Information Security Policy

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 and Cyber Assurance Committee**
Implementation Date:	**September 2010**
Version Number:	**2.6.7**
Last Review Date:	**Oct 2023**
Review Date:	**Nov 2026**

CONTENTS

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

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
June 2010	A Ashforth	Revised in view of new policy template	1.3
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 Responsibilities – All Staff – bullet point 5 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) including:- • Added additional explanation of Caldicott Guardian role • Added new role of Senior Information Risk Owner • Added new role of Information Governance Manager • Replaced role of Data Owner with Information Asset Owner • Added new appendix – Assigned Roles Appendix 2	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 Responsibilities section - provided description of the Cyber Security Group. Responsibilities section - provided more detailed description of IG Committee. Assigned Rolls section - updated name of Chief Executive. Added new Appendix 3 - Governance Committee Structure. Added new Appendix 4 - eHealth Governance Structure/Topology.	2.6.5
Mar 2022	A Ashforth	Update Caldicott Guardian on Page 16	2.6.6
Oct 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. References Appendix 1 – updated. Assigned Roles Appendix 2 - name of Chief Executive updated. Digital Cyber Security Structure Appendix 4 - updated.	2.6.7

1. Introduction

This policy relates to Information Security policy 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

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

This policy forms part of the 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

Overview

The purpose of information security is to ensure business continuity and manage risk by minimising the likelihood and impact of security incidents. Information security enables information to be shared while ensuring the protection of information assets.

Information takes several formats; it can be stored electronically, transmitted across IT networks, printed out or written down on paper. From an information security perspective, appropriate protection should be applied to all forms of information stored including paper-based information, computer databases, portable and fixed IT media and any other methods used to communicate information.

This policy sets out clear Management direction and support for information security at NHS Lanarkshire in accordance with business requirements, legislation, regulations, standards and guidance.

It demonstrates Management support for, and commitment to, information security through issuing this policy for user acceptance and compliance, as well as any related policies, procedures and guidelines, including user education and awareness across NHS Lanarkshire.

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

Applicability and scope

Applicability

This policy applies to all electronic information assets held by NHS Lanarkshire and is intended to be fully consistent with the Information Security Policy and Standards of NHS Scotland.

This policy applies to all staff who undertake work for NHS Lanarkshire or use any part of the IT infrastructure, whether as an employee, a student, a volunteer, a contractor, partner agency, external consultant or 3rd party IT supplier.

Scope

Management require that all NHS Lanarkshire information assets are properly safeguarded against breaches of confidentiality, integrity and availability.

To achieve this, the following attributes will at all times be in place with respect to matters relating to information assurance:

- Information Security Policy, objectives, activities and improvements will be aligned with the business objectives and organisational culture of NHS Lanarkshire and meet the requirements of ISO/IEC27002, the Code of Practice for Information Security Management.
- A risk based approach to Information Security will be maintained enabling informed decisions on information security initiatives and ensuring that budget and resources are focussed appropriately. These security initiatives will meet the following objectives:
    - prevention of incidents via the identification and reduction of risks;
    - detection of incidents before damage can occur;

  - recovery from incidents via containment and repair of damage and prevention of reoccurrence.

- Information security will be promoted at all levels of the business through comprehensive user awareness education and training.
- Management will actively support information assurance initiatives, ensure they remain abreast of the risks to information assets and champion the continual improvement of information security at NHS Lanarkshire.
- An effective Information Security Policy and corresponding security operating procedures will be maintained ensuring that:
  - all information assets are protected against unauthorised access and disclosure;
  - confidentiality of information will be assured at all times;
  - integrity of information will be maintained at all times;
  - business requirements for availability will be met;
  - breaches of security both actual and suspected are reported and investigated;
  - classification and ownership of information assets will be applied; and
  - regulatory and legislative requirements will be met, including compliance with current data protection legislation

Responsibilities

Chief Executive

Final responsibility for the secure operation of all systems used to process information in NHS Lanarkshire is vested in the Chief Executive. This responsibility is delegated to all staff developing, introducing, managing and using information systems in accordance with this policy. The Chief Executive is ultimately responsible for accepting the residual risks evaluated by the information risk management process.

