Data Protection Policy

Title: **Data Protection Policy**			
Date effective from:	June 2022	**Review date:**	June 2025
Approved by:	Policy Approval Group		
Approval Date:	7 June 2022		
Author/s:	NHS Lothian Data Protection Manager		
Policy Owner:	Information Governance and Security Manager		
Executive Lead:	Executive Medical Director		
Target Audience:	All NHS Lothian staff		
Supersedes:	Data Protection Policy v3.1 (2018)		
Keywords (min. 5):	Data, protection, information, records, breach, Caldicott, legal, controller		

Data Protection Policy

Version Control

Date	Author	Version/Page	Reason for change
Jan 2018	NHS Lothian Data Protection Manager	v3.1	Approved by Information Governance Sub-Committee
June 2022	NHS Lothian Data Protection Manager	v4.0	Approved by Policy Approval Group

Executive Summary

NHS Lothian is required to process a large variety of personal data in order to carry out its statutory functions. NHS Lothian processes patient and carer data for healthcare related purposes, including provision of care, administration of healthcare services, teaching and research. Personal data is also held on current, past and prospective employees, suppliers, and others with whom it communicates. All such this policy outlines NHS Lothian intention to process personal data professionally and securely regardless of how the data is collected, recorded and used – whether on paper, in a computer system or recorded on other media.

NHS Lothian will ensure appropriate Data Protection Impact Assessment(s) are completed with any new use of personal data is proposed. This will ensure all aspects of the processing are considered and risks are documented and where necessary address before the commencement of processing.

When data sharing is necessary NHS Lothian will ensure appropriate Data Sharing or Data Processing Agreement are in place documenting the processing taking place.

NHS Lothian complies with Data Protection legislation and will ensure all data is processed respectfully and in accordance with the law.

Data Protection Policy

Contents

1.0 Purpose

The purpose of this policy is to detail how NHS Lothian needs to process a variety of personal data in order to carry out its statutory functions. NHS Lothian processes patient and carer data for a variety of healthcare related purposes including provision of care, administration of healthcare services, teaching and research. Personal data is also held on current, past and prospective employees, suppliers, and others with whom it communicates. All such personal data will be dealt with properly and securely no matter how it is collected, recorded and used – whether on paper, in a computer system or recorded on other media.

NHS Lothian will observe the requirements of Data Protection Legislation when processing personal data. NHS Lothian will ensure that the organisation continues to treat personal data with due care and diligence.

2.0 Policy statement

- NHS Lothian will:

- Observe, fully the conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply checks to determine the length of time information is held.
- Ensure that the rights of people about whom personal data is held can be fully exercised under the Act. These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.
- Ensure Data Protection Impact Assessment(s) are undertaken when any new use of personal identifiable data is proposed.
- Where necessary ensure appropriate Data Sharing and Data Processing Agreements are in place with trusted partners.
- Ensure that personal data is not transferred out with the UK without suitable safeguards.
- Take appropriate technical and organisational security measures to safeguard personal data.
- All Information Assets should be logged in the organisations Information Asset Register.

2.1 Organisational Issues

- NHS Lothian will ensure that a full, correct and up-to-date notification is lodged in its name with the Information Commissioner.
- The Data Controller for NHS Lothian will be the Chief Executive, who will delegate day-to-day responsibility for the operational application of the Data Protection Legislation to the Executive Medical Director.
- NHS Lothian will observe the Caldicott principles and ensure that there is a nominated Caldicott Guardian.
- NHS Lothian employ a Data Protection Officer suitably qualified with specific responsibility for advising on, and monitoring data protection practice in the organisation.

