# HEALTH RECORDS POLICY
Management and Maintenance, Security, Storage, Distribution and Retention of Health Records

<table>
<thead>
<tr>
<th>Author:</th>
<th>Head of Health Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Lead Executive Director:</td>
<td>Director of Information and Digital Technology</td>
</tr>
<tr>
<td>Endorsing Body:</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Governance or Assurance Committee</td>
<td>Healthcare Quality Assurance &amp; Improvement Committee</td>
</tr>
<tr>
<td>Implementation Date:</td>
<td>November 2011</td>
</tr>
<tr>
<td>Version Number:</td>
<td>V4.0</td>
</tr>
<tr>
<td>Review Date:</td>
<td>May 2021</td>
</tr>
<tr>
<td>Responsible Person</td>
<td>Head of Health Records</td>
</tr>
</tbody>
</table>
CONTENTS

i) Consultation and Distribution Record
ii) Change Record

1. INTRODUCTION
2. AIM, PURPOSE AND OUTCOMES
3. SCOPE
   3.1 Who is the Policy Intended to Benefit or Affect
   3.2 Who are the Stakeholders
4. PRINCIPAL CONTENT
5. ROLES AND RESPONSIBILITIES
6. RESOURCE IMPLICATIONS
7. COMMUNICATION PLAN
8. QUALITY IMPROVEMENT – Monitoring and Review
9. EQUALITY AND DIVERSITY IMPACT ASSESSMENT
10. REFERENCES

APPENDIX 1 – GUIDANCE PROTOCOLS
## CONSULTATION AND DISTRIBUTION RECORD

<table>
<thead>
<tr>
<th>Contributing Author/Authors</th>
<th>Head of Health Records</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consultation Process/Stakeholders:</strong></td>
<td>• Information Governance Committee</td>
</tr>
<tr>
<td></td>
<td>• Patient Safety</td>
</tr>
<tr>
<td></td>
<td>• Quality Department</td>
</tr>
<tr>
<td></td>
<td>• Divisional Management Teams (through IGC)</td>
</tr>
<tr>
<td></td>
<td>• Health Records Managers</td>
</tr>
<tr>
<td><strong>Distribution:</strong></td>
<td>• Information Governance Committee October 2011</td>
</tr>
<tr>
<td></td>
<td>• Information Assurance Committee December 2013</td>
</tr>
<tr>
<td></td>
<td>• Information Governance Committee October 2016</td>
</tr>
<tr>
<td></td>
<td>• Information Governance Committee May 2018</td>
</tr>
</tbody>
</table>
## CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 13</td>
<td>JD</td>
<td>Policy scheduled review over due Review with service representatives to ensure compliance with PRSA</td>
<td>2.1</td>
</tr>
<tr>
<td>January 14</td>
<td>JD</td>
<td>Amendments as per IAC comments</td>
<td>2.2</td>
</tr>
<tr>
<td>February 14</td>
<td>JD</td>
<td>Amendments from IAC committee members</td>
<td>2.3</td>
</tr>
<tr>
<td>12th Feb 14</td>
<td>JD</td>
<td>Final copy distributed to Director Acute Services\Director of Public Health for approval</td>
<td>2.3</td>
</tr>
<tr>
<td>13th Feb</td>
<td>JD</td>
<td>Director of Public Health agreed as Executive Director and re-issued to IAC for final approval</td>
<td>2.4</td>
</tr>
<tr>
<td>Sept 16</td>
<td>JD</td>
<td>Major revision</td>
<td>2.5 draft 1</td>
</tr>
<tr>
<td>October 16</td>
<td>JD</td>
<td>Updated to reflect comments from key stakeholders Issued to IGC members for comment Issued to Acute Division and North and South JIBs for comments</td>
<td>2.5 draft 2</td>
</tr>
<tr>
<td>November 16</td>
<td>JD</td>
<td>Comments rcvd from above and editing and tidying of Appendix 1 Guidance Notes</td>
<td>2.6</td>
</tr>
<tr>
<td>November 16</td>
<td>JD</td>
<td>Comments received from Clinical Quality Dept regarding arrangements for record keeping audits and a change to roles of Exec Directors for Medicine and NMAHP. Submitted to Information Governance Committee 15th November 2016</td>
<td>2.7</td>
</tr>
<tr>
<td>July 2017</td>
<td>JD</td>
<td>Updated to reflect Records and Information Scheme Protocol requirements and Information Asset register</td>
<td>2.8</td>
</tr>
<tr>
<td>April\May 2018</td>
<td>JD</td>
<td>GDPR statement added into section 3 and updated name of Data Protection Act</td>
<td>2.9</td>
</tr>
<tr>
<td>October 2018</td>
<td>JD</td>
<td>Reviewed prior to publication on NHSL public website. Section 3 updated to include data protection statement.</td>
<td>3.0</td>
</tr>
</tbody>
</table>
Health Records Policy