Caldicott Guardian

The responsibility for protecting the confidentiality of person identifiable information rests with the NHS Lanarkshire Caldicott Guardian.

This is an advisory role and the conscience of the organization, and a focal point for patient confidentiality & information sharing issues.

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.

Information Governance Manager

The Information Governance Manager will provide strategic leadership for Information Governance across NHS Lanarkshire, providing assurance to the NHS Board regarding the performance of NHS Lanarkshire in line with governance and accountability structures.

She/He is responsible for leading and developing Information Governance and Data Protection management within the broad national and local framework, which includes the confidentiality and safety of patient and staff information.

Data Protection Officer (DPO)

The DPO is responsible for ensuring that:

- A register of all NHS Lanarkshire information assets is maintained. The register will record the data owners and identify those assets that are confidential or sensitive as defined in Data Protection legislation and Caldicott guideline.
- Ensuring that NHS Lanarkshire lodges a full, correct and up-to-date notification in its name with the Information Commissioner to comply with current data protection legislation
- Advising on and monitoring data protection practices in NHS Lanarkshire.
- Assisting the organisation with their responsibilities in relation to Data Protection.
- Undertaking regular audits of how personal information is handled is carried out.

Information Security Manager

The Information Security Manager for NHS Lanarkshire is responsible for:

- Ensuring that all Information Security Policies are implemented and enforced throughout the NHS Lanarkshire.
- Ensuring that System Security Policies (SSP) and Secure Operating Procedures (SOP) are in place and maintained for all new and existing IT systems.
- Determining the level of security required for any new IT systems.
- Ensuring that all 3rd party connections or NHS Lanarkshire local methods of remote connectivity comply with the Scottish Wide Area Network (SWAN) code of connection.
- Ensuring regular risk assessments are performed on IT systems and the appropriate controls are identified to manage risk to acceptable levels.
- Monitoring and reporting the state of IT security within NHS Lanarkshire.
- Developing and enforcing procedures to maintain Information security.
- Ensuring compliance with relevant legislation and NHS Scotland Information security guidance.
- Developing IT Security awareness training material to ensure that all staff are aware of their responsibilities and accountability for information security.
- Monitoring, recording, investigating and reporting actual or potential IT security breaches.
- Auditing external service providers for access to IT systems and data.

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 Digital and across NHSL to ensure that all

systems are securely managed through the IGC in accordance with the Information Security Management System (ISMS).

The remit of the group is to:

- Provide assurance to the IGC as to the effective management and delivery of cyber security work across the organisation, to include but not limited to, detailed consideration of quarterly reports covering key aspects of performance, resource utilisation, risk and delivery.
- Review, agree and monitor work programmes across all aspects of cyber security including but not limited to work Cyber Essential Plus, NIS and Cyber Resilience Scottish Public Sector Action Plan and the related implementation and delivery methodologies and programme management arrangements.
- Require assurance of compliance with statutory and regulatory requirements and have regard to guidance and standards from other organisations (such as Scottish Government and other relevant bodies) including, but not limited to, Cyber Security and IT Resilience.
- Horizon scan so that the IGC is kept informed of such emerging policies, research, data, technical, clinical or other innovative developments as might have a bearing on the organisation's approach to development and delivery of its strategies and work programme for digital.
- Alert the IGC to any matters requiring governance action and oversee such action on behalf of the IGC.
- Deal with any such matters as may be assigned to the Cyber Security Group by the IGC and make recommendations as might be necessary.
- Monitor progress towards compliance with the Scottish Public Sector Cyber Resilience Framework.
- Review the Information Security Management System (ISMS).
- Review New and Existing Systems.
- Patch Management.
- Incident Management.
- Risk Management.
- Threats & Vulnerabilities.

The Group has been given the authority by the Information Governance Committee to manage cyber security programme and associated risks and incidents. The group will prepare regular highlight report for the Information Governance Committee.

Information Governance Committee

The Information Governance Committee (IGC) 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. The NHS Lanarkshire Information Governance Committee has the responsibility to oversee the delivery of the Board's Cyber Security Action Plan, including the review and approval of all Information Security policies and training.

