TRANSFER OF PERSON IDENTIFIABLE/COMMERCIALLY SENSITIVE DATA POLICY

Author:	**Head of Information Management**
Endorsing Body:	**Information Governance Committee**
Governance or Assurance Committee	**Healthcare Quality, Assurance, Improvement Committee**
Implementation Date:	**June 2024**
Version Number:	**9**
Review Date:	**May 2026**
Responsible Person	**Director of Information and Digital Technology**

NHS Lanarkshire

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• G. Johnston
Consultation Process / Stakeholders:	• Health Records Service Manager, NHSL staff via NHS Lanarkshire staff brief – March 2017 • NHSL staff via NHS Lanarkshire staff brief – February 2019 • Information Governance Group
Distribution:	

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
November 14	G. Johnson	Updated Housekeeping & change to NHSL Format	2
March 17	G. Johnson	Minor housekeeping - Explanation of abbreviation (FM)	3
July 2017	J. Duncan	Minor housekeeping – Wording changes to reflect NHSL Records and Information Classification Scheme	4
May 2018	G. Johnson	GDPR statement added into section 3 and updated name of Data Protection Act	5
February 2019	J. Duncan	Minor housekeeping - Additional wording to provide reference to use of lockable bags where appropriate	6
	G. Johnson	Wording change – delete 'Data Protection Act 1998' and 'General Data Protection Regulation 2018', replace with 'current data protection legislation'	6
March 2019	G. Johnson	Wording change - Include reference to specific data protection legislation, remove RICS acronym in section 4.1 and addition of statement requiring security alarm to be engaged added at section 4.6	7
	G. Johnson	Change title of policy from Patient Identifiable to Person Identifiable plus all associated references within policy	7
May 2020	K. Torrance	Extended until March 2022 (COVID-19)	7
March 2022	A. Topping	Change title of policy to 'Transfer of Person Identifiable/Commercially Sensitive Data Policy', additional section added to 4.7 'Use of Health Records at Home'	7
March 2022	L. Taggart	Update format to current policy template and minor wording changes	8

March 2024	L. Taggart	Changes to job titles. Change to section 4.8. Addition of section 4.9 electronic data. Formatting changes	9

1. INTRODUCTION

1.1 NHS Lanarkshire recognises the importance of ensuring that all person identifiable/commercially sensitive data is treated in a manner which maximises safety and security and minimises the opportunity for confidentiality to be compromised.

2. AIM, PURPOSE AND OUTCOMES

2.1 This document sets out the policy to be adhered to in relation to the terms of all person identifiable / commercially sensitive data. This includes:

- Mail
- Health Records
- Laboratory specimens
- Information held on CD or any other portable media

2.2 NHSL must comply with Data Protection Act 2018 & UK GDPR, the Freedom of Information (Scotland) Act 2002 and the UK General Data Protection Regulation which specifies measures which must be taken by users of information to ensure that it is acquired, held, used and transferred/disposed of in accordance with best practice.

2.3 The implementation of the policy will:

- Follow the principles of the Data Protection Act 2018 and NHS Scotland Information Governance Standards.
- Adhere to the principles of the Freedom of Information (Scotland) Act 2002.
- Adhere to the principles of the UK General Data Protection Regulation 2018
- Be subject to appropriate levels of quality assurance and monitoring.

3. SCOPE

3.1 Who is the policy intended to benefit or affect?

This Policy applies to all staff and relates to both electronic and paper records and is supported by a range of Information Governance Policies including the Transportation of Records Policy.

3.2 Who are the stakeholders?

All staff

NHS Lanarkshire takes care to ensure your personal information is only accessible to authorised people. Our staff has 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."

4. PRINCIPAL CONTENT

4.1 Principles

It is the responsibility of operational managers to ensure that the chosen delivery method is appropriate to the classification of the documents and that it is security marked in accordance with the appropriate Records Management Policy. The Information Asset owner can provide advice in this regard.

For the purpose of this policy there are two defined work areas identified:

(i) Public Accessible Areas (non-secure)
(ii) Non-Public Accessible Areas (secure)

All printed material which is being used or transported requires to be managed in accordance with a defined policy to ensure that confidentiality remains intact at all times. This document sets out:

(i) A protocol for use by all staff when issuing printed matter covering transfer of internal mail, external mail, Health Records, etc.
(ii) Optimal arrangements for the uplift, distribution and delivery of person identifiable media

4.2 General Mail

Mail will include many items of Person Identifiable Information which can safely be sent by the routine mail processes internally and externally. This will normally include items such as appointments, results, discharge letters, etc. which do not require to be double wrapped. Specific reference to Health Records is dealt with in sections 3, 4, 5 and 6. Where there is any doubt regarding the appropriateness of the arrangements being deployed there is a requirement to undertake a risk assessment before proceeding.

- Mail must never be left unattended in a non-secure area.

- Mail will be collected from agreed designated collection points within each hospital or health premises by NHS Lanarkshire portering staff (or contracted out Facilities Management (FM) staff where appropriate).