February 2019  | JD  | CMT approval to amend policy  
|  |  | • Records belonging to Blood Transfusion and Infectious Diseases (University Hospital Monklands) must not be destroyed.  
|  |  | • A check that it does not relate to blood, tissue transplants, infectious diseases will be made. Any relevant records will then be subject to further checks and authority to destroy provided by the appropriate Director. To facilitate this a list of key words will be provided.  
|  |  |  

October 2019  | JD  | Revised guidance on changes to patient demographics.  
|  |  | Process for misfiled documents  
|  |  | Additional guidance on Transgender patients.  
|  |  |  

May 2020  | K.T  | Extended until May 2022 (COVID-19)  

1. INTRODUCTION

A record can be recorded in computerised or manual form or in a mixture of both. Data can be held on a range of media, including text, sound, image, and/or paper. Increasingly records are being kept on electronic and document management systems. Records may include such things as hand-written notes; emails and correspondence; radiographs and other imaging records; printouts from monitoring equipment; photographs; videos; and tape-recordings of telephone conversations.

- A health record has an essential role in the delivery of care to individual patients and the safe, effective and efficient delivery of patient care. The ongoing retention of a patient’s health record allows for previous history to be made available upon next attendance, as a repository for prospective notes and also for clinical governance purposes. The ways in which health records are managed, stored, filed, accessed and transported must be undertaken in a manner which is efficient and effective whilst ensuring NHS Lanarkshire’s obligation to protect patient confidentiality.
- Compliance with current data protection legislation, Public Records Act (Scotland) 2011, Caldicott Principles and NHS Scotland Information Assurance Standards.
- The health record must contain accurate patient demographics at all times and checked and updated at every point of contact. Secondary care staff must never change CHI number, Forename (given name), sex or DOB on Trakcare or the primary computer system they use.
Health Records Policy

Health Records are used for other purposes such as teaching of others, clinical supervision, research, clinical audit, as well as evidence in the event of litigation, complaints and external inspection. Patients themselves can request access to their own record(s). The process for describing this is covered by NHSL Subject Access protocol.

This policy is designed to ensure all users are clear about their responsibility and what is expected of them.

2. AIM, PURPOSE AND OUTCOMES

NHS Lanarkshire recognises

• The importance of effective Health Records Management. It will ensure that all Health Records are readily accessible and available for use, stored, distributed, archived and disposed of in accordance with current data protection legislation, Caldicott Principles and NHS Scotland Information Governance Standards and best practice.

• That every patient has the right to expect their health record to be dealt with confidentially ensuring compliance with current data protection legislation’

• Inappropriate disclosure of a health record whether deliberate or unintentional is unlawful. Any breaches will be dealt with under ‘The Effective Management of Employee Conduct policy’.

• From May 2018 data protection legislation gives individuals greater rights to restrict how we process their information, their right to data erasure and their right to data portability but not all of these are relevant to NHSL health records.

• The need for appropriate archive facilities which are provided by North Lanarkshire Council.

• Accurate patient demographics are crucial for patient communication and the importance that these are checked at all times and updated at every point of contact.

• The following demographics must only be changed by the patient’s GP CHI number, Forename (given name), sex or DOB on Trakcare or the primary computer system they use

• Transgender patients have the right to update their Health Records but also recognises the importance of maintaining relevant medical history and the additional information sharing requirements.

3. SCOPE
3.1 Who is the Policy intended to Benefit or Affect?

This policy is for all staff who use and handle health records in the course of their day to day duties. The policy does not cover records created prior to 1948. This policy excludes those records owned by Independent Contractors.

- Third party contractors acting on behalf of NHS Lanarkshire will sign a confidentiality statement ensuring adherence to this policy and to current data protection legislation.
- NHS Lanarkshire take care to ensure your personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. In order to find out more about current data protection legislation and how we process your information, please visit the Data Protection Notice on our website at www.nhslanarkshire.scot.nhs.uk or ask a member of staff for a copy of our Data Protection Notice.

