Information Security Policy
Data Protection

Uncontrolled when printed

Author:	**Information Governance Manager, Data Protection Officer (DPO)**
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:	**2.6.5**
Last Review Date:	**Aug 2021**
Review Date:	**Aug 2024**

CONTENTS

Uncontrolled when printed

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Michelle Nobes, Information Governance Manager, Data Protection Officer (DPO) eHealth • 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 changes - rewording of 1 Introduction, rewording of 4.1 Data Protection in NHS Lanarkshire, insertion 4.3 The Caldicott Principles 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	M Nobes	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

Uncontrolled when printed

July 2021	A Ashforth/M Nobes	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section Roles & Responsibilities section – provided description of the Cyber Security Group. New section re NISD requirement for DPIAs inserted '4.10 Data Protection Impact Assessment (DPIA)'.	2.6.5

Uncontrolled when printed

1. Introduction

This policy relates to Data Protection and forms part of the overall Information Security policy for NHS Lanarkshire.

This is a statement of data protection policy adopted by NHS Lanarkshire (NHSL). Its purpose is to remind staff of the principles of the current data protection legislation in summary format to assist in avoiding misuse of personal information under the law. NHSL's Information Governance Manager, designated as the NHSL Data Protection Officer (DPO) can be contacted via the IT Service Desk should further clarification on any related issues be required.

NHSL requires to collect and use a variety of sensitive and personal information about people in order to operate. This information includes data on current, past and prospective staff, suppliers, clients/customers, and others with whom it communicates. In addition, NHSL handles patient data for a variety of administrative, research and medical purposes. All such personal information will be handled properly and securely no matter how it is collected, recorded and used – whether on paper, in a computer or recorded on other material.

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

To 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.

Uncontrolled when printed

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

4.1 Data Protection in NHS Lanarkshire

Information Governance can be described as a series of best practice guidelines and principles of the law to be followed by NHS Lanarkshire in using and protecting person identifiable information. These guidelines are subject to oversight via NHSL Board Committees.

Every member of staff has a responsibility to keep all personal and sensitive information secure at all times, you can do this by adhering to all organization policies, protecting information physically, practice password management, transfer information securely and report all actual and attempted breaches of security immediately.

4.2 Data Protection Principles

Principle (a) – Data should be processed lawfully, fairly and in a transparent manner in relation to individuals.

Principle (b) – Data should be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific

Uncontrolled when printed

or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Principle (c) – Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle (d) – Data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Principle (e) – data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the legislation in order to safeguard the rights and freedoms of individuals.

Principle (f) – Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.3 The Caldicott Principles

The Caldicott Guardian has responsibility at Board level for protecting patient identifiable data. In NHS Lanarkshire, the Caldicott Guardian is the Director of Public Health.

The Caldicott Principles are:

1. Justify the purpose for which the information is required.
2. Do not use patient-identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient-identifiable information.
4. Access to patient-identifiable information should be on a strict need-to-know basis.
5. Everyone with access should be aware of their responsibilities.
6. Everyone should understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

4.4 Individual Rights

4.4.1 The right to be informed

NHS Lanarkshire uses multiple ways to communicate how personal information is used, including:

Uncontrolled when printed

- A Data Protection Notice on the internet and intranet.
- Information leaflets for staff and patients.
- staff providing care who communicate verbally with patients and carers

4.4.2 The right of access

Individuals have the right to access their own personal information.

This right includes making an individual aware of what information we hold along with the opportunity to satisfy them that we are using their information fairly and legally.

Further information on subject access requests can be obtained by reading the Subject Access Protocol.

4.4.3 The right to rectification

If the personal information we hold about an individual is factually inaccurate or incomplete they have the right to have this corrected. Further guidance should be sought from the Information Governance Team.

