Information Security Policy
Secure Use of Faxes

Author:	**Information Security Manager**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Quality Assurance and Improvement Committee**
Governance or Assurance Committee	**Information Governance Committee**
Implementation Date:	**February 2013**
Version Number:	**2.6.5**
Last Review Date:	**Aug 2021**
Review Date:	**Aug 2024**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Alan Ashforth, Information Security Manager, eHealth
Consultation Process / Stakeholders:	• Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance Committee members
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
Feb 2013	C Tannahill	1st draft for review	Draft
Aug 2013	C Tannahill	Initial review for publication	1.0
May 2014	C Tannahill & A Ashforth	Reviewed in view of comments	1.1
Aug 2014	C Tannahill & A Ashforth	Minor change - Reference appendix updated Minor change - some rewording throughout	2.4
Jan 2015	C Tannahill & A Ashforth	Typo section 1 and typo corrected in section heading 5.2 Receiving Confidential Information by Fax	2.5
Aug 2015	A Ashforth	Minor change - Reference appendix	2.5.1
Oct 2016	A Ashforth	Reviewed in line with SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	2.5.2
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.3
July 2017	A Ashforth & J Duncan	Minor change – Section 4 – Risk assess the faxing of RED category information	2.5.5
July 2017	A Ashforth	Minor change – Changed author to Alan Ashforth	2.5.5
April 2018	A Ashforth	Reviewed in line with General Data Protection Regulation (GDPR)	2.6
June 2018	A Ashforth	Updated to show new director of information and digital technology	2.6.1
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.2
Sept 2018	A Ashforth	Data protection statement added into Section 3 - Stakeholders	2.6.3
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.4

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 Amend Introduction at top of page 5 – add 'NHSL are in the process of phasing out Fax machines and are unlikely to approve new or replacement fax machines due to the inherent security issues posed by the use of fax.'	2.6.5

1. Introduction

This policy relates to the use of faxes for the transmission of commercially sensitive and person identifiable information. This policy forms part of the overall Information Security policy for NHS Lanarkshire (NHSL). NHSL are in the process of phasing out Fax machines and are unlikely to approve new or replacement fax machines due to the inherent security issues posed by the use of fax.

2. Aim, Purpose and Outcomes

This is an agreed set of administrative and physical security controls that have been designed to minimise the risks of breach of confidentiality or loss of information when sending or receiving personal information via Fax.

This policy will provide guidance to staff of their obligations in relation to the faxing of information.

A fax poster is provided in Appendix 3, this should be displayed at fax locations.

This policy forms part of eHealth 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

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. Information Security

- Information that has been classified as RED following the Records and Information Classification Scheme (RICS) protocol must not be faxed. Operational Managers must review and risk assess their operational processes and if it is determined that Fax is the only method available they should seek Caldicott Guardian approval. The Head of Health Records should be contacted for advice on the application of the RICS protocol.

- Do not fax personal or confidential information unless it is absolutely necessary. Where possible choose a safer method of sending information.

- If it is absolutely necessary e.g. urgent clinical purposes, confidential information can be sent and received by fax if the following procedures are followed to reduce the information security risks.

STEPS for sending information by fax

 **Classification of Sensitivity**	**Handling of faxes**
Secure - Red (Person Identifiable Information) **If Lost:** ✓ **Could cause distress** ✓ **Could identify individuals** ✓ **Could undermine confidence in service** ✓ **Could release commercially sensitive information**	 **Faxes:** In all cases Safe Haven fax machines must be located in secure areas, which have no public access, the area should be capable of being locked when unoccupied, the fax machine itself should be capable of being programmed with regularly dialed fax numbers to minimise the risk of human error. A fax which meets this criteria would be deemed to be a Safe Haven fax. A list of approved Safe Haven faxes is available on Firstport. When considering the use of a fax for transmitting information, the following questions must be asked: ✓ Have I got Caldicott Guardian approval

	✓ Do I really need to use a fax? Is there an alternative method which may be more secure - use the fax only for urgent communication. ✓ Is it really that urgent? ✓ Will normal mail be sufficient? **Handling Instructions:** ✓ If there is a legitimate need to access/share information ✓ Only send to the intended recipient who requires access to this information ✓ Check recipient phone number carefully ✓ Contact recipient to confirm fax number ✓ Get a colleague to check the fax number before sending ✓ Use NHS Lanarkshire's standard fax template cover sheet ✗ Never send to patients or wider public ✗ Do not include personal details on the front sheet
Insecure - Amber (With consent of Individual or Patient) **If Lost:** ✓ **Could cause distress** ✓ **Could identify individuals** `	**Faxes:** In all cases Safe Haven fax machines must be located in secure areas, which have no public access, the area should be capable of being locked when unoccupied, the fax machine itself should be capable of being programmed with regularly dialed fax numbers to minimise the risk of human error. A fax which meets this criteria would be deemed to be a Safe Haven fax. A list of approved Safe Haven faxes is available on Firstport. **Handling Instructions:** ✓ Faxes are professional (not personal) ✓ Agree fax is only solution for transferring information by telephone prior to sending ✓ State the number of pages being faxed ✗ Do not use faxes if the information can be transferred by a more secure method ✗ Medical records are not to be faxed
Insecure - Green (Unclassified)	