3.2 Who are the Stakeholders?

The stakeholders are:

- Managers
- Clinical Staff
- Nursing Staff
- AHP staff
- Administrative staff
- Property and Support Services Staff (including PFI staff)
- Patients

Roles and responsibilities are detailed elsewhere in the policy. All other stakeholders without specific roles and responsibilities must be aware of the main principles of the policy in particular the security of the record and the patient’s right to have confidentiality respected at all times.

4. PRINCIPAL CONTENT

Additional operational guidance is available in Appendix 1

Health Records Management Policy
Health Records Policy

- All Health Records should be entered into the Board’s Information Asset Register and have an assigned Information Asset Owner.

- The Head of Health Records should be contacted in first instance for advice on how existing health records should be security classified following the Records and Information Classification Scheme (RICS) protocol.

- All new record systems created under this policy and the supporting operational guidance notes must follow the RICS protocol. The Head of Health Records must be contacted for advice and guidance.

- Every patient has the right to expect their health record to be dealt with confidentially ensuring compliance with current data protection legislation.

- The conditions for processing applied by NHSL will determine the extent of the patients rights.

- Inappropriate disclosure of a health record whether deliberate or unintentional is unlawful. Staff should ensure that they are aware of what constitutes “inappropriate access” and should never access a health record unless they have a clinical or administrative reason for doing so. This includes accessing their own record or that of a relative, even where they believe they have permission to do this. Any breaches will be dealt with under ‘The Effective Management of Employee Conduct policy’.

- The patient’s health record is a legal document and must be maintained in accordance with this policy and the standards set by the relevant clinical registration body.

- All health records must clearly identify the CHI number (and local filing number if appropriate).

- All patient demographics must be checked and updated at every attendance or contact with secondary care

- The following demographics must only be changed by the patient’s GP, CHI number, Forename (given name), sex or DOB on Trakcare or the primary computer system they use. See Transgender section below.

- Transgender patients have the right to update their Health Records but also recognises the importance of maintaining relevant medical history. See Appendix 1 section 14 for more detail.

- All Health Records must follow an agreed filing structure with documents securely filed in chronological order.
Health Records Policy

- If a document is misfiled in the health record the clinical impact must be assessed and the health record updated as per the procedure at Appendix 1 Section 13.

- All Health Records will be stored securely at all times and never in a disused building.

- All Health Records must be kept in a structured filing system.

- If appropriate they should be accessible 24/7.

- Records will be kept in accordance with current data protection legislation, which requires that personal data is not kept longer than is necessary. Retention periods for health records will be in accordance with ‘CEL 31 (2010), Annex D’.

- A system that supports such reviews will be established in all records storage locations to ensure that dated records are appropriately managed.

- In order to maximise storage space and the efficiency of retrieval records should be organised and categorised as Active, Current, Non-current and records considered to be of Archival Value.

- Records transferred to off-site storage remain under the ownership of the sender at all times and must always comply with this Policy.

- Only approved 3rd party storage contractors can be used and owners should contact Head of Health Records in first instance for advice.

- Systems should be in place to accurately track the record.

- When transporting records they must be secure, clearly addressed and not disclose personal identifiable information. See ‘Transporting Printed Matter Policy’.

- Health Records must always be available at the point of care or provided within 2 working days if the need for the health record was identified upon attendance.

- If the absence of the health record had potential to lead to a clinical governance issue then the clinician must record this on Datix.

- When a health record is not available a temporary health record must be raised which must be clearly marked as temporary. This record should contain sufficient clinical information to ensure continuity of patient care and replicate any alerts.

- In order to allow clinicians to undertake their duty of care Health Records can be taken outside the base location subject to a risk assessment and approval by the...
manager ensuring adherence to current data protection legislation, Caldicott and NHS Lanarkshire policies and procedures.