4.4.4 The right to object

When NHS Lanarkshire is processing personal information for the purpose of the performance of a task carried out in the public interest or in the exercise of official authority, individuals have the right to object to the processing and also seek that further processing of the personal information is restricted. Provided NHS Lanarkshire can demonstrate compelling legitimate grounds for processing the personal information, for instance; patient safety or for evidence to support legal claims, the right will not be upheld. Further guidance should be sought from the Information Governance Team.

4.4.5 Other rights

There are other rights under current Data Protection Law however these rights only apply in certain circumstances. If you require further information on these rights please contact the Information Governance Team.

4.5 Legal Basis for Processing Data

NHS Lanarkshire, as data controller, is required to have a legal basis when using personal information. NHS Lanarkshire considers that performance of our tasks and functions are in the public interest. So when using personal information our legal basis is usually that its use is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.
In some situations we may rely on a different legal basis; for example, when we are using personal information to pay a supplier, our legal basis is that its use is

Uncontrolled when printed

necessary for the purposes of our legitimate interests as a buyer of goods and services.
Another example would be for compliance with a legal obligation to which NHS Lanarkshire is subject to, for example under the Public Health etc (Scotland) Act 2008 we are required to notify Health Protection Scotland when someone contracts a specific disease.

When we are using more sensitive types of personal information, including health information, our legal basis is usually that the use is necessary:

- for the provision of health or social care or treatment or the management of health or social care systems and services; or
- for reasons of public interest in the area of public health; or
- for reasons of substantial public interest for aims that are proportionate and respect people's rights, for example research; or
- in order to protect the vital interests of an individual; or
- for the establishment, exercise or defence of legal claims or in the case of a court order.

On rare occasions we may rely on explicit consent as our legal basis for using personal information. When we do this we will explain what it means to the individual, and the rights that are available to them.

4.6 Statement

NHSL will obey the law and will ensure that the organisation continues to treat personal information with due care and diligence.

4.7 Implementation (General)

NHSL will:

4.7.1 Observe conditions regarding the fair collection and use of information.
4.7.2 Meet its legal obligations to specify the purposes for which information is used within the Board's Information Asset Register, assigning the legal basis for processing personal data for each information asset in line with current data protection legislation.
4.7.3 Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
4.7.4 Ensure the quality of information used.
4.7.5 Apply strict checks to determine the retention periods for information held.
4.7.6 Ensure that the rights of people about whom information is held can be fully exercised under current data protection legislation. This information is available within our Data Protection Notice on our public website for patients and visitors, and on Firstport for staff.
4.7.7 Ensure that personal information is not transferred out with the European Economic Area (EEA) without suitable safeguards being in place.
4.7.8 Take appropriate technical and organisational security measures to safeguard personal information.

Uncontrolled when printed

4.8 Organisational Issues

4.8.1 NHSL will ensure that a full, correct and up-to-date notification is lodged in its name with the Information Commissioners Office.

4.8.2 The Data Controller for NHSL will be the Chief Executive who delegates day-to-day responsibility for the operation of data protection legislation to Executive Directors.

4.8.3 NHSL will observe the Caldicott principles and ensure that there is a nominated Caldicott Guardian (MEL 1999/19).

4.8.4 NHSL will appoint a person with specific responsibility for advising on and monitoring information governance practice including data protection within the organisation.

4.9 NHSL will ensure that:

4.9.1 That confidentially statements are a component of employment contracts for all staff.

4.9.2 Staff are appropriately trained in information governance and are supervised.

4.9.3 Anyone wishing to make enquiries about handling personal information knows whom to approach.

4.9.4 Queries about handling personal information are promptly and courteously dealt with.

4.9.5 Methods of handling personal information are clearly described.

4.9.6 A regular review and audit is made of the way personal information is managed.

4.9.7 The methods of and performance in the handling of personal information are regularly revised, assessed and evaluated.

