NHS
HDL (2006)41

SCOTTISH EXECUTIVE

Health Department
Directorate of Primary Care and Community Care

Dear Colleague

NHSSCOTLAND INFORMATION SECURITY POLICY

Summary

1. NHSScotland IT Security Policy was established in 1993 under MEL(1993)59. This policy has now been updated.

Background

2. The overarching Information Security Policy Statement is attached at Annex A. Information Security Policy Principles covering authority, accountability, assurance and awareness are attached at Annex B. Specialist guidance material can be found at www.show.scot.nhs.uk/security.

Action

3. Chief Executive Officers are directly responsible for implementing the Policy, and for ensuring that line managers are aware of their responsibilities, which include ensuring that all staff adhere to the Policy. You should be aware that if anyone does not comply with the Policy and procedures, we do take this seriously and it may be treated as a disciplinary offence.

4. I would be grateful if information strategies for Boards and their Divisions could be reviewed to ensure that they reflect the standards set out on the website.

5. SEHD will arrange for the Policy to be reviewed annually.

Yours sincerely

Paul Gray

Paul Gray
Director of Primary and Community Care

11 July 2006

Addresses

For action

Chief Executives, NHS Boards, Special Health Boards and NHS National Services Scotland

Directors of Clinical Leads NHS Boards

IM&T Leads, NHS Boards, Special Health Boards and NHS National Services Scotland

Enquiries to:

Charlie Knox
eHealth
Room 05
Basement Rear
St Andrews House
EDINBURGH EH1 3DG

Tel: 0131-244 3577
Fax: 0131-244 5063
email:
charles.knox@scotland.gsi.gov.uk

ANNEX A

NHSSCOTLAND
INFORMATION SECURITY POLICY STATEMENT

The aim of this Information Security Policy is to safeguard the confidentiality, integrity and availability of all forms of information within NHSScotland. Information is one of our most valuable assets and it is essential that we have adequate safeguards to ensure that it is not lost, compromised or subject to unauthorised disclosure.

The purpose of this Policy is to protect personal and corporate information from all threats, whether internal or external, deliberate or accidental. This Policy correctly applied and adhered to will achieve a comprehensive and consistent approach throughout NHSScotland, ensure business continuity, and minimise both the likelihood of occurrence and the impact of any actual security incidents and breaches.

It is the Policy of NHSScotland to ensure that:

- Information will be protected against unauthorised access.
- 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.

A comprehensive framework is in place to support this policy. This takes the form of a series of policy, standards and best practice guideline documents on all aspects of IT security in NHSScotland organisations. These are available to NHSnet / N3 users under IT Security on the SHOW website at www.show.nhs.uk/security. They will be upgraded regularly as required.

All persons involved in the handling of information in the NHS have a legal duty of confidence towards patients, reinforced through their contract of employment (or equivalent formal relationships) with NHSScotland. A breach of patient confidentiality resulting from a breach of agreed procedures has always been and will remain a serious disciplinary matter.

The purpose of setting down a single national policy for IT security in NHSScotland is to ensure a consistently high standard of security across NHSScotland.

Organisations within NHSScotland are required to make arrangements for adequate levels of computer audit to be undertaken. Their Internal Audit function will review and report upon the controls and security levels that operate currently within computer installations and applications. Specifically, Internal Audit will report on the compliance with this national policy on IT Security.

The Scottish Executive Health Department (SEHD) will arrange for the Policy to be reviewed annually.

ANNEX B

NHSSCOTLAND Information Security Policy Principles

NHSScotland actively focuses on the following:

- developing a security culture through training and awareness events and by providing awareness education and training materials;
- adhering to Scottish, national 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.

This framework addresses four fundamental security principles - authority, accountability, assurance and awareness.

Its objectives are to ensure that:

- all Information Technology (IT) systems used in NHSScotland 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; and
- all employees are aware of the limits of their authority and the levels of their accountability for their actions.