- Access to health records is covered by current data protection legislation.
- Agencies such as the Police, Health and Safety Executive, SPSO sometimes have a legal entitlement for immediate access to a record on production of the appropriate legal document.
- Only in very exceptional circumstances should the original records be released but only after the permission of the manager on-call. The Health Records Manager must be informed immediately once usual working hours commence.
- Appraisal of records will be undertaken by appropriately trained personnel. The purpose of this appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed. In the majority of cases, appraisal will apply to the entire series of records rather than being conducted on individual records.
- Additional checks prior to destruction to identify records relevant to the UK Infected Blood Inquiry are:
  - Records belonging to Blood Transfusion and Infectious Diseases (University Hospital Monklands) must not be destroyed.
  - A check that it does not relate to blood, tissue transplants, infectious diseases will be made. Any relevant records will then be subject to further checks and authority to destroy provided by the appropriate Director. To facilitate this a list of key words will be provided.
- Health records will be destroyed securely using the NHS Lanarkshire approved contractor.
- If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or the legal process completed.
- Permission to scan records must be sought from the Head of Health Records and this will ultimately require a business case to be submitted if scanning is the only option.
- Patients have the right to access their record and these requests must be handled in accordance with NHSL Subject Access Request protocol.
Health Records Policy

- If a patient requests that NHSL restrict how we process their information, their right to data erasure and their right to data portability then these types of request must be passed to the Information Governance Team

5. **ROLES AND RESPONSIBILITIES**

The management of Health Records and the confidentiality of the information contained within it is the responsibility of all staff. Accountability for Health Records Policy implementation, compliance and monitoring is as follows:

5.1 **Chief Executive**
Will ensure that there is an effective policy relating to the management of health records.

5.2 **Senior Information Risk Owner**
A Senior Information Risk Owner (SIRO) has overall responsibility for NHS Lanarkshire's information risk policy.

The SIRO is accountable and responsible for information risk across the organisation. They ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

5.3 **General Manager, eHealth\ Director of information and Digital Technology**
As the designated Senior Manager for Health Records Management, the General Manager, eHealth, will be responsible for co-ordinating the implementation of this policy throughout NHS Lanarkshire.

5.4 **Head of Health Records**
Will ensure that the policy is relevant and up to date and manage requests for right to be forgotten, restriction of processing and data portability as appropriate.

5.5 **Information Governance Manager, DPO**
Will maintain the Information Asset Register annually.

5.6 **Medical Director and Executive Director of NMAHPs NHS Board**
Health Records Policy

Have professional accountability for their respective professions and a responsibility to ensure record keeping standards for these groups of staff are in place.

5.7 The Caldicott Guardian
Is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Has responsibility for reflecting patients’ interests regarding the use of patient identifiable information.

Will act as advisor to the Chief Executive on use of patient identifiable information.

5.8 Operational Directors (Acute and Health and Social Care Partnerships)
Will oversee the effective implementation of the Health Records Policy within their area of responsibility.

5.9 Unit and Divisional General Managers/Clinical Leads/Service Managers/Senior Nurses/Operational Service Managers/Directorate Support Managers.
Are responsible for implementing the policy.

Will ensure that staff in their areas of responsibility, are aware of, and understand this policy.

Will ensure that all staff implement best practice in accordance with this policy.

Will ensure systems are in place to audit compliance with this policy using agreed core question set stored within LanQIP.

Will ensure that systems are in place to report and investigate failure to comply with this policy.

Will ensure all staff are trained in Safe Information Handling Awareness and relevant staff are trained in Records Management

Will identify Information Asset Owners

5.10 Medical, Nursing and Allied Health Professional Staff
Will ensure they adhere to the standards for record keeping as laid down by their respective professional bodies.

5.11 Administrative Support Staff
Will adhere to this policy and supporting procedures.

Will ensure that before the health record leaves their control it meets the minimum standard as laid down in this policy.
Will ensure they are adequately trained in records management.

Will ensure that demographic checks are undertaken at every contact whether face to face or on telephone or other non-face to face contact.

6. RESOURCE IMPLICATIONS

No resource implications

7. COMMUNICATION PLAN

To be deployed through Executive Directors and Divisional Management Teams.

8. QUALITY IMPROVEMENT - Monitoring and Review

Health Records audits should form a core audit in clinical governance. Each clinical group should audit its own record keeping using the core question set contained in LanQip and undertake remedial actions as required.

- Clinical note keeping
- Record keeping standards

Health Records audits should be recorded on the LanQip which enables an overview of the findings and actions to be collated for consideration by Clinical Governance Groups.

Where possible audit tools used should be standardised or contain compliance items to enable an NHS Lanarkshire compliance position to be identified. Efficient audit methodologies should be used.

