Information Security Policy
Fraud

<table>
<thead>
<tr>
<th>Author:</th>
<th>Information Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Lead Executive Director:</td>
<td>Director of Information and Digital Technology</td>
</tr>
<tr>
<td>Endorsing Body:</td>
<td>Healthcare Quality Assurance and Improvement Committee</td>
</tr>
<tr>
<td>Governance or Assurance Committee</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Implementation Date:</td>
<td>September 2010</td>
</tr>
<tr>
<td>Version Number:</td>
<td>2.6.4</td>
</tr>
<tr>
<td>Review Date:</td>
<td>September 2020</td>
</tr>
</tbody>
</table>
CONTENTS

i) Consultation and Distribution Record
ii) Change Record

1. INTRODUCTION

2. AIM, PURPOSE AND OUTCOMES

3. SCOPE
   3.1 Who is the Policy Intended to Benefit or Affect
   3.2 Who are the Stakeholders

4. PRINCIPAL CONTENT

5. ROLES AND RESPONSIBILITIES

6. RESOURCE IMPLICATIONS

7. COMMUNICATION PLAN

8. QUALITY IMPROVEMENT – MONITORING AND REVIEW

9. EQUALITY AND DIVERSITY IMPACT ASSESSMENT

10. SUMMARY OF POLICY / FAQS

11. REFERENCES – APPENDIX 1
## Information Security Policy – Fraud

### 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) |
| Distribution: | All staff |

### CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2006</td>
<td>Revis</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Mar 2007</td>
<td>Revis</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Sept 2010</td>
<td>Revis</td>
<td>Revised in view of new policy template</td>
<td>2.0</td>
</tr>
<tr>
<td>May 2013</td>
<td>Revis</td>
<td>Revised in view of comments</td>
<td>2.2</td>
</tr>
<tr>
<td>May 2014</td>
<td>Revis</td>
<td>Revised in view of comments</td>
<td>2.3</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>Minor change</td>
<td>Reference appendix updated</td>
<td>2.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor change - some rewording throughout</td>
<td></td>
</tr>
<tr>
<td>Aug 2015</td>
<td>Minor change</td>
<td>Reference appendix</td>
<td>2.5</td>
</tr>
<tr>
<td>Oct 2016</td>
<td>Reviewed</td>
<td>in line with SG DL (2015) 17 Information Governance and Security</td>
<td>2.5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Improvement Measures 2015-2017 (NHSS Information Security Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Framework)</td>
<td></td>
</tr>
<tr>
<td>April 2017</td>
<td>Minor change</td>
<td>– Aim, Purpose and Outcomes regarding eHealth Information Security</td>
<td>2.5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management System (ISMS), information security standards and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>legislation.</td>
<td></td>
</tr>
<tr>
<td>April 2018</td>
<td>Reviewed</td>
<td>in line with General Data Protection Regulation (GDPR)</td>
<td>2.6</td>
</tr>
<tr>
<td>June 2018</td>
<td>Updated</td>
<td>to show new director of information</td>
<td>2.6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and digital technology</td>
<td></td>
</tr>
<tr>
<td>Aug 2018</td>
<td>Updated</td>
<td>reference to Data Protection Act 2018</td>
<td>2.6.2</td>
</tr>
<tr>
<td>Sept 2018</td>
<td>Data protection statement added into Section 3 - Stakeholders</td>
<td>2.6.3</td>
<td></td>
</tr>
<tr>
<td>Oct 2018</td>
<td>Adapt IS policy for use in General Practice</td>
<td>2.6.4</td>
<td></td>
</tr>
<tr>
<td>March 2020</td>
<td>K. Torrance</td>
<td>Extended until September 2021 (COVID-19).</td>
<td>2.6.4</td>
</tr>
</tbody>
</table>
1. **Introduction**

This policy relates to Fraud 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

The purpose of this policy is to inform staff within NHSL of their obligations in respect of the prevention of computer fraud.

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).

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](http://www.nhslanarkshire.scot.nhs.uk) or ask a member of staff for a copy of our Data Protection Notice.
4. Principal Content

Access to computer systems

Access is provided to staff to assist them in their day to day operational duties. These systems are provided for particular purposes and staff should only make use of the systems for the purposes which they are provided. NHSL allows personal usage of the Internet if it is reasonable and does not interfere with work e.g. lunch or other suitable work breaks.

This is particularly relevant to software systems where personal or financial information is collected, stored and processed.

Inappropriate Use of Computer Systems

If staff are unclear regarding the appropriate use of any computer system, they should contact their system administrator or line manager.

Inappropriate use of computer systems that could lead to the suspicion of computer fraud may result in NHSL taking action under the relevant HR policy.

System Administration

In order to ensure that the systems in use by NHSL are appropriately protected from the threat of computer fraud the following is implemented (where appropriate or operationally feasible) in all NHSL computer systems.

System Administration

A named individual (s) will be responsible for the administration of the system. This will cover initial access, password control, access control levels, user maintenance, and review of audit functionality where available.

System administrators will also provide discrete division of functions where this is a requirement of the system.

Procurement Requirements

As part of the procurement / replacement process for all systems, suppliers will be required to demonstrate where appropriate how their proposed systems provide protection from computer fraud.

Audit

All NHSL computer systems are subject to regular audit scrutiny of which computer fraud may be a facet, dependent upon the perceived risk.
Information Security Policy – Fraud

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

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:
    - General Data Protection Regulation (GDPR)
    - Network and Information Systems Regulations 2018 (NIS Regulations)
    - Civil Contingencies Act 2004
    - Computer Misuse Act 1990
    - Copyright, Design and Patents Act 1988
    - Data Protection Act 2018
    - Freedom of Information (Scotland) Act 2002
    - 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
Information Security Policy – Fraud

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000