Authority – to act

- All actions by IT systems or individuals using IT systems must conform to this policy, to comply with national NHS and legal requirements;
- NHSScotland, its separate bodies and agencies, must maintain an organised security infrastructure through which IT security matters can be discussed, approved and monitored;
- Each IT system requires an organised System Security Policy within which personnel using each system are authorised to act;
- Only correctly authorised persons may access IT systems;
- Access will be restricted to information required for the authorised person’s job function on a need to know basis;
- Updating and other activities, which could affect the integrity of information, will be restricted to authorised and authenticated persons needing to do so as part of their job functions;
- Controls and restrictions will be imposed to ensure that access to IT systems is restricted to such authorised and authenticated persons at designated terminals, workstation, laptops or any hand-held IT device (memory stick, PDA, Blackberry, smartphone, etc);
- Access to NHSScotland systems from external networks or via dial-up communication lines must be treated as extremely vulnerable and be subject to an additional layer or additional layers of security;

- Access will be restricted to information required for the authorised person's job function, and to processes which enable the authorised person to perform that function optimally;
- All IT equipment and media are protected from physical loss or damage, whether caused by accidental or malicious means;
- All personnel are given appropriate and proportionate authority, defined within job descriptions, for their use of NHSScotland systems.

Accountability - for actions

- Staff who authorise the development, purchase or procurement of IT systems will be responsible for ensuring that the specification conforms with the purpose or purposes for which the systems are required;
- Developers or procurers of IT systems, including service providers, will be responsible for ensuring that systems produce results as specified, are fully compliant, and provide adequate means of security;
- Operators of IT systems, including service providers, will be responsible for ensuring that they are suitably protected from security risks;
- Where an IT system may be accessed by more than one user, each user of such shared IT systems will have a unique and verifiable identity [6];
- All transactions on shared IT systems should be attributable to the individual who initiated them;
- Interaction with external shared systems will be recorded and monitored;
- All staff, contractors and service providers who use or influence the use of NHSScotland IT systems must conform to the standards expected and described in accordance with NHSScotland information security policies;
- Specific security related responsibilities required of key personnel will be defined in their job description and in secure operating procedure documentation, and a rolling programme of staff education will be initiated in line with section 1.2.4. (Awareness). The advice given in IT Security Manual Volume 9 Secure Operating Procedures applies;
- Compliance with the terms and conditions expressed in the NHSScotland Information Security Policy will be enforced through NHSScotland conduct and disciplinary procedures for staff, or through contractual arrangements for external contractors or service providers;
- There will be a regular audit of external contractors and service providers in respect of their need for access to systems and data and their awareness of responsibilities regarding security and confidentiality.

Assurance - that required actions are being taken

- NHSScotland will apply appropriate security in accordance with this policy to all its systems on the basis of perceived system risks, business criticality and management priority. This will enable the development and maintenance of procedures and best practice guidelines for staff;
- Contingency and recovery procedures ensuring an acceptable level of service and control will be considered for all IT systems and an appropriate contingency plan will be prepared where it is required. All contingency plans will be maintained and tested regularly as part of an ongoing IT Security management programme;

- NHSScotland is required to make arrangements for adequate levels of computer audit to be undertaken. The Internal Audit function will review and report at defined intervals upon controls and security levels, which operate at a general and application level. Specifically, Audit should report upon the degree of compliance of NHSScotland with this policy, derived from national policy and standards, and recommend alterations based on perceived gaps or derogations from standards;
- A list of the principle legislation and formal administrative guidance on IT Security with which NHSScotland bodies must currently comply is provided in the file Risk Management Framework - Legislation and Regulations.htm;
- Service Level Agreements (SLAs) defining the required availability must exist between the provider of a system and its users;
- All breaches of IT Security and other security incidents will be recorded and investigated and reported initially to the Health Board Information Services Manager, IT Manager, or designated IT Security Officer, and to the Information Security Consultant at NISG. Where a breach of IT security is likely to affect patient care, or to become public knowledge, the NISG must be informed immediately. It is the NISG's responsibility to ensure that any breach of IT security is fully investigated and the findings documented, and that standards and procedures are reviewed following the result of the investigation.

Awareness - by individuals, of the actions required of them

- All NHSScotland staff will be made aware of their responsibilities in maintaining an adequate level of IT Security;
- All NHSScotland staff with access to IT systems will be kept aware of this IT Security Policy and of relevant standards and procedures;
- All staff required to use IT systems will be adequately trained in their security-related roles and responsibilities and in the correct use of those systems;
- All staff must sign a copy of the NHSScotland Confidentiality Statement, as issued by their local organisation;
- All third party contractors, agents or others who need access to NHSScotland IT systems will be made aware of these requirements.