9. EQUALITY AND DIVERSITY IMPACT ASSESSMENT

This policy meets NHS Lanarkshire’s EDIA

10. REFERENCES

RELEVANT REFERENCES

The Access to Health Records Act (1990)
General Data Protection Regulation (GDPR)
Health Records Policy

Public Records Act (Scotland) 2011
Scottish Government Records Management: NHS Code of Practice (Scotland)
Version 2.0 March 2010
APPENDIX 1 Operational Guidance

1. SECURITY OF THE HEALTH RECORD

- All Health Records will be stored in a structured filing system that is used to permanently store health records and facilitate their efficient retrieval and distribution.
- A register of all health records storage locations will be maintained by the General Manager.
- Such filing systems must have controls in place that ensure they are secure at all times.
- Access is restricted to authorised users.
- They are accessible in accordance with the needs of the service.
- An annual management audit to assess compliance with Health and Safety and Security and any defects rectified immediately.
- Any location where records are stored locally on a semi-permanent basis to aid convenient retrieval are subject to the same levels of security and confidentiality.
- Health records must not be left unattended while in transit.
- Records kept in any department which is not staffed constantly e.g. outpatients, should be locked away securely.
- Where records are kept in an office, the office must be locked at all times when not in use.
- Health records must be protected from damage or disclosure during estates work.
- In accordance with NHSL policy, health records must not be kept in a disused building or department.

2. MANAGEMENT AND MAINTENANCE OF THE HEALTH RECORD

- Written entries must adhere to the standards laid down by the respective professional bodies.
- Alerts should be recorded in a prominent position inside the health record.
- The cover of a health record should be robust enough to securely retain all documents filed within it.
- All documents must be securely filed in the health record.
- All health records must have an agreed structured filing system which must be followed at all times.
- All documents must be filed in strict chronological order with the most recent episode uppermost.
- A health record is considered to be full when documents can no longer be easily and securely fastened inside the notes. At that point, a 2nd or subsequent health record should be raised and cross referenced to existing volumes.
- Any health record found to contain details of belonging to another patient record will be reported using Datix and managed in accordance with the NHSL Risk Management policy.
• Health records will be audited by the relevant Clinical Groups at least annually to ensure compliance with these standards.
• Duplicate records will only be merged by designated trained staff nominated by the manager of the service.
• Whenever a health record is duplicated this will be a reportable incident using Datix.
• Positive Patient Identification must be undertaken at all times to ensure that the correct record is available and prevent duplication of records.
• Patient demographics will be maintained throughout their attendance ensuring that paper and electronic information match.
• With the exception of duplicated documentation no document should be removed from a record.

3. STRUCTURED FILING

• Each health record has a home library base location, where it is returned when it is no longer in use.
• Health records will be filed in an order that allows for easy retrieval.
• Filing system procedures will be maintained and all staff involved in the filing, storage, retrieval and distribution of records will follow these procedures at all times.
• In accordance with current data protection legislation a system of review must be established to ensure that records are not kept longer than necessary.
• In order to maximise storage space and efficiency of retrieval records should be organised and categorised into the following.

**Active Records**
Are defined as patients who are attending or are due to attend.

**Current**
Patient has attended within past 3 years but is not active at present.

**Non-current**
Patient has not attended for 3 years.

**Records considered to be of Archival Value.**
These are records that were created prior to 1948 and are outwith the scope of this policy. The Head of Health Records can provide further advice as required.

All non-current health records stored in Secondary Storage facilities remain under the control of the manager whose responsibility is to make all necessary access arrangements to ensure that records are stored in an order that allows for efficient storage, retrieval and disposal.
4. TRACKING

- Systems should be in place to accurately track the current whereabouts of the health record and must be used by users of that health record.
- Trakcare is the electronic system for tracking otherwise a tracer card should be used.
- Records must be secured and appropriately tracked when they are being transported from one location to another.

5. TRANSPORTATION

- Privacy marking should always be used on packages, carriers and purpose designed boxes used to transport records, documents or media containing person, identifiable information.
- Records sent through the internal mail system must always be put in a sealed container/bag/envelope marked ‘confidential’.
- When transporting bundles of health records these must be securely tied in a manner which prevents patient details being visible.
- The delivery address must be clearly visible and legible.

6. ACCESS TO HEALTH RECORDS (INCLUDING POLICE & SOLICITOR REQUESTS)

Access to health records is covered by the current data protection legislation, Access to Health Records Act 1990 and the NHS Lanarkshire Policy on Release of Health Records. Release of health records or their contents should only be for authorised purposes, including:

Internal
Direct patient care (subject to local access rules for sensitive health records). When a health record is required for purposes other than direct patient care, the appropriate authority should be received before release.