NHS Lothian will ensure that:

- Everyone processing personal data understands that they are contractually responsible for following good data protection practice is appropriately trained to do so and provided with appropriate support.
- Anyone wishing to make enquiries about processing personal data knows whom to approach.
- Enquiries regarding processing personal data are timeously dealt with in line with Data Protection Legislation.
- Methods of processing personal data are clearly defined and reviewed regularly to ensure best practice guidance is followed within the organisation.
- A regular review and audit are made on the ways data are processed.
- When sharing information with Public Authority or voluntary partners, or when required for statutory purposes, this is managed in accordance with the NHS Lothian Information Sharing Protocols. Where deemed appropriate by managers, breaches of the Data Protection Act 2018 and associated policy may result in action being taken through the current Disciplinary Policy.

3.0 Scope

This policy applies to all staff working for or on behalf of NHS Lothian. Temporary and agency staff, volunteers, contractors, students and work experience personnel will also be expected to ensure compliance with this policy.

The Data Protection Policy covers the following areas to set out the approach to Information Governance in NHS Lothian:

- Statement of intent
- Responsibilities for Information Governance
- Guidance to all aspects of data processing.

4.0 Definitions

Information Governance Principles:

NHS Lothian recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. NHS Lothian fully supports the principles of corporate governance and recognises its public accountability but equally places importance on the confidentiality and security of personal information regarding patients, staff and the population, and commercially sensitive information.

NHS Lothian also recognises the need to share patient information with other healthcare organisations and outside agencies in a controlled manner which is consistent with the interest of individual patients, the health of the people of Lothian and, in some circumstances, the public interest.

NHS Lothian believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are four key inter-linked strands to Information Governance:

- Openness
- Confidentiality
- Information Security
- Quality assurance

5.0 Implementation roles and responsibilities

5.1 Chief Executive

This policy is authorised by the Chief Executive as the officer responsible for the duties of the employer under legislation

The Chief Executive has overall responsibility for ensuring that an organisational structure and effective arrangements exist to ensure the compliance of data protection legislation

This will include responsibility for:

- The staff employed within NHS Lothian
- The work processes, activities and systems performed within NHS Lothian

5.2 Executive Medical Director

The Executive Medical Director is responsible for the following:

- Ensuring that the provisions of this policy are implemented throughout the organisation.

- Ensuring through the various line management structures and the NHS Lothian Staff Governance Committee that the NHS Lothian Board is meeting all its legal obligations.

5.3 Senior Information Risk Owner

NHS Lothian's Senior Information Risk Owner will implement and lead the information governance risk assessment and management processes and advise the Board on the effectiveness of information risk management across the organisation.

5.4 Digital Department

Implementation of this policy will follow continued good practice as outlined in the appendices. NHS Lothian Digital Department will provide a compliance and advice to support the organisation, this will include the statutory requirement of a Data Protection Officer post and service

5.5 Line Managers

All line managers should have local dissemination and implementation plans in place to ensure all staff who need to interact with identifiable data, manual, IT or other electronic equipment are familiar and adhere to all aspects of this policy.

All line managers should have local dissemination and implementation plans in place to ensure all staff are familiar with and adhere to all aspects of this policy. This includes non-clinical areas and non-clinical staff at all locations within NHS Lothian.

5.5.1 Good Practice for Managers

Has identified the staff in his or her area to whom this policy applies and has given the policy (or selected excerpts) to them.

Has assessed the impact of the policy on current working practices and has an action plan to make all necessary changes to ensure that his or her area complies with the policy.

Has set up systems to provide assurance to him or her that the policy is being implemented as intended in his or her area of responsibility.

5.6 All staff

Information Governance and Security training will be provided as part of the mandatory induction program for new NHS Lothian employees.

All staff must attend mandatory updates every 24 months. Included in this is the Information Governance module, which ALL staff must complete.

Unauthorised breaches of IT security policy will be taken very seriously and may result in an investigation into the alleged breach, and may result in disciplinary action in accordance with NHS Scotland Workforce Conduct Policy

5.6.1 Good Practice for Employees

Has read the policy (or selected excerpts) and considered what it means for him or her, in terms of how to conduct his or her duties.

