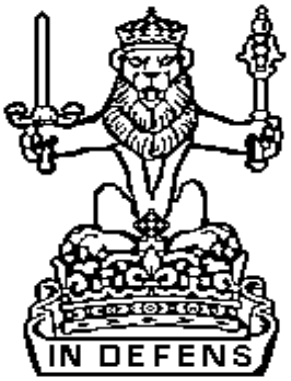

General Register Office for Scotland
information about Scotland's people

Paper NHSCR GB 1/08

NHSCR Scotland
Information Governance Standards

This is a draft on which the Board's comments would be welcome.

Contents

Introduction

Information Governance standards are in place to ensure that NHSCR Scotland handles and safeguards personal information.

This paper will highlight background to the current position and set out the standards (pages 4 to 11) as agreed with the Scottish Executive Health Department and NHS Quality Improvement Scotland (NHS QIS). These standards will:

- Give back office information to Health Care staff to help them.
- Support the provision of high quality care by promoting the effective and appropriate use of information.
- Encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- Develop support arrangements and provide staff with the tools they need to discharge their responsibilities to consistently high standards.
- Let NHSCR understand their own performance and manage improvement in a systematic and effective way.

To assist NHS organisations comply with the national Information Governance initiative. We are making the Information Governance standard available to all of our stakeholders.

About Information Governance

Information Governance means handling information in a confidential and secure manner to appropriate ethical and quality standards. It is important to NHSCR Scotland because we collect and use lots of information for administrative, research and medical purposes, which contribute to improving people's health. Information Governance is a key issue for all organisations and is fundamental to the effective delivery of health and other services.

We take account of:-

- The Data Protection Act 1998
- The Freedom of Information (Scotland) Act 2002
- Confidentiality: NHSScotland Code of Practice (CSAGS)
- Records Management
- Information Security Standard
- NHS Data Quality Assurance (Data Accreditation)
- Caldicott Guardians
- Section 57 of the Local Electoral Administration and Registration Services
  (Scotland) Act 2006 (LEARS Act)

A governance framework is in place, which promotes the ethical and lawful use of information in enhancing decision-making to support and drive improvement.

Information Governance Policy and Planning

Standard
There is a designated Director with responsibility for the Board's Information Governance policy and implementation plan.
The Board has approved an Information Governance policy.
The Board has agreed a plan for the implementation and monitoring of the Information Governance policy.
The Board's Information Governance plan includes appropriate training for all staff on the elements of Information Governance (e.g. confidentiality, data protection, security and professional standards in information collection and processing).
All staff contracts contain clauses that clearly identify staff responsibilities for confidentiality, data protection and security.
Information Governance is embedded in the Board's business planning cycle and risk management agenda.

Confidentiality

Standard
The NHSCR has mechanisms in place to ensure that all employees and other individuals participating in the delivery of information are aware of their responsibilities described in the NHSScotland Code of Practice on Protecting Patient Confidentiality.
The NHSCR has mechanisms in pace to ensure that information is given to inform patients/clients about proposed uses of their personal information.
The NHSCR has an incident reporting procedure, which is known, accessible and used by all staff.

Freedom of Information

Standard
The GRO(S) has a clearly identified, suitably qualified and supported lead individual responsible for the Freedom of Information (Scotland) Act 2002 (FoISA).
The GRO(S) has mechanisms in place to ensure that its statutory duties under FoISA are met.

A comprehensive system is in place to ensure the secure and confidential management of personal information including how it is obtained, recorded, used, shared, stored and disposed of in line with current legislation.

Administrative Records

Standard
There is a Senior Manager, responsible for the implementation of the GRO(S) Records Management policy and implementation plan.
The GRO(S) has agreed a plan for the implementation and monitoring of the Records Management policy.
There are approved Records Management procedures for the closure, disposal and retention of documents, which may be enforced only by authorised personnel.
All GRO(S) staff are provided with appropriate information, instruction and training on Records Management.

Patients are informed about how their personal information is recorded and used, how to access their personal information, and about their rights to determine how their personal information is shared and protected.

Data Protection

Standard
There is a clearly identified, suitably qualified and supported lead individual responsible for Data Protection.
The GRO(S) ensures that all formal contractual arrangements include appropriate patient confidentiality, information security and data protection requirements for all contractors and support organisations.

Formal policies are in place to manage situations where consent to share information is withheld, and where disclosure of personal information is required without consent.

Caldicott

Standard
The NHSCR has a clearly identified, suitably qualified and supported Caldicott Guardian.
The NHSCR has mechanisms in place to control, monitor and audit access to confidential patient information.
The NHSCR has agreed protocols governing the sharing of patient-identifiable information with non-health organisations.

Information Security

Information management links clearly into clinical governance arrangements and engages staff in the development and application of information and communication technology.

Systems are in place to ensure that staff have access to information to supported identity decision-making and facilitate delivery of quality services.

Standard
The GRO(S) has a formal risk assessment and management programme. It is supported by an Information Security Policy and overseen by senior management.
The GRO(S) has a clearly identified, suitably qualified and supported Information Security Officer (ITSO) as part of an active management forum giving direction and visible support for initiatives relating to confidentiality, data protection and security.

Standard
The GRO(S)/NHSCR follow standards to reduce the risks of human error, theft, fraud or misuse or abuse of facilities. All its employees contract to abide by the contents of these standards.
The GRO(S) has procedures in place to prevent unauthorised access, damage and interference to its business premises and information.
The NHSCR management of network communications and operations ensures that all responsibilities for operational procedures are fully documented, including personnel roles and responsibilities, and the standards and procedures for the management and operation of Board networking services. All alteration to existing procedures are subject to formal change management and change control procedures.
All NHSCR personnel have defined and documented access rights and other security measures to protect the confidentiality, integrity and availability of any information processed by computers and communications systems. Business requirement for access control are defined and documented.
The NHS Contract Management Team ensures that the development and introduction of new information systems, software, IT projects and IT support activities are conducted in a secure manner.
The NHSCR has clearly defined and documented procedures for managing Information Security incidents.
The NHSCR has a fully managed process in place for developing and maintaining business continuity for all its critical infrastructure components and core services.
The NHSCR has appropriate procedures in place to ensure that information passed to and from other organisations is done so securely.

Data Quality

Standard
There is an audit trail linking data entered to an individual.
There are agreed processes and timescales for the correction of errors and omissions identified by validation or internal users.
There is a clearly identified, suitably qualified and supported lead individual responsible for data quality.

Related Information

The source of this document is the NHSScotland Information Governance Standards December 2005.

The NHSScotland Information Governance Website
www.isdscotland.org/infogov

The NHSCR website

http://www.gro-scotland.gov.uk/national-health-service-central-register/index.html

The NHS paper link

http://www.nhshealthquality.org/nhsqis/files/CGRM_CSF_Oct05.pdf