If Lost:	Faxes:
✓ **Will not cause distress** ✓ **Will not breach confidence** ✓ **Will not cause financial or other harm** ✓ **Does not refer to person's physical or mental state**	Any fax machine **Handling Instructions:** ✓ Send to anyone with a legitimate need to see information. Ensure reciepient details are correct Faxes are professional (not personal) ✓ Wherever possible, disable the fax or prevent access to it out-of-hour

5. Faxing – Good Practice

5.1 Sending Information by Fax

- ✓ Telephone the recipient of the fax to let them know that you are going to send the confidential information and confirm the number.
- ✓ Verify the correct number by sending a cover sheet first and asking the recipient to acknowledge receipt of the fax by sending it back or confirming by phone.
- ✓ Always use a fax cover sheet (appendix 2) which states who the information is for, who the information is from and your contact number.
- ✓ Anonymise information wherever possible. If information cannot be anonymised, use only the minimum amount of patient/personal details necessary for the purpose. Where possible use only an identification number.
- ✓ Double check to make sure you have dialled the correct the fax number before sending the cover sheet and information.
- ✓ Request confirmation of receipt or request a report sheet to confirm that the transmission was successful.
- ✓ If you send information to a fax number on a regular basis, complete this process by programming the number into the fax directory.
- ✓ Pre-programmed numbers should be checked periodically to ensure they remain valid or following office relocations, departmental moves or any other reorganisation.
- ✗ Try not to send faxes when the recipient's office may be closed.
- ⚠ Once the send button pressed you loose control of the fax.
- ⚠ Information faxed in error to the wrong person must be reported as a security incident to the IG Manager.

5.2 Receiving Confidential Information by Fax

- ✓ Each department should have a least one designated secure area on which to receive confidential information.
- ✓ If the fax machine is shared with several staff, and/or it is not within the user's office, the fax should be collected as soon as possible to prevent others reading the contents.
- ✓ Confidential faxes should be removed upon receipt. The documentation should be placed inside an envelope to await collection by the addressee.
- ✓ Where possible, Safe Haven fax machines should be turned off out of office hours.
- ✗ Do not locate fax macines in public areas
- ✗ Confidential faxes are not left lying around for unauthorised staff to see
- ✗ No printouts should be left unattended at the fax machine.

6. Managerial Authority

6.1 Legal

- ⚠ Faxes can be used as evidence in a court of law
- ⚠ Faxes can be released under the Freedom of Information Act (this excludes personal information)

6.2 Storage

- ⚠ Faxes should be retained in line with the NHSL Administrative Records Policy and the NHSL Health Records Policy.

7. Roles and Responsibilities

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

8. Resource Implications

No resource implications

9. Communication Plan

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

10. Quality Improvement – Monitoring and Review

To be reviewed at regular intervals by Information Security Manager.

11. Equality and Diversity Impact Assessment

This policy meets NHS Lanarkshire's EDIA [X]

(tick box)

12. Summary of Frequently Asked Questions (FAQs)

N/A

13. Appendix 1 - References

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)
- Scottish Health Competent Authority - NCSC Cyber Assurance Framework
- Scottish Health Competent Authority - Information Security Policy Framework (ISPF) 2018
- Scottish Government Public Sector Cyber Resilience Framework
- Scottish Government Public Sector Action Plan 2017-18
- 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 Strategy 2016
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012
- 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

14. Appendix 2 – Cover Sheet

Hospital Name

Tel:

Fax:

FAX MESSAGE
PATIENT INFORMATION

DATE:

TO:

FROM:

No OF PAGES INCL COVER SHEET:

PATIENT NAME:

CHI NUMBER:

HOSPITAL ID:

REGISTERED GP:

IMPORTANT INFORMATION:

The sender of this fax MUST follow Best Practice Protocols

This message is private and confidential. If you have received this message in error, please notify us and destroy this facimile

The information contained in this facsimile transmission is confidential and is intended only for the named recipient. It may contain sensitive information and if you are not the intended recipient, you must not copy or distribute the contents. If you have received this facsimile in error, please notify the sender immediately. Any unauthorised disclosure of the information in this communication is strictly prohibited and may result in disciplinary or legal action being taken.

15. Appendix 3 – Fax Protocol Poster

Are you faxing Person Identifiable Information?

YES

You must follow the Protocols listed below:

- Are you sending this fax from a designated Safe Haven
- Telephone the recipient of the fax to confirm the fax number is correct
- Request a colleague to check that the fax number entered is correct
- Ensure the fax header states who the information is for and mark it 'Private and Confidential'
- Send the fax transmission
- Ring fax recipient to confirm receipt

By following the above steps this ensures compliance with both the current data protection legislation and Caldicott Principles