Has completed any mandatory education or training that may be required as part of the implementation of the policy.

Has altered working practices as they expected by the policy

5.7 Records Management Plan

NHS Lothian has a Records Management Plan, and the Corporate Records Manager will submit to The Keeper of the Records when required. This plan sets out the overarching framework for ensuring that NHS Lothian's records are managed and controlled effectively, and commensurate with the legal, operational and information needs of the organisation.

6.0 Associated materials

In conjunction with the Data Protection Legislation, NHS Lothian will apply the Principles of Caldicott, IT Security, Information Sharing, Confidentiality, social media and Records Management as defined in their supporting Policies and Protocols to meet the Information Governance standards as prescribed by Scottish Government.

Subject Access Policy

Access to Health Records further guidance

Parental Responsibility

Processing Access Requests

Staff files process

Safe Transfer of Health Records

Consent to Process Personal Data

Personal Data Breach Flowchart

Warnings and Alerts Policy (Available on the NHS Lothian Intranet)

Data Protection Impact Assessment Form/Guidance

Data Sharing and Data Processing Agreements/Guidance

7.0 Evidence base

Access to Health Records Act 1990

Data Protection Act 2018

UK General Data Protection Directive (GDPR) 2016

Human Rights Act 1998

Computer Misuse Act 1990

Network and Information Systems regulation 2018

Public Records (Scotland) Act 2011

Disposal of Records (Scotland) Regulations 1992

Freedom of Information (Scotland) Act 2002

Scottish Government Records Management Health and Social Care Code of Practice 2020

Scottish Health Memorandum 60 of 1958 (SHM58/60)

MEL (1993)152 – Guidance for Retention and Destruction of Medical Records

NHS (Scotland) HDL (2006) 41 - NHS Scotland Information Security Policy

The Management, Retention and Disposal of Administrative Records HDL (2006) 28

8.0 Stakeholder consultation

NHS Lothian consultation groups for this policy will be Information Governance Working Group and Digital & Innovation Executive Team.

A draft version of this policy was placed on the NHS Lothian Consultation Zone to give all NHS Lothian staff the opportunity to provide comment/feedback.

9.0 Monitoring and review

The strategic direction for Information Management and Information Governance will be set out in the Information Governance Working Group and eHealth Executive Team. The Digital Oversight Board, accountable to NHS Lothian Board will have overarching responsibility for monitoring the strategy and for ensuring that NHS Lothian has effective policies and management arrangements in place, which cover all aspects of Information Governance.

Assessments of compliance with relevant information governance standards will be undertaken each year, and an appropriate information governance improvement plan will be produced as a result. Delegated responsibility for overseeing the Information Governance Strategy, Policy and Implementation plan sits with the NHS Lothian Digital Oversight Board chaired by the Director of Digital. This group will secure the necessary resources to implement the Information governance action plan and will monitor activities and annually report progress to The Healthcare Governance Committee. Full terms of reference will be available on NHS Lothian Intranet.

The Executive Medical Director and Caldicott Guardian, is the named executive director on the Board with responsibility for Information Governance. The Director of Public Health & Health Policy is the designated interim Senior Information Risk Owner (SIRO) delegated responsibility for implementation and monitoring of the Information Governance Action plan which sits with the Information Governance and Security Manager.

Regular monitoring of compliance with this policy will be performed via National and local audits both internally and also by external contractors.

The effectiveness of this policy may also be monitored and evaluated using outputs from the following:

- IT Security investigations
- SAE reviews
- DATIX investigations
- Complaint investigations
- Regularly scheduled internal and external audits
- Staff feedback via conversations, queries, compliments & complaints
- Information Governance Working Group and also the eHealth Executive Team.
- Post training feedback from staff

This policy, and its associated materials, will be reviewed every 3 years, as a minimum, or as a result of any changes in legislation, guidance, as the result of inspection or audit, or any other factors which may render the policy in need of earlier review.