- Mail will be transported between designated collection points by NHS Lanarkshire portering staff (or contracted out FM staff where appropriate) in accordance with the agreed local delivery schedule in a secure lockable container. Mail for collection by internal portering staff may be left in an open basket if it is in a secure area i.e. not accessible by public. A risk assessment and a defined operational procedure will require to be undertaken for each designated collection point.

- In all circumstances where mail is left for collection in a non-secure or public accessible area, it must be in a secure locked box or cage that can only be accessed by designated staff.

4.3 Internal Transfer of Health Records out with NHSL

Where Health Records are being transferred on an adhoc basis by the internal portering service, this will require the submission of a portering request to PSSD via Firstport.

Health records must be transferred in secure manner, appropriate to volume of health records, (to be determined locally), which will be transported by NHS Lanarkshire administrative staff or by the general portering system.

- Health records will be collected from the designated storage location (securely tied) and transported to the relevant location.

- Records must not be left unattended in a non-secure area. Care should be taken to ensure records are not left in wheelchairs/trolleys.

- Health records sent through the internal mail system must always be put in a sealed container/bag/envelope marked "**MEDICAL IN CONFIDENCE**".

- 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. Preferably type address to avoid potential handwriting mistakes.

4.4 External Transfer of Health Records outwith NHSL

Royal Mail or equivalent

- The Health Record must be double wrapped and marked 'Medical in Confidence' on the inner envelope only.

- The Health Record must be sent using a method that records the receipt of the item e.g. Recorded Delivery. Recorded Delivery only ensures that the item has been received and a signature of receipt is obtained.

- In certain circumstances consideration should be given for the use of Royal Mail "Special Delivery". This service provides tracking of the package transit from uplift to delivery. This service should be used where the information being sent would be considered as being extremely sensitive the practitioner. This may arise in any situation, but may include child or by adult protection or mental health information. This decision should be made the practitioner based on clinical judgement.

- All records should have a "return to" address if undelivered. Preferably type address to avoid potential handwriting mistakes.

4.5 Process for ensuring safe receipt of Health Records not being sent for the purposes of appointments or admission

- Large volume of records are routinely transferred as part of the day to day function of health Records i.e. for clinics, elective admissions and emergency attendances. Where records are being transferred for other purposes the following process should be applied.

- An audit trail should be in place which ensures all records are tracked during the transportation process; the system can be paper or electronic.

- When records are being sent for purposes other than patients attendance at clinics or admission the following processes should be followed:

    - The person requesting the record will be asked to confirm that they received the record. The sender must include appropriate contact details to allow contact.
    - Where NHSL staff have instigated the sending of a record either internal or external to NHSL, the sender should ensure that the record has been received.
    - At no time should a record be sent without knowledge of the intended recipient.

4.6 Removal of Health Records from Base Location

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 appropriate manager ensuring adherence to Data Protection, Caldicott and NHS Lanarkshire policies and procedures.

Clinicians may use their own vehicles (leased or otherwise) for this purpose providing:

- The records are not visible and are carried at all times in the boot of vehicle.

- When health records are left unattended, e.g. domiciliary visit, this must be for the minimum time possible and for not longer than one hour unless exceptional circumstances apply.

- All vehicles used for this purpose should be alarmed and alarm engaged.

- Health records must not be left in vehicles overnight.

- An assessment is undertaken to determine, based on the sensitivity of documents being carried by staff, whether additional security should be provided. An example of this is lockable bags. Records should be always kept in a bag. This reduces potential for dropping paperwork outside or being blown away in the wind.

4.7 Use of Health Records at Home

- Risk assessment should be done by manager on whether records should be used at staff member’s home.

- Records being stored in the most secure location of the home and stored securely out of sight of other residents when not in use.

- Only being kept at home for necessary amount of time and returned to base site as soon as is possible.

- If using work laptop that has access to health/staff records, ensure this is also kept secure and locked when not in use.

4.8 Mail or Specimens which require to be collected by a Third Party

This applies to all items which cannot be transported within the regular mail and delivery service.

All mail or specimens which require to be collected by a third party e.g. courier; taxi driver or other NHS staff must be stored at a secure area which is accessible but remain safe. All items will be transferred in a secure wallet which is visibly securely sealed. A record will require to be kept of all items for collection which will include:

- Description of item
- Contact details of sender
- Date
- Time
- Details of party who will collect them
- Time of collection
- Signature and ID of person collecting

Items will only be released when the person collecting identifies that they are authorised to do so. This authorisation process should be recorded formally.

All NHS Lanarkshire premises will require to clearly define a collection/delivery point which will be staffed between the hours of 9.00am and 5.00pm Monday to Friday. Out with these times defined local arrangements will be required.

Additional information regarding the packaging of specimens can be found in NHS Lanarkshire Guidelines and Procedures for the safe packaging, labelling and transport of specimens.

