Information Security Policy
Transfer of Data (including International Transfers)

Author:	**Information Security Manager** **Enterprise Architect**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Governance Committee**
Governance or Assurance Committee	**Information Governance and Cyber Assurance Committee**
Implementation Date:	**September 2010**
Version Number:	**2.6.9**
Last Review Date:	**Jan 2025**
Review Date:	**April 2027**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Information Security Manager • Enterprise Architect
Consultation Process / Stakeholders:	• Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance and Cyber Assurance Committee
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
April 2018	A Ashforth	New policy to meet requirements of General Data Protection Regulation (GDPR)	2.6
April 2018	R Hall	Combine policies for transfer of data and international data transfer	2.6.1
April 2018	A Ashforth	Simple change to advice on the use of electronic email, and added new sections for NHS SFT file transfer and Sectra Image Exchange Portal file transfer processes	2.6.2
June 2018	A Ashforth	Updated to show new director of information and digital technology	2.6.3
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.4
Sept 2018	A Ashforth	Data protection statement added into Section 3 - Stakeholders	2.6.5
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.6
June 2021	A Ashforth	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section	2.6.7
April 2024	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. Replaced 4.4 NHS Secure File Transfer with 4.4 SWAN Secure File Transfer Service. References Appendix 1 – updated.	2.6.8
Jan 2025	A Ashforth	Updated references appendix for broken link (from 'NHSL Risk Management	2.6.9

		Framework' with 'NHSL Risk Management Policy') and provided the updated link for the Scottish Government's Records Management Code of Practice. Change all references of 'IG Committee' to 'Information Governance & Cyber Assurance Committee (IG & CAC)' Change all references of 'Healthcare Quality Assurance and Improvement Committee' with 'Healthcare Governance Committee'	

1. Introduction

This policy relates to the Transfer of Data (including International Transfers) and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

To ensure that INFORMATION SECURITY is maintained

- Ensure that confidentiality and integrity of personal and sensitive information is maintained
- Ensure that information is available to ***authorised*** users
- Ensure that information is not disclosed to ***unauthorised*** people
- To prevent ***destruction*** of information

The aim of this policy is to support staff in the movement of NHS Lanarkshire (NHSL) data and the implications of moving data outside the EU.

Advise staff of their obligations to maintain information confidentiality, integrity, and availability.

This policy forms part of the Information Security Management System (ISMS) and should be read in conjunction with all the IS policies.

This policy has been written in line with the best practice for information security standards ISO 27001 and ISO 27002 and the policy will be reviewed to meet future changes to this standard.

This policy has been written to comply with current legislation and the policy will be updated appropriately to suit new and/or modified legislation. The references appendix will be updated to reflect this legislation.

3. Scope

3.1 Who is the Policy intended to Affect?

This policy is intended for all NHS Lanarkshire staff to maintain information security. In the interests of clarity all references to 'staff' includes all staff within NHS Lanarkshire and all staff who are employed, engaged or partners within each GP practice (contracted to NHS Lanarkshire).

3.2 Who are the Stakeholders

All staff.

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.

4. Principal Content

At a glance

This policy will cover both the transfer of information within and out with the European Union. GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

In brief

Requirements for Transferring Information

The sender must consider the various methods / media of transfer available and whether they are appropriate. This section lists the main methods / media and sets out any restrictions and the requirements for secure transfer of information.

For all transfers of information, it is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender.

This section defines the different methods of minimising the risks when transferring information in different ways and provides information on individual and bulk transfers.

4.1 Bulk Transfer

It is essential that all NHS Lanarkshire departments have in place systems to ensure that bulk transfers of information are appropriately controlled, implementing appropriate security measures around these transfers.

All bulk transfers must be authorised by the head of department, and they will decide whether to authorise the transfer of the information after careful consideration of the content, format and method of transfer. It will be their responsibility to inform the Information Governance Manager, and to seek their guidance where needed.

A log will be held by the Information Governance Manager of all bulk transfers of information; this will be updated as each new bulk transfer takes place.

4.2 Electronic Mail

Electronic mail should be used in accordance with the Email Acceptable Usage Policy.

Personal email accounts (e.g. Hotmail, Gmail etc.) should not be used to send information.

Even when the above conditions are met, the following points need to be adhered to:

- Ensure that the name and email address of the recipient are correct

- Email message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.

- Check with the recipient that his / her email system will not filter out or quarantine the transferred file.

- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

- Ensure the message has been received, via contacting the recipient.

- Ensure that the information within the email is stored in the agreed format for the record type i.e. in line with professional record keeping guidelines

4.3 Electronic Data Transfer (FTP (File Transfer Protocol), Secure FTP)

Standard FTP without encryption is inherently insecure and must not be used for transmitting personal information.

Secure FTP file transfers are acceptable but such transfers must be set up and administered by the Digital Department.

4.4 SWAN Secure File Transfer Service

The NHSS has a secure file transfer facility to exchange files SWAN Secure File Transfer Service, see SWAN SFT user manual on Firstport.

4.5 Sectra Image Exchange Portal (IEP)

The PACS departments in NHSL use the Sectra Image Exchange Portal (IEP) to securely transfer images between NHSL and other health boards, as well as insurance companies. IEP have a secure portal for registered staff to request images and approve images as well as uploading and downloading of images.

