NHS Lothian Digital IT Security Policy

Title: NHS Lothian Digital IT Security Policy			
Date effective from:	June 2022	**Review date:**	June 2025
Approved by:	NHS Lothian Policy Approval Group		
Approval Date:	7 June 2022		
Author/s:	NHS Lothian IT Security Manager		
Policy Owner:	NHS Lothian Information Governance and Security Manager		
Executive Lead:	NHS Lothian Executive Medical Director		
Target Audience:	All staff, contractors or volunteers working for, or on behalf of, NHS Lothian		
Supersedes:	eHealth IT Security Policy v2.5.14 Nov 2020		
Keywords (min. 5):	Data, protection, IT, digital, security, Digital & IT, information, controller, cyber		

NHS Lothian Digital IT Security Policy

Version Control

Date	Author	Version/Page	Reason for change
Nov 2020	NHS Lothian IG Working Group	v2.5.14	Technical update authorised by Director of Digital & IT
May 2022	NHS Lothian IT Security Manager	v2.6	Under review
June 2022	NHS Lothian IT Security Manager	v3.0	Approved by Policy Approval Group

Executive Summary

The Digital IT Security policy exists to comply with NHS Scotland Guidance in addition to ensuring that NHS Lothian continues to treat IT assets and personal identifiable data with due care and diligence.

All staff using IT should understand that they are contractually responsible for following good IT security practice, are appropriately trained, and know where to locate appropriate support. This policy applies to all staff employed by NHS Lothian, including agency and bank staff, all students, volunteers and agency and contractors working on behalf of NHS Lothian.

The policy ensures that:

- appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems; and
- all employees are aware of the limits of their authority and the levels of their accountability for their actions.

Contents

1.0 Purpose

The purpose of this policy is to protect NHS Lothian's information assets from threats, internal or external, deliberate or accidental.

Its objectives are to ensure that:

- All Information Technology (IT) systems used in NHS Lothian are properly assessed to ensure that corporate procedures, responsibilities and IT security objectives, in particular the legal requirements, are fully met
- Appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems
- All employees are aware of the limits of their authority and the levels of their accountability for their actions

Further guidance on the four security principles is given in the NHS Scotland Information Security Policy

2.0 Policy statement

NHS Lothian processes patient and carer personal data for a variety of healthcare related purposes including provision of care, administration of healthcare services, teaching and research, and in order to carry out its statutory functions. 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.

Under Data Protection Legislation, NHS Lothian, as a Data Controller, is responsible for the maintenance and security of all personal identifiable data and records it holds on any media including health and staff records; *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." (DPA, 2018)*

Information Security, within the NHS in Scotland, is managed as part of its commitment to Information Governance, which is an integral part of Clinical Governance. Adherence to this policy will ensure that the minimum requirements are always met and, where possible, meet the highest levels recommended.

NHS Lothian is, as an employer, committed to providing its employees a working environment safe from bullying, harassment or threat and is obliged to set an example in the manner in which it protects its assets and contributes to that role.

NHS Lothian will facilitate the implementation and use of Office 365 as part of the Scottish national tenancy, providing applications, communications, cloud services, device management and security.

This policy addresses four fundamental security principles

- Authority

- Accountability
- Assurance
- Awareness

The Digital IT Security policy exists to comply with legislation and NHS Scotland guidance to ensure that NHS Lothian continues to treat IT assets and personal identifiable data with due care and diligence.

NHS Lothian Digital Security policies will ensure that:

- Confidentiality of information, required through regulatory and legislative requirements, will be assured
- Integrity of information will be maintained
- Information will be available to authorised personnel, as and when required
- Regulatory and legislative requirements will be met
- Business Continuity Plans will be produced, maintained and tested
- Information security training will be available to all staff
- All breaches of information security, actual or suspected, will be reported to and investigated by an IT Security Officer
- Appropriate technical and organisational security measures are implemented to safeguard personal data

NHS Lothian follows the guidance of HDL (2006) 41, in that it focuses on:

- Developing a security culture through training and awareness events and by providing awareness education and training materials
- Adhering to Scottish, UK, and European policy, standards and best practice guidelines for security and data protection in the NHS
- Managing Incident Reporting, so that all security incidents are reported and recorded using an Incident Reporting Form

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.

3.0 Scope

This policy applies to all health, personnel, finance or any other information held on electronic media or written on paper including all associated hardware.

Data and information take many forms, including but not limited to, data and metadata stored on emails, system and Internet access logs, network areas, computers (including cloud storage), transmitted across networks, printed out or written on paper, sent by fax, stored on devices (including mobile devices) CD, DVD, USBs, tapes, phones, tablets or spoken in conversation, including over the telephone.

It is the responsibility of each employee, contractor or volunteer working for, or on behalf of NHS Lothian, to adhere to this policy.

NHS Lothian will be responsible for the introduction and maintenance of the NHS Lothian Digital IT Security Policy and providing advice and guidance on its implementation and content.

4.0 Definitions

4.1 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, members of the public, and commercially sensitive information.

