Information Security Policy
Incident Reporting

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 Committee**
Implementation Date:	**September 2010**
Version Number:	**2.6.6**
Last Review Date:	**Aug 2021**
Review Date:	**Aug 2024**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• 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
Sept 2012	A Ashforth	Revised in view of comments	2.1
May 2013	A Ashforth	Revised to reflect NHSL Incident Recording System (Datix)	2.2
May 2014	A Ashforth	Revised in view of comments	2.3
Aug 2014	A Ashforth & C Tannahill	Main changes - rewording of Section 4 - insertion of sub-section Possible Outcomes of Security Incidents, significant rewording of sub-sections Security Incident Reporting and Monitoring Responsibilities - All Staff – bullet point 5 Minor change - Reference appendix updated Minor change - some rewording throughout	2.4
Jan 2015	A Ashforth & C Tannahill	In Monitoring section change terminology for Critical Incident Review (CIR) to Significant Adverse Event Review (SAER), and grading of incident categories from High or Very High to the two Category 1 options - Category 1 Major & Category 1 Extreme	2.5
Aug 2015	A Ashforth	Minor change - Reference appendix	2.5.1
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)	2.5.2
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.3
April 2018	A Ashforth	Reviewed in line with General Data Protection Regulation (GDPR)	2.6

April 2018	A Ashforth	New section for reporting Significant Cyber Security Incidents	2.6.1
June 2018	A Ashforth	Updated to show new director of information and digital technology	2.6.2
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.3
Sept 2018	A Ashforth	Data protection statement added into Section 3 - Stakeholders	2.6.4
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.5
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	2.6.6

1. Introduction

This policy relates to Incident Reporting 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 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.

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).

This relates to the procedures to be followed when dealing with an information security breach. It defines what is meant by an information security breach. It also specifies the roles of ICT/eHealth staff in respect of dealing with security breaches.

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

Definition of Security Incidents

An information security incident can be any event which results in or could result in any of the following:

- Physical Loss or Theft of IT equipment
- Loss of Person Identifiable Data or Commercially Sensitive Information including paper and electronic formats
- Inappropriate access to electronic systems
- Inappropriate disclosure of confidential information

Possible Outcomes of Security Incidents

A security incident could result in:

- The integrity of the system or its data being compromised
  The availability of the system or information being put at risk
  An adverse impact, for example: embarrassment to the Organisation
- Potential for adverse publicity
- Breach of privacy/confidentiality
- Litigation
- Financial loss
- Disruption of service

Security Incident Reporting

All staff have a duty to report the incident to their line manager in the first instance. All non-General Practice incidents should then be recorded using the NHSL Adverse Event/Incident Recording System; general practice staff must use their own incident reporting system to record incidents.

Specific advice and support in relation to the incident can be obtained from the Information Security Manager or Information Governance Manager/Data Protection Officer where appropriate, following discussion with line management.

All security incidents including thefts of IT equipment should also be recorded on the NHSL Adverse Event/Incident Recording System system and should be notified to the IT Service Desk.

All incidents recorded on NHSL Adverse Event/Incident Recording System are graded in accordance with the risk matrix.
We have two Category 1 options – Category 1 Major & Category 1 Extreme (the difference in definitions can be found on the risk matrix). Incidents should be managed and escalated depending on the verified grading of the incident as within the risk management guidance refer to - NHSL Lanarkshire Adverse Event Management Policy

Incidents graded as Category 1 – Major or Extreme must be reported immediately to your line manager.

Notifiable Cyber Security Incident Reporting

Notifiable Scottish Public Sector Cyber Incidents are defined as incidents or attacks against Scottish public sector network information systems which:

- have the potential to disrupt the continued operation of the organisation or delivery of public services; and/or
- carry a likelihood that other public, private or third sector organisations may experience a similar attack, or that the incident could spread to those organisations; and/or
- could have a negative impact on the reputation of the Scottish public sector or Scottish Government; and/or
- carry the likelihood of Scottish Parliament or national media interest.

The eHealth department must report these cyber security incidents using the 'Scottish Public Sector Cyber Incident Notifiable Report' as early as possible by email or phone to a number of UK and Scottish Cyber security groups.

Monitoring

The Information Security Manager and IG Manager/Data Protection Officer will regularly review incidents recorded on NHSL Adverse Event/Incident Recording System, and provide appropriate advice and input where required. The Information Security Manager will report trends to the General Manager for eHealth.

The IG Manager/Data Protection Officer reviews all information governance incidents on NHSL Adverse Event/Incident Recording System and reports all incidents through the IG Committee on a regular basis. This will include the submission of any Situation Background Assessment and Recommendations (SBAR) or Significant Adverse Event Review (SAER) in relation to any serious incidents.

Freedom of Information and Other Public Disclosures of Incidents

Staff should be aware that the Organisation has a legal requirement to disclose details of incidents to external parties where requests are made using the appropriate legislation.

5. Roles and Responsibilities

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