Information Security Policy
Home Working

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:	**September 2010**
Version Number:	**2.6.6**
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.**
Mar 2006	A Ashforth	Revised in view of new policy template	1.0
Mar 2007	A Ashforth	Revised in view of new policy template	1.0
Sept 2010	A Ashforth	Revised in view of new policy template	2.0
May 2013	A Ashforth	Revised in view of comments	2.2
May 2014	A Ashforth & C Tannahill	Revised in view of comments	2.3
Aug 2014	A Ashforth & C Tannahill	Main change - rewording of Security Section - Transport and Storage of NHSL Equipment, Files and Paper Documents Minor change - Reference appendix updated Minor change - some rewording throughout	2.4
Aug 2015	A Ashforth	Minor change - Reference appendix	2.5
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)	2.5.1
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.2
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
Oct 2019	A Ashforth	Staff need to consider the risks of taking of written or printed materials of patients or	2.6.5

		staff home (out with of board premises) and cross reference with Home Working and Transfer Of Person Identifiable/Commercially Sensitive Data policies	
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	2.6.6

1. Introduction

This policy relates to Home Working 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 that use NHS Lanarkshire (NHSL) computers at home, by ensuring staff are aware of computer security issues. In order to protect staff and others as well as NHSL assets and systems, staff who work at home must take appropriate security measures. The security issues covered in this policy include the physical security of computer equipment, data confidentiality, and the security of NHSL office systems and network.

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

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

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

Appropriate Usage

- Should you require to work from home a laptop should be procured by eHealth using the budget code supplied by your department, this combined with an application for remote access will provide access to NHSL systems and data from home.

Security

- Files containing personal identifiable information (PII) MUST have additional protection against unauthorised access using encryption, therefore even authorised staff of encrypted media MUST NOT store or transfer PII onto non-NHSL computers or other non-NHSL devices, and not email PII to a personal email address.

- Staff may connect to NHSL network systems from home if there is a need to do so and they have been authorised to do so. You must ensure that appropriate security measures are taken to protect computers and networks from unauthorised access by taking the following actions:

    - Staff must comply with the NHSL Remote Access Policy.

    - Staff should not store your credentials together with the client device (laptop/tablet), as this defeats the aim of preventing access to the computer or NHSL network if it were stolen.

- Transport and Storage of NHSL Equipment, Files and Paper Documents:

    - When you remove equipment and data from NHSL premises you are responsible for ensuring its safe transport and storage as far as is reasonably practical. For larger equipment such as a removable hard drive or laptop, it may be necessary to leave the equipment in a car, if doing so, it should be placed in the boot and the car locked. In the case of a car which has no cover over the boot such as an estate car, the equipment should not be visible to passers-by. The storing of equipment in a car should not be for extended periods of time such as overnight, it is much safer for the portable computer to be brought into your home.

- You must take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

- Any confidential paper documents taken home must be stored in the most secure area of the home.

- Staff need to risk assess what materials containing personal identifiable information (PII) they take home (and other locations out with board premises), such as paper records, diary etc which relate to patients or staff. Also, refer to the other NHS Lanarkshire policies regarding Home Working and Transfer of Person Identifiable/Commercially Sensitive Data for further advice.

Legal Liability

There is a legal requirement for the Chief Executive to report any computer crime involving accessing illegal material to the police. Staff use of the Internet are committing a criminal offence by downloading illegal material and NHSL would be required to involve the police if such materials were found on any of its computers.

Support

The telephone help line is available during office hours. However, you will need to bring the equipment to the eHealth Department for repair.

Terminating Employment

On terminating employment with NHSL all equipment, software and information must be returned to your line manager or eHealth directly.

5. 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

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 EDIA [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:

- Home Working Policy
- Transfer of Person Identifiable/Commercially Sensitive Data Policy
- 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