The IEP solution could be used for other transfers, for more details contact the PACS admins.

4.6. Encrypted USB drive

Personal Information must be enclosed in a file and encrypted using a product approved by the Information Security Manager.

- Any attachment is required to be password protected.

- Any password must be to Organisation standard. 7 characters, mix of alpha and numeric.

- Any password to open the attached file must be transferred to the recipient using a different method than email, e.g. a telephone call to an agreed telephone number, closed letter.

- An accompanying message must contain clear instructions on the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.

- An accompanying message and the filename must not reveal the contents of the encrypted file.

- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

4.7. External and Internal Post / Courier

Postal and courier services can be used to transfer personal information either in paper format or as electronic information on removable media.

There are a number of standard requirements which must be adhered to when transferring information by post or courier services. There are also additional requirements around removable media and bulk transfers.

4.7.1. Standard Requirements

- Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel

- Mark the envelope/parcel, private and confidential and add on return address details where this will not compromise confidentiality

- Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit e.g. a tamperproof wallet

- Consider use of an approved courier or secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

- An appropriate delivery method must be used.

- Package must have a return address and contact details.

- The label must not indicate the nature or value of the contents.

- Package must be received and signed for by addressee.

- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

- When sending Medical Records / Health Care Records copies should be sent whenever possible and the sender must send them in sealed double envelopes with the address on both. The private and confidential marking should only be on the inner envelope.

4.7.2. Removable Media

- Electronic personal information to be sent by post or courier, must be encrypted prior to transfer, in line with Health Board standards

- Processes must be in place for the appropriate disposal of information on the removable media once transfer is complete

4.7.3. Bulk Transfers

- When transferring bulk personal information you must use an approved courier or secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

- When transferring personal information by approved courier:

- The individual responsible for passing the information to the courier, must check the ID of the Courier and obtain a receipt from the Courier when the bulk personal information is collected

- The sender must confirm the bulk transfer has been received by contacting the recipient.

- The courier must only hand this information over to the recipient or to a nominated individual and obtain a signature when delivered

4.8. In Person

On occasions, personal information may need to be transferred in person. This may be due to the needs of the team or because this may be the most secure method of transferring the information. Examples of this include handing a patient/service user health care record over to a colleague off site, handing over an encrypted CD of personal data to another organisation etc.

Due to the number of different approaches to transferring personal information in person e.g. on foot, by car, public transport, in electronic or paper formats, it is not possible to give a definitive list of actions to be taken. However careful consideration must be given to all the potential security and confidentiality risks involved and agree and document actions to mitigate these. Much of the guidance already provided in this policy. Further advice can be obtained from the Information Governance Manager.

4.9. Fax Transmission

Fax is inherently insecure and is not recommended for transfer of personal information.

However it is acknowledged that certain circumstances demand it.

- The sender must check that the Fax number is correct and that the receiver is awaiting transmission.

- For personal information the number must be double-checked by a colleague before transmission and telephone contact must be maintained throughout transmission.

- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine and a clear requirement to securely destroy the message when no longer required.

- The message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.

- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

4.10. Text messaging (SMS), instant Messaging (IM)

Due to increased use of mobile phones, transfer of information, especially personal information, text messaging (SMS) is now being considered as a way of staff communicating with patients/service users and other staff. This method is likely to continue to increase as SMS messaging services progress but must not be used for personally identifiable information or other sensitive information unless the service has been risk assessed, approved for use and explicit consent has been obtained from the patient.

4.11. International Data Transfer

When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

What about transfers on the basis of a Commission decision?

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Relevant provisions in the GDPR - see Article 45 and Recitals 103-107 and 169

What about transfers subject to appropriate safeguards?

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Relevant provisions in the GDPR - see Article 46 and Recitals 108-110 and 114

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

According to its work plan, the Article 29 Working Party will publish guidelines on data transfers based on binding corporate rules and contractual clauses in 2017.

What about transfers based on an organisation's assessment of the adequacy of protection?

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Relevant provisions in the GDPR - see Articles 83 and 84 and Recitals 148-152

Are there any derogations from the prohibition on transfers of personal data outside of the EU?

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Relevant provisions in the GDPR - see Article 49 and Recitals 111 and 112

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);

- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Relevant provisions in the GDPR - see Article 49 and Recital 113

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance Committee

6. Resource Implications

No resource implications

7. Communication Plan

This policy will be managed through the Corporate Policies intranet site and will be announced through the staff briefing.

8. Quality Improvement – Monitoring and Review

To be reviewed at regular intervals by Information Security Manager.

9. Equality and Diversity Impact Assessment

This policy meets NHS Lanarkshire's EQIA [X] (tick box)

10. Summary of Frequently Asked Questions (FAQs)

N/A

11. References Appendix 1

The principal Acts of Parliament, Scottish Government circulars, and internal guidance documents relevant to this policy are:

- UK General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- National Cyber Security Centre Cyber Assurance Framework

- Scottish Government Public Sector Cyber Resilience Framework
- CEL 25 (2012) NHS Scotland Mobile Data Protection Standard
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- MEL 2000 (17) Data Protection Act 1998
- NHSL Risk Management Policy
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management Code of Practice for Health and Social Care
- SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000