External
- Patient consent to release the records should be obtained. In the case of Deceased patients the legal Guardian\executor of the patient’s affairs should be obtained.
- Permission from the clinician in charge should be sought but the clinician has no right to refuse access to the whole record.
- Prior to the release of records the records should be checked for third party information. This will only be released if consent has been obtained by the third party or circumstances that requires disclosure e.g. child protection, vulnerable adults etc.
Health Records Policy

- Agencies such as the Police, Health and Safety Executive, SPSO sometimes have a legal entitlement for immediate on the day access to the records but they must always produce the appropriate legal document showing their entitlement to access. These records should also be certified as a true copy of the original.
- The original notes must be copied before being released. Health records requested under current data protection legislation and Access to Health Records Act 1990 to be supplied ensuring adherence to the prescribed timescales.
- Only in very exceptional circumstances should the original records be released but only after the permission of the manager on-call. The Health Records Manager must be informed immediately usual working hours commence.
- If in doubt advice should be sought from the Health Records Manager, Information Governance Manager and/or the responsible clinician.

7. AVAILABILITY OF HEALTH RECORDS

- Availability of Health Records is vital for patient care and it is essential that all Health Records are available for every patient event.
- Health records must be available the day before any planned care and immediately for unplanned care with an escalation procedure in place to ensure compliance with these timescales.
- If a record is not available for an episode of care because the clinician in charge may decide to raise a Datix incident, the clinician should always record in the clinical notes taken that the patient’s record was not available.
- When the health record is out with the health records library it must be held in a secure location with access to authorised personnel for retrieval within and out with usual working hours.

8. TEMPORARY RECORDS

- When a health record is not available a temporary health record must be raised which must be clearly marked as temporary. This record should contain sufficient clinical information to ensure continuity of patient care and replicate any alerts.
- A system should be in place to monitor the continued use of temporary health records.
Health Records Policy

9. MINIMUM RETENTION PERIODS

- Records will be kept in accordance with principles of current data protection legislation, which requires that personal data is not kept longer than is necessary. Retention periods for health records will be in accordance with ‘CEL 31 (2010), Annex D’.

- Facilities exist for individual Consultants to retain the health records longer than the periods set out above. Consultants wishing to do so should discuss this with the Clinical Director and Head of Health Records and make a written statement of case to the Information Governance Committee in cases of dispute.

- In accordance with current data protection legislation principles, all records will be subject to regular review to ensure that they remain appropriate for retention. A system that supports such reviews will be established in all records storage locations to ensure that dated records are appropriately managed. Where appropriate, health records should be categorised and stored as active, current, and non-current health records.

- Appraisal of records will be undertaken by appropriately trained personnel. The purpose of this appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed. In the majority of cases, appraisal will apply to the entire series of records rather than being conducted on individual records.

- Health records will be destroyed securely using an NHS Lanarkshire approved contractor who meets BS EN 15713:2009 destruction certificates obtained and retained along with a register kept of records destroyed.

- Health records should not be kept longer than necessary ensuring adherence to the relevant minimum retention periods.

- The retention status of the health record should be identified at the point at which records are being categorised as non-current.

- Health records requiring to be retained must be clearly marked by the clinician.

- A record of all health records destroyed will be maintained by the manager. Description of records, oldest date, proposer and seconder, method of destruction and if external attach certificate of destruction.

- If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or the legal process completed.

- Where records are considered to be of archival preservation the responsible manager should seek guidance from the Information Governance Committee.
outlining the reasons for their preservation and the arrangements in place for their long term storage.

10. SCANNING OF HEALTH RECORDS
Departments may consider the option of scanning into electronic format, records which exist in paper format, for reasons of business efficiency. Scanning needs to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the “Evidential Weight and Legal Admissibility of Information Stored Electronically” (BIP 0008-1:2008) and the Document Scanning: Guide to Scanning Business Documents (PD 0016:2001) which provides guidance to evaluate scanners to user requirements. The scanning process should be considered to have at least 4 stages to convert documents into ready to use electronic images. These are as follows:

- Document preparation: ensuring that the scanning process is as efficient as possible.
- Data capture: ensuring that all documents are scanned to an appropriate file type and quality.
- Quality Assurance: ensuring that all documents are captured and are legible. This may be done on a sampling basis depending on the records being scanned and should be undertaken by NHSL staff and be over and above QA undertaken by any 3rd party document scanning company.
- Indexing: ensures that the records can be retrieved.

