section 17 form. Copies of the form should be given to the service user, any appropriate relatives or friends and any professionals in the community who need to know

- The service user's legal status in respect of their detention, leave and consent to treatment should be immediately apparent from the medical notes

**Incident forms**

- Where an incident relates to one service user the incident form must be added to the record or as a minimum the Datix reference logged

- Where incidents relate to more than one service user they may be added / logged in each record provided person identifiable information relating to the other service user(s) is redacted. Otherwise they should be filed with the locality SI Co-ordinator or Clinical Governance Manager and reference to the incident made in the progress notes. Any associated documentation should reflect this.

- Any Duty of Candour correspondence or conversation should routinely be uploaded to the clinical system

## Complaints records

Complaints records must be filed separately from the service user's health record unless there is a need to record the complaint (for example where it is directly relevant to the service user's health and failure to recognise this when caring for the service user could have a detrimental effect on the health and well being of that individual).

## Child Health Records (Community Health Newham only)

Community Health Newham staff should currently refer to the Record Keeping and Management Procedure for Integrated Health Visiting and School Nursing Service

## Transfer of records from CAMHS to adult mental health services

For service users admitted to an adolescent inpatient service within the Trust or elsewhere (e.g. the private sector), who are approaching 18 years of age and are known to community CAMHS, it will usually be the responsibility of community CAMHS to initiate the transfer process. All CAMHS records are now electronic. .Detailed information is available in the CAMHS Transition policy

## Research and teaching

The Trust has teaching hospital status for students in a number of disciplines. All students are bound by the principles of confidentiality. The following standards apply:

- Service user records may be used for teaching purposes and clinical supervision within the clinical area

- If records are to be used for teaching purposes outside of the clinical area then service user details must be made completely anonymous.

- The principles of access and confidentiality remain the same and the right of the patient to refuse access to their records should be respected and documented in their notes

- The Local Research Ethics Committee must approve the use of service user records for research

- Any use of service users' records for research purposes must comply with the Department of Health's Research Governance Framework

## Service closure or transfer

- If a service or site is closed, split or amalgamated with or from another service or Trust, the service manager should work with the electronic clinical records team, access to records leads / local Records managers and Estates to ensure appropriate transfer, access, storage and retention of the relevant records. The centralised information governance team should always be consulted

- In some circumstances an information sharing agreement or SLA may be required. In such cases the Integrated Governance Manager should be consulted.

## 5.0    Electronic records

The Trust's primary record keeping systems are electronic. Duplicate paper records systems should not therefore be used.

### Principles

The following principles apply:

- Only Trust approved scanners will be used for scanning documents

- All information about a service user received electronically will be uploaded to the clinical system

- All information about a service user received in paper format will be scanned and subsequently uploaded to the clinical system

- All services will set up team based shared folders on the K drive. Folders and files / documents will be locked down to those individuals with a specific need to access the information. Standardised naming conventions will be used. Folders will be used only for drafting, processing and auditing information prior to uploading to the clinical system and will not become a secondary clinical system.

- When the clinical system is unavailable paper records should be scanned and temporarily held in the team folder on the K drive. Electronic records should similarly be temporarily held on the K drive rather than individual mailboxes or H drives. When the clinical system becomes available priority should be given to uploading documents

- The electronic clinical system record is the primary record. No other current records will be kept other than a small temporary folder outlined below. All original paper and electronic information will therefore be deleted once the scanned copy on the electronic clinical system has been verified as attaining the same standard as the originating copy. This is to prevent duplication of systems and information and the potential for information to be missed, incorrectly added to or otherwise inappropriately processed

- Teams will set up a systematic process for alerting all members of the treating team to newly received and uploaded information including incoming electronic and paper documents

- Where teams or individuals outside the treating team add information to a clinical system they will routinely alert the treating team to raise awareness of any immediate or significant issues

- Clinicians will routinely check the clinical system for newly received information prior to an appointment / intervention with a service user

- Correspondence must not be filed in the clinical system unsigned. Typed correspondence must always contain an electronic signature. Where the clinician prefers to delegate authority to an administrator for adding the signature, this should be confirmed by email and the email also retained in the clinical system

- Electronic records are subject to the same retention and deletion periods as paper records (i.e. the retention period does not alter simply because the format is electronic rather than paper)

- Electronic records are subject to regular audit including record keeping standards and legitimate relationship access to records. This may include targeted audits

- Records pre-dating clinical system implementation will be retained in paper format and will not currently be uploaded to the clinical system except in instances where the Responsible Clinician believes there is distinct value in doing so

- Requests for access to records will be centrally managed by the Access to Records leads. Where solicitors require access to the service user's electronic record this should be printed out and filtered for third party information. This should comply with the 40 day timescales referred to within the Data Protection Act 1998

- Services should always access Reporting Services for contemporaneous clinical information when RiO is unavailable

- The electronic record is the primary record. No other current records will be kept other than the temporary folder outlined below. Original documents will be deleted once the scanned copy has been verified as attaining the same standard as the original document. This is to prevent duplication of systems and information and the potential for information to be missed, incorrectly added to or otherwise inappropriately processed