4.10 Data Protection Impact Assessment (DPIA)

Information Asset Owners will ensure that any new or substantially changed use of personal data (such as a new or upgraded clinical system, new business process using patient or staff information) will be subject to a Data Protection Impact Assessment using the nationally agreed template and consulting the Data Protection Officer (DPO) as appropriate. The DPO will validate the impact statement contained in the DPIA regularly based on the review date of the DPIA. All contracts with external suppliers and contractors who process patient or staff personal data on behalf of NHS Lanarkshire will be subject to a Data Processing Agreement (DPA) compliant with GDPR article 28, based on the nationally agreed template.

Uncontrolled when printed

5. Roles and Responsibilities

All staff working within NHS Lanarkshire are bound by a legal duty of confidence to protect and keep up to date personal information that they may come into contact with during the course of their work. This is both a legal and contractual responsibility and also requirement under the common law duty of confidence.

In order to ensure both new and current staff continue to receive appropriate training in data protection and confidentiality, NHS Lanarkshire will ensure there is a comprehensive training and awareness programme in place.

Person identifiable information is anything which contains the means to identify an individual, such as name, address or CHI number.

Confidential information within the NHS is commonly thought of as health data and can include information that is private and not public knowledge, or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records and occupational health records.

Information can relate to patients and staff, including temporary staff, however stored. Information may be held in many formats including paper, CD/DVD, USB sticks, computer file or printout and mobile devices.

The following staff within NHS Lanarkshire have a responsibility to protect data:

5.1 Chief Executive

The Chief Executive is the Accountable Officer for all the organisation's information assets and its security, including but not restricted to any personal (staff and patient) or confidential information.

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 eHealth/Director of Information and Digital Technology

The eHealth/Director of Information and Digital Technology sets the conditions for the operation of a Data Protection Function for the organisation as a whole. To ensure that the Data Protection Function abides by Corporate Governance rules and ensure that it is adequately resourced and supported.

Uncontrolled when printed

5.4 Caldicott Guardian

The Caldicott Guardian has responsibility at Board level for protecting patient identifiable data. In NHS Lanarkshire, the Caldicott Guardian is the Director of Public Health.

5.5 Information Governance Committee

The Information Governance (IG) Committee is a standing committee reporting to the Healthcare Quality Assurance and Improvement Committee, and, ultimately is accountable to the Lanarkshire NHS Board. Its purpose is to support and drive the broader Information Governance agenda and provide the Board with the assurance that effective Information Governance best practice mechanisms are in place within the organisation.

5.6 Cyber Security Group

The Cyber Security Group is a sub-group of the Information Governance Committee (IGC), with the primary purpose of providing oversight, scrutiny and assurance of Cyber Security within NHS Lanarkshire. Specifically, the Cyber Security Group will: be responsible for reviewing the processes and procedures within eHealth and across NHSL to ensure that all systems are securely managed through the IG Committee in accordance with the Information Security Management System (ISMS).

5.7 Information Governance Team & Data Protection Officer

The Information Governance Team and Data Protection Officer provide advice and guidance on compliance with current data protection legislation and associated information governance law. NHS Lanarkshire has an Information Governance Committee meeting which meets every six weeks. Formal notes are produced and can be found on Firstport.

5.8 Information Security Manager

The Information Security Manager will provide technical expertise on the security of Information systems and equipment.

5.9 Freedom of Information Team

The Freedom of Information Officer handles all Freedom of Information requests on behalf of NHS Lanarkshire.

5.10 Information Asset Owner

Uncontrolled When printed

Information Asset Owners are senior members of staff whose business areas use one or more registered NHS Boards Information Asset. Their role is to understand what information is held, what is added, what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information, and ensure that it is fully used within the law for the public good.

5.11 All staff

All staff have a responsibility to ensure that they comply with the principles of data protection and Caldicott. This must be done by adhering to Information Governance and Information Security policies.

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 Infrastructure Operations Manager (Security).

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:

- 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

Uncontrolled when printed

- 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

Uncontrolled when printed