Director of Information and Digital Technology

The Director of Information and Digital Technology has the responsibility to ensure that:

- The NHS Lanarkshire IT infrastructure is implemented in accordance with this policy.
- Changes to the infrastructure are subject to security risk assessment.
- Digital staff work within a clear framework which promotes Information Security and that this framework is documented and regularly reviewed within the department.

Digital Department

The Digital Department has the responsibility to ensure that:

- IT systems are held in secure areas that provide protection from unauthorised access and environmental threats such as fire, flood and loss of power.
- IT systems used to store NHS Lanarkshire data are recorded and any movements tracked to ensure that theft or loss is detected.
- All information is securely removed and appropriately destroyed before equipment is re-allocated or sent for secure disposal/destruction.
- Protection against malicious code (e.g. viruses, malware, etc) is operated on all workstations, servers and data exchange systems.
- All incoming data (including data held on IT media, e-mail and Internet downloads) is scanned on opening for malicious code.
- Back-up and recovery procedures are in place to assist in contingency arrangements to support business continuity.
- Interaction with external IT systems is recorded and monitored. This includes the monitoring of e-mail and other data streams up-loaded to, or downloaded from, any NHS Lanarkshire system.
- Back-ups of IT systems are kept in a secure place and procedures are in place to ensure that systems can be recovered in accordance with business needs.

Information Asset Owner

The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information asset within the Board. Key responsibilities include, but are not limited to:

- IAOs will work closely with other IAOs within the Board to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities, especially where information assets are shared by multiple services.
- IAOs will support the Senior Information Risk Owner (SIRO) in their overall management function.
- Preparing a register of approved systems users - who can access what information, how and when, according to the particular classification of information.
- Ensuring compliance with good practice in relation to application and password control.
- Ensuring compliance with media and equipment disposal procedures in liaison with the Digital Department.
- Responsibility for data subject access requests (as required by current data protection legislation) in conjunction with the Information Assurance Manager.

Functional, Service and Departmental Managers

Line managers are responsible for:

- Notifying the Service Desk of changes to staff personnel so that IT access can be provided and withdrawn in a controlled and auditable manner.
- Ensuring that all current and future staff are trained in their personal IT security responsibilities.
- Ensuring that any staff who use IT systems/media are trained in their secure use and disposal.
- Ensuring that no unauthorised staff are allowed to access any of NHS Lanarkshire IT systems.
- Determining which staff should be given authority to access specific IT systems. The level of access to IT systems will be based on job function need, irrespective of status.
- Implementing procedures to minimise NHS Lanarkshire exposure to fraud/theft/disruption of its IT and information assets.
- Ensuring that key documentation is maintained for all critical job functions to ensure Departmental business continuity in the event of staff unavailability is maintained.

All Staff

All staff, including contractors and service providers, who influence the use of NHS Lanarkshire information systems are responsible for:

- Conforming to the standards expected and described in this and any other associated information security policies.
- Reading and 'signing up' (accepting) to this and any other relevant information security policies which are relevant to their job role.
- Complying with specific information security responsibilities required of them as defined in their job description and also within IT systems secure operating procedure documentation.
- Taking personal and professional responsibility for dealing securely with any information they have access to in the course of their duties.
- Ensuring their actions when using these assets fully conform to this and related policies, NHS Scotland standards and legal requirements.
- Take all reasonable precautions to ensure no breaches of Information security result from their personal actions. This is also equally applicable for staff authorised to access and use NHS Lanarkshire Information systems remotely.
- Staff must report to the Service Desk any suspected or actual breaches of IT security.
- Fully complying with all NHS Lanarkshire Information Security Policies, Standards and Procedures.
- Notifying their Line Manager of all suspected or actual breaches of Information security.

Failure to observe this policy may result in disciplinary action according to local disciplinary procedures or legal proceedings being taken. Standard supplier contracts will also require contractors and other third parties to comply fully with the provisions of this and other NHS Lanarkshire Information Security policies.

Third Parties

NHS Lanarkshire and external organisations need to share information with each other and, in some cases, allow access to IT resources. Information sharing brings with it increased risk to the security of the data and the systems on which it is held.

Before allowing third party access, a risk assessment will be carried out by the Information Security Manager to establish the level of risk and to recommend any necessary counter-measures before access can be authorised.