4.9 Transfer of Electronic Records

There are a number of instances when NHS Lanarkshire will have to send sensitive data via electronic means, for examples:

- Subject Access Requests
- Court Orders
- Procurator Fiscal
- Central Legal Office
- Ombudsman

- Solicitors
- Social Work
- Other health care providers e.g. Ross Hall
- Police
- Children's Reporter
- Post Mortem
- Insurance Companies

When transferring electronic records NHS Lanarkshire's Information Security Policy for the Transfer of Data (including International Transfers) must be adhered to. This policy details the approved methods of transferring electronic records. Methods of transferring electronic records:

- SWAN Secure File Transfer Service – An IT ServiceDesk call should be logged and the SWAN Secure File Transfer Service User Guide should be followed. This is the preferred method of sharing sensitive information.
- Electronic mail - should be used in accordance with the Email Acceptable Usage Policy. Users must be migrated to M365 in order to send sensitive information. An encrypted channel must be set up, see Appendix 3 of the Email Acceptable Usage Policy.
- Sectra Image Exchange Portal (IEP) – is used primarily by the radiology/PACS department in NHSL to securely transfer images between other health boards (as well as insurance companies). The IEP solution could be used for other transfers; for further information contact the radiology/PACS or legal department.

It is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender prior to sending any sensitive data.

5. ROLES AND RESPONSIBILITIES

5.1 The transfer of person identifiable / commercially sensitive data and the confidentiality of associated information is the responsibility of all staff. Accountability for transfer of person identifiable / commercially sensitive data implementation, compliance and monitoring is as follows:

5.1.1 Chief Executive
Will ensure that there is an effective policy relating to the transfer of person identifiable / commercially sensitive data.

5.1.2 Director of Information and Digital Technology
Reporting to the Director of Information and Digital Technology, the Head of Information and Records Management and the Board Secretary, as the designated senior managers for Records Management, will be responsible for co-ordinating the implementation of this policy throughout NHS Lanarkshire.

5.1.3 Operational Directors (Acute and CHP)
Will oversee the effective implementation of the Policy within their area of responsibility.

5.1.4 Hospital Site Directors/General Managers/Clinical Leads/Service Managers/Senior Nurses

- 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 implement and maintain relevant procedure manuals.
- Will ensure that systems are in place to report, record on Datix and investigate failure to comply with this policy and those supporting procedures.
- Will identify training needs and ensure staff are appropriately trained in the transfer of patient identifiable / commercially sensitive data.

5.1.5 Administrative Support Staff
Will adhere to this policy and supporting procedures and record on Datix any information assurance breaches.

6. RESOURCE IMPLICATIONS

6.1 Any additional resource will be identified locally and will be funded locally. There is no additional staff resource required to implement this Policy.

6.2 There is a comprehensive training programme for information governance in NHSL, and the transfer of patient identifiable/commercially sensitive data will become integral to this programme and local induction/orientation.

6.3 Staff will receive further training as deemed appropriate by their departmental manager and this will be recorded in their eKSF.

7. COMMUNICATION PLAN

7.1 This policy will be managed through the Corporate Policies intranet site and will be communicated on through the Staff Briefing.

8. QUALITY IMPROVEMENT – Monitoring and Review

8.1 The Policy will be subject to review every 2 years or earlier if in response to any legislative change. A regular audit will be undertaken by the internal auditors on compliance with this Policy. The Chief Executive will be responsible for the audit arrangements through the Boards Information Governance Committee. Areas to be targeted will be in accordance with the Boards and auditors assessment of level of potential risk. The NHS Lanarkshire Risk Management Steering Group will review audit reports and action plans.

9. EQUALITY IMPACT ASSESSMENT

9.1 This policy meets NHS Lanarkshire's EQIA ☑

(tick box)

10. SUMMARY OR FREQUENTLY ASKED QUESTIONS (FAQS)

10.1 NHS Lanarkshire has a responsibility to comply with all relevant legislation that will ensure effective management of the transfer of person identifiable / commercially sensitive data, and where this is breached, will be able to report, record, investigate incidents and make improvement as necessary.

10.2 Every staff member has a responsibility to treat patient, staff, commercial and contractual information, both paper and electronic, as confidential, which means following the NHSL policies and applying good practice when accessing and managing information.

11. REFERENCES

Data Protection Act 2018
UK General Data Protection Regulation (GDPR)
NHS Scotland Information Governance Standards
HDL (2006) 28 THE MANAGEMENT, RETENTION AND DISPOSAL OF ADMINISTRATIVE RECORDS
https://www.nhslanarkshire.scot.nhs.uk/download/information-security-policy-email-acceptable-usage/
https://www.nhslanarkshire.scot.nhs.uk/download/information-security-policy-cloud-computing/
https://www.nhslanarkshire.scot.nhs.uk/download/information-security-policy-transfer-of-data-including-international-transfers/

12. CHECKLIST

To be sent to Corporate policies:-

Copy of completed policy
Copy of EQIA
Copy of assurance process document for all policies
Copy of fast-track document if applicable