**Temporary paper folder actions**

| Document type | Retain in paper format once episode of care complete? | Action on completion of episode of care |
|---|---|---|
| 'This is me' first person care plan | No | Stamp and upload to clinical system |
| Prescription / depot charts | Yes | |
| Observation forms | Yes | Also upload to clinical system |
| Outcome measures & other questionnaires | No | Upload to clinical system |
| Written copy of CPA form with signatures | Yes, temporarily until next review | Upload to clinical system |
| Sticky labels with patient details (for ordering investigations) | No | |
| Registration form printout | Yes | |
| Current care plan | No | Upload to clinical system |
| Current risk assessment | No | Upload to clinical system |
| Patient property receipts | No | Upload to clinical system |
| MHA documents (excluding police documentation which should be uploaded to RiO | Yes | |
| Alerts with an immediate | Yes | Also upload to clinical |

| impact on patient care | | system |
|---|---|---|
| Do not resuscitate forms | Yes | Also upload to clinical system |
| Results / investigations / bloods | No | Upload to clinical system |
| Audio visual recordings | No | Transcribe and upload to clinical system |
| Artwork / non standard scan size documents | Check if patient wants | Take photo and upload to clinical system |
| Process notes | No | Destroy. Do not scan / upload unless Therapist advises should be kept |
| Seclusion documents | No | Scan and upload to clinical system |
| ECGs | Yes. Store in the resealable wallets provided specifically for this purpose | |
| Growth charts | No | Scan and upload to clinical system. Download back to hardcopy if patient presents again. |

- For services using RiO the processes on the RiO user guide pages on the intranet will be followed at all times

## 6.0    Paper records

**Principles**

Although the primary record is electronic, the Trust still holds historic paper records. The following principles apply:

Paper records must be stored in an area where service users, members of the public and unauthorised staff are unable to gain access to them.

- Requests for records held in an external repository (e.g. Iron Mountain) must be made via the Access to Records Leads / local Records Managers.

- Trust individuals are only allowed access to records stores during normal working hours with the permission of the relevant local Records Manager / Access to Records Leads and on production of valid identification. Out of Hours the only access is via the Duty Senior Nurse / Manager in charge.

- Where records are stored in areas that do not have a 24/7 staff presence then they must be secured in an area that is securely locked when the premises are unstaffed.

- Missing or part missing health records must be reported via the Trust's incident reporting process and as a result will be investigated.

**Tracking procedure**

- Tracer cards should be used to document the movement of paper records unless there is an electronic tracking system.

- Only medical records staff or the Duty Senior Nurse / Manager in charge are authorised to retrieve records and update tracer cards. In smaller centres where there are no dedicated medical records staff, the service manager will assign responsibility to relevant staff members to ensure compliance with the record tracking procedure.

**Filing area standards**

The following standards apply at all times:

- Place files on the shelf in the correct numerical or alphabetical order with the spine underneath and the case note number facing outwards

- Leave the tracer card in situ at all times. Complete movements and mark RETURNED when case notes are filed back. Do not add any other documentation

- The file storage area should be regularly audited utilising the above standards

- Separate records over three inches thick into separate volumes

- Do not eat, drink or smoke near records

**Paper records in transit**

If paper records need to be transported from one clinical area to another it is the personal responsibility of the individual transporting the records to ensure their safety and security whilst in transit and ensure they cannot be accessed by an unauthorised individual at any time during transit. The following standards apply:

- Records should be handled carefully - never thrown, transported with materials that could cause risk to the records (e.g. chemicals) or exposed to weather, excessive light or risk of theft

- Records must not be transferred internally using the internal mail service as this service does not meet Trust confidentiality standards. They should be transferred using the internal courier service (man with a van / man with a car service)

- An approved courier must be used when transferring health records externally (normally TNT, Loomis or Royal Mail Special Delivery) using 'track and trace' including the provision of a signature on delivery

- Couriers transporting records for archiving / off site storage purposes must meet information governance standards

- Large quantities of health records should be boxed in suitable crates or boxes that give adequate protection. Otherwise, tamper proof envelopes or padded envelopes should be used

- All packaging should be clearly marked with the recipient's name and address. The Trust's PO Box Return to Sender address must be included on the reverse of the envelope

- All packages should be marked 'Private and Confidential. To be opened by the addressee only'

- Records in transit must be stored securely e.g. in the locked boot of a car rather than the back seat

- Where practical records should not be left unattended in a vehicle

- If it is absolutely necessary to retain records overnight in no circumstances should they be left in a vehicle. They must be kept under the same conditions of security as on Trust premises i.e. in a locked cupboard within a locked building

- Records should not be looked at in a public place

**Paper records review**

Inactive records that have reached the minimum retention period should be reviewed annually to identify the need for extended retention or destruction.

- A sticky year label should be affixed in the 'year label' box on the folder front cover at the service user's first contact with the service

- The sticker should be updated if the service user has subsequent contacts. The last contact is the date used to determine retention or destruction

- Deceased patients' folders should be marked 'Deceased' with marker pen on the front cover of the folder

- An electronic clinical system search should be undertaken annually to identify inactive and deceased patients' records. The search should be verified with the paper records before any decision regarding destruction is taken. In the same way all information about a service user should be drawn together to assist the review

- Records that have been identified as potentially reaching the end of their retention period should be listed by the local Records Manager to include:

  - Name
  - Date of birth
  - NHS number
  - Address
  - Last contact date
  - Record status – inactive or deceased

- After review the list should be updated to show those identified for destruction and those identified for extended retention (e.g. research or legal value, historical retention at the Public Records Office, identified familial illness). This should be approved by a senior clinician and documented in the record and a Do Not Destroy sticker attached to the record.

- The services' local clinical governance committee will agree destruction / extended retention. Prior to destruction this should be agreed by the Information Governance Steering Group

- On notification of final approval from IGSG record destruction should be undertaken in a secure manner. Approved contractors should be used to destroy records under secure conditions. A certificate of destruction must be obtained and permanently kept with the locality records manager