11. RESTRICTING, DATA PORTABILITY AND RIGHT TO ERASURE

BACKGROUND
This procedure describes the processes that NHSL will follow if they receive a request from a Data Subject to have their data processing restricted, to have data portability and data erasure (referred to as right to be forgotten) by NHSL.

Person identifiable data relates to patient, staff, volunteers and other files that contain personal information about a living individual.

It is important that all risks associated with the request are assessed.

PROCEDURE
Health Records Policy

All requests must first of all be routed through the Information Governance Team who will record the request. The Information Governance Team may reject the request at this stage.

Upon receipt of the request being passed to the relevant Head of Service (HoS) they will acknowledge receipt of request within 7 days. The letter will explain that the right they are requesting may not apply. Standard letter will be used.

HoS will identify relevant records – they may need to contact the data subject for more information.

HoS will consult with the Information Governance Manager, Data Protection Officer if the requested right applies. If not HoS will inform the patient or staff member the reasons why by letter (Standard letter will be used).

HoS will in conjunction with relevant managers\clinicians assess the risk of exercising the right.

Approved

• The HoS will contact the relevant Information Asset owners asking them to take necessary steps to fulfil the request.

• The Information Asset owners will confirm that this has been completed within 21 days of the requests being received by NHSL.

• The Data Subject will be advised of the right has been enacted including any restrictions that may apply by the HoS within 30 days of the request.

Not approved

• If the risk in exercising the right will be detrimental to the data subject this will be discussed further with the Information Governance Team and if in agreement the HoS will advise the requestor of the decision and the reasons within 14 days. (Standard letter to be used)

• If the Data Subject is not happy with the response then they will be advised to utilise the Complaints Procedure and of their right to contact the Information Commissioner

12 Patient Demographic Checks

The following details must be checked by administrative staff (or clinical staff in lieu of administrative staff), at every face to face and telephone contact and on referral. The patient must be asked to provide the information to ensure security of information.
13 PROTOCOL FOR AMENDING HEALTH RECORDS AS A RESULT OF A MISFILED DOCUMENT

1 INTRODUCTION
This protocol describes the processes that should be considered and followed when a document belonging to another patient is found in another patient's health record.

2 PROCEDURE AND ROLES AND RESPONSIBILITIES

Clinician finding the document (or secretary working on behalf of consultant)
- Inform health records
- Raise a Clinical Governance category Datix

Clinician finding the document
- Review if any potential harm to their patient has resulted from the misfiled documents and action accordingly.
- Contact other patient’s clinician if result is urgent or indicates potential for harm.

Health Records
- Re-index the misfiled document to Section T misfiled document folder.
- Scan into correct record- annotate document showing scanned date to correct record and that it was previously misfiled.
- Inform responsible clinician that a new result is now in their patient’s record.
- Retain a register of all incidents.

Service Managers
- Assess for any potential information governance breach implications

14 Records of transgender (trans) patients
Changing and Storing Trans Information in Patient Records

Any protected information in the record relating to someone’s gender identity can only be shared with the express permission of the patient.
Names and titles on records can be changed upon request from the patient or GP Practice. Requests are made to Practitioner Services Division (PSD) who amend CHI, names and gender titles. A patient does not required to possess or provide a Gender Recognition Certificate (GRC) before an application is made and should not be asked. A patient’s record may hold treatment history that would disclose their trans status. For example a trans man may have a history of Gynae treatment. Placing an open alert on the medical record disclosing the patient as trans would constitute a breach of the Gender Recognition (Disclosure of Information) (Scotland) Order 2005 (unless the criteria previously mentioned had been met).

Trans people seeking to change their CHI and amend their medical records should be advised of the possible implications this may have. For instance – changing a patient’s CHI sex identifier may create some challenges for screening programmes that use CHI sex identifiers as inclusion criteria. At the moment once PSD receive notification from a patient to change the CHI they will amend the record in such a way that screening programmes will be informed that screening should be offered (i.e. trans man will be offered cervical screening). If PSD do not amend the record appropriately the onus then is on the GP Practices and other services to alert the Screening Department if patients should be offered the appropriate screening prompt and reminders. Any queries relating to Breast Screening should be directed to regional centres. NHS Inform have developed screening information for the transgender community that captures possible permutations and should remove concerns.