Information Security Policy
Event Log Management

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:	**March 2017**
Version Number:	**2.6.6**
Last Review Date:	**Dec 2023**
Review Date:	**Dec 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.**
March 2017	A Ashforth	First Draft : New policy identified as a gap after review using SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	2.5
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.1
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
May 2019	A Ashforth	Converted from internal policy to public policy re Information Security Policy Framework 2018 and Network & Information Security Regulations 2018	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	2.6.5
Dec 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. References Appendix 1 – updated.	2.6.6

1. Introduction

This policy relates to event log management and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

The aim of this policy is to provide a consistent and robust event log management to ensure the availability of information and telecommunication services within NHS Lanarkshire.

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 purpose of this policy is to define the standards, and procedures for protecting and reviewing event logs and system auditing 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

Protecting & reviewing event logs and information systems audit

4.1 Event logging

Control
Event logs recording user activities, exceptions, faults and information security events must be produced, kept and regularly reviewed.

Implementation guidance
Event logs must include, when relevant:
a) user IDs;
b) system activities;
c) dates, times and details of key events, e.g. log-on and log-off;
d) device identity or location if possible and system identifier;
e) records of successful and rejected system access attempts;
f) records of successful and rejected data and other resource access attempts;
g) changes to system configuration;
h) use of privileges;
i) use of system utilities and applications;
j) files accessed and the kind of access;
k) network addresses and protocols;
l) alarms raised by the access control system;
m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;
n) records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

Other information
Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures must be taken.

Where possible, system administrators must not have permission to erase or de-activate logs of their own activities.

4.2 Protection of log information

Control
Logging facilities and log information must be protected against tampering and unauthorized access.

Implementation guidance
Controls must aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

a) alterations to the message types that are recorded;
b) log files being edited or deleted;
c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence.

Other information
System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalization must be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

4.3 Administrator and operator logs

Control
System administrator and system operator activities must be logged and the logs protected and regularly reviewed.

Implementation guidance
Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

Other information
An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

4.4 Information systems audit controls

Control
Audit requirements and activities involving verification of operational systems must be carefully planned and agreed to minimize disruptions to business processes.

Implementation guidance

The following guidelines must be observed:
a) audit requirements for access to systems and data must be agreed with appropriate management;
b) the scope of technical audit tests must be agreed and controlled;
c) audit tests must be limited to read-only access to software and data;
d) access other than read-only must only be allowed for isolated copies of system files, which must be erased when the audit is completed, or given appropriate

protection if there is an obligation to keep such files under audit documentation requirements;
e) requirements for special or additional processing must be identified and agreed;
f) audit tests that could affect system availability must be run outside business hours;
g) all access must be monitored and logged to produce a reference trail

4.5 Systems to support this policy

Event Log Management System
NHS Lanarkshire have invested in an event log management system for event management to:
a) automate the collection of event logs;
b) automatic alerting system managers of indicators of impending system failure e.g. no disk space, high CPU or high memory use;
c) anti-tamper protection of event logs by duplication into the event log management system database;
d) archive of event logs to provide retrospective examination
e) system manager to review event logs monthly

Policy Breach Management System
NHS Lanarkshire also automatically flags unusual system access by staff on key systems such as the patient management system using the nationally procured policy breach management system. The outputs from this system allows systems managers to focus on possible misuse of these key systems that host sensitive patient and/or staff data.

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 Policy/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