Access to information assets by third parties will only be allowed when the appropriate security measures have been implemented and an agreement has been signed defining the terms for the sharing of data. A regular audit of external service providers in respect of their need for access to systems and data and their responsibilities regarding security and confidentiality will be carried out by the Information Security Manager.

Operational systems

Confidentiality of IT Systems

This will be maintained by ensuring that:

- Only authorised NHS Lanarkshire staff will be granted access to information systems and that access will be restricted to the information required for the person's job function i.e. only on a *need to know* basis.
- Where multiple staff share access to an NHS Lanarkshire Information System, each member of staff will be provided with a unique identifier. All transactions on such systems must be attributable and auditable to the user who conducts the transactions. In circumstances where such systems do not provide an auditable trail of use, measures should be put in place to manually audit user transactions.
- Passwords must be defined in line with national NHS Scotland standards and kept confidential at all times.
- Access to NHS Lanarkshire information systems from external IT networks and other types of communication link will only be permitted on an exception basis and be subject to an additional layer of security, in line with national and NHS Scotland remote connectivity standards and regulations.
- NHS Lanarkshire controls and monitors internal access to external networks and reserves the right to disconnect immediately, and if necessary, permanently, any member of staff or organisation attempting to breach this or any other NHS Lanarkshire Information Security Policy.

Integrity of IT Systems

This will be maintained by ensuring that:

- All NHS Lanarkshire information assets will operate in accordance with IT systems manufacturer specifications.
- Updating and other activities that could affect the integrity of information must be restricted to authorised staff needing to do so as part of their job function, in line with Caldicott principles on access to confidential information.

Availability of IT Systems

This will be maintained by ensuring that:

- Regular backups are taken of all IT systems and stored in a secure manner.
- Backups are tested regularly to ensure that systems/files can be restored if and when required.
- Business continuity/disaster recovery plans are in place.

Mobile Computing

This policy applies fully in situations where NHS Lanarkshire deploys mobile memory devices. NHS Lanarkshire will provide other Standards, guidelines and policies specific to the secure use of such devices.

System Development

Staff who authorise the development or purchase of information systems will be responsible for ensuring that the specification conforms to the purpose for which the systems are required. Developers or procurers of information systems, including service providers, will be responsible for ensuring that systems produce results as specified and provide adequate means of security:

- New Information systems being considered for procurement by NHS Lanarkshire must include adequate security measures that are clearly documented in the Business Case and defined in the requirements specification. The regulatory framework of the NHS, as well as Data Protection legislation and recommendations of the Caldicott Report must be adhered to throughout the requirement, design and implementation stages.
- The testing of all applications must be documented and attention paid to all aspects of security. Configuration Management must be used for each system - specifically, all initialisation files, data and test results files and system files must be identified and preserved with appropriate security and accountability. Under no circumstances will operational data be provided for use in application development or testing outside of NHS Lanarkshire own secure IT environment.
- All new systems must have a System Security Policy (SSP) produced. The SSP must address the different aspects of:
  - physical, personnel and document security principles;
  - communications security;
  - hardware and software security measures;
  - administrative and procedural security rules.
- The SSP may also incorporate the risk assessment for new systems.

Compliance

NHS Lanarkshire staff will comply fully with all relevant legislation and give consideration to advisory instructions from NHS Scotland and the Scottish Government. A list of the principal legislation and formal administrative guidance on information security with which NHS bodies must currently comply is provided in Appendix 1.

In particular:

- The NHS Lanarkshire Internal Audit function will review and report at defined intervals upon controls and security levels which operate at a system and application level. Specifically, Internal Audit will report upon the compliance of NHS Lanarkshire with this policy.
- NHS Lanarkshire is required to make arrangements for adequate levels of audit to be undertaken.

Risk management and business continuity

NHS Lanarkshire will complete risk assessment and management documentation for all information systems to ensure that threats and vulnerabilities are identified and risk is minimised through the application of balanced security controls

NHS Lanarkshire will ensure suitable disaster recovery and contingency arrangements are in place.

Recovery procedures will be developed for all IT operational systems and, where relevant, appropriate contingency plans will be documented and tested to ensure an acceptable level of service and control is maintained following a system failure.