NHS Lothian also recognises the need to share patient information with other healthcare organisations and external 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 quality 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

4.2 Data Protection Legislation

This includes but is not limited to UK Data Protection Act and the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data must follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently.

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

4.3 Office 365 (O365)

This is an IT platform that exists as part of the Scottish national tenancy, providing applications, communications, cloud services, device management and security.

5.0 Implementation roles and responsibilities

5.1 NHS Lothian 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 compliance with Data Protection legislation.

This will include responsibility for:

a) The staff employed within NHS Lothian

b) The work processes, activities and systems performed within NHS Lothian

5.2 NHS Lothian Executive Medical Director

The Executive Medical Director is responsible for ensuring that:

- the provisions of this policy are implemented throughout the organisation.
- 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 (SIRO)

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 Managers

Implementation of this policy will follow continued good practice as outlined in documents listed in section 6 of this policy. NHS Lothian Digital Department will provide compliance and advice regarding this policy to support the organisation This includes 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 with, and adhere to, all aspects of this policy. Line managers are directly responsible for implementing this policy within their business areas, and for adherence to the policy by their staff. This includes all clinical and non-clinical areas, and all clinical and non-clinical staff at all locations within NHS Lothian.

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

It is the responsibility of each employee, contractor or volunteer working for, or on behalf of NHS Lothian to adhere to this policy.

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.

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 Training

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

Additionally, all staff must undertake mandatory training updates every 24 months. Included in this is the Information Governance module, which ALL staff must complete.

6.0 Associated materials

In conjunction with Data Protection Legislation, NHS Lothian will apply the Caldicott Principles, and the principles relating to IT Security, Information Sharing, Confidentiality, Social Media, and Records Management, as defined in their respective policies and associated materials, to meet the Information Governance standards as prescribed by the Scottish Government.

This policy, and its associated materials, set out specific controls and standards by which the aims of the policy are met. It also has a number of guidance documents which enable users to adhere to the policies by following the guidance.

NHS Lothian Access to Applications and Network Policy

Email: Acceptable Use

Internet: Acceptable Use

Computer Device Controls, including Generic workstations

Contractor Accounts Removal Process

Remote Access Guidance, including University of Edinburgh and other organisations

Mobile Computing Devices, including Laptops, Tablets, Phones, Wireless Devices and Removable Media

Removal of PCs, for investigation or quarantine of server as evidence

Data Access for Research Policy

Data Access Policy

RHCYP and DCN Internet Access Loan Devices Policy

Information Security Management System (ISMS) Policy

Information Risk Management Policy

Wireless Radio Appropriate Use

Secure Storage Disposal and Destruction of Electronic Equipment

NHS Lothian Staff Guide to Digital Security Policies

Research Data Storage

Safe Email Transmission

NHS Lothian Data Protection Policy

NHS Lothian Confidentiality Policy

Clinical (Patient) Photography and Video Policy

Social Media Policy

NHS Scotland Workforce Conduct Policy

System Name System Security Policy

Data Access for Research, support documents

7.0 Evidence base

Scottish Government Cyber Resilience

https://www.healthca.scot/

ISO/IEC 27005:2018, Information technology Security techniques: Information security risk management

National Cyber Security Centre (NCSC) Risk Management Guidance

National Cyber Security Centre (NCSC) Cyber Essentials

Cyber Resilience: Public Sector Action Plan

Association of Chief Police Officers' (ACPO) Good Practice Guide for Computer-Based Electronic Evidence v4

National Police Chiefs' Council (NPCC)

NHS Digital: NHS Wi-Fi

Sharing workplace wireless networks guidance, UK Government

Network and Information Systems Regulations (NISR) 2018, UK Government

NHS Scotland National ICT Infrastructure Standard

NHS (Scotland) HDL (2006) 41

NHS Scotland Information Security Policy

Caldicott Principles

Protecting Patient Confidentiality, Confidentiality and Security Group Scotland (CSAGS) Report 2001

CEL 25 (2011) Safeguarding the confidentiality of personal data processed by third party contractors

Records Management: Health and Social Care Code of Practice (Scotland) 2020, Scottish Government

CEL 25 (2012) NHS Scotland Mobile Data Protection Standard

Network and Information Systems Regulations 2018

Data Protection Act 2018

Computer Misuse Act 1990

Civic Government (Scotland) Act 1982

Copyright Design and Patents Act 1988

Defamation Act 1996

Obscene Publications Act 1964

Civil Contingencies Act 2004

Freedom of Information Act (Scotland) 2002

Human Rights Act 1998

Public Records (Scotland) Act 2011

Regulation of Investigatory Powers (Scotland) Act 2000

8.0 Stakeholder consultation

NHS Lothian colleagues from the Information Governance Working Group and Digital & IT Executive Team were consulted in the review of this policy.

A draft version of this policy was placed on the NHS Lothian Consultation zone to give all NHS Lothian staff an 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 Digital & IT 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 Digital & IT 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.