Policy distribution

The Information Security Policy and all subsequent associated policies will be communicated to all members of staff in NHS Lanarkshire and to any appropriate third-party individuals or companies working on behalf of the organisation. The document will also be made available in Firstport.

Review

This Policy will be reviewed every two years or more frequently if appropriate to take into account changes to legislation that may occur, and/or guidance from the Scottish Government and/or the UK Information Commissioner. The review will be conducted in line with existing NHS Lanarkshire procedures.

5. Roles and Responsibilities

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

- UK General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- National Cyber Security Centre Cyber Assurance Framework
- Scottish Government Public Sector Cyber Resilience Framework
- 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 Framework
- 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

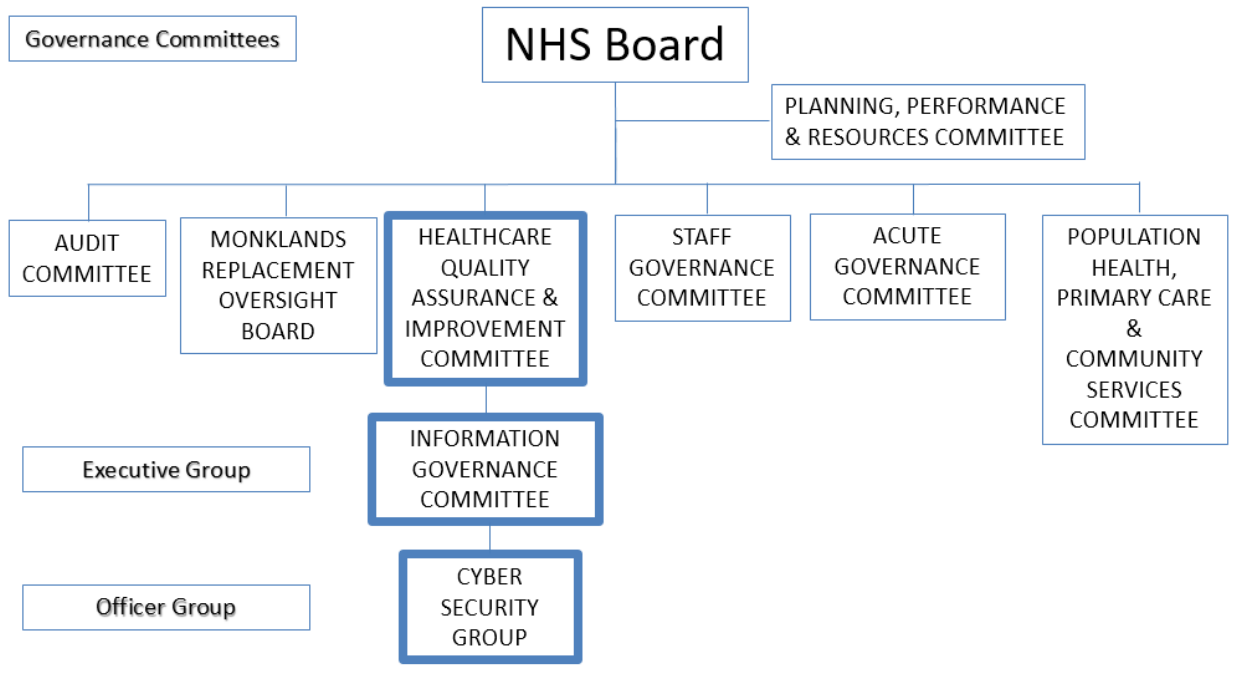
12. Assigned Roles Appendix 2

Staff assigned key roles as follows:-

- Chief Executive: Jann Gardner
- Caldicott Guardian: Professor Josephine Pravinkumar, Director of Public Health and Health Policy
- Director of Information and Digital Technology & Senior Information Risk Owner (SIRO): Donald Wilson
- Information Governance Manager & Data Protection Officer: Michelle Nobes
- Information Security Manager: Alan Ashforth

13. Governance Committee Structure Appendix 3

NHS Lanarkshire – Governance Committee Structure
1 April 2020



14. Digital Cyber Security Structure Appendix 4