NHS ORKNEY

Information Governance Policy

Policy Author:	Health Intelligence and Clinical Governance Manager
Policy Owner (for updates)	Director of Public Health
Engagement and Consultation	**Date**
Information Governance Group CMT	Dec 2015 Jan2016
Approval Record	**Date**
Information Governance Group	Jan 2016
Quality and Improvement Committee	Feb 2016
Equality and Diversity Rapid Impact Assessment	30 January 2013
Version Control	
Version Number	2.0
Date of Original Document	January 2010
Last Change and Approval Date	February Feb 2016
Last Review Date	April 2015
Next Formal Review Date	February 2018
Location and Access to Documents	
Location of master document	Clinical Safety and Quality folder on G drive
Location of backup document	EQIA folder on G drive
Location of E&D assessment	Attached
Access to document for staff	Blog
Access to document for public	NHS Orkney Website
Post holders names at last review	
Director of Public Health Health Intelligence & Clinical Governance Manager	Louise Wilson Jackie Gratton

If you require this or any other NHS Orkney publication in an alternative format (large print or computer disk for example) or in another language, please contact the Health Intelligence and Clinical Governance Department:

Telephone: (01856) 888283 or
Email: ork-HB.clinicalgovernance@nhs.net

Contents

1. Introduction

NHS Orkney recognises the importance of our information assets, both in terms of delivering healthcare to the people of Orkney, and in the efficient management of services and resources. Information governance plays a key part in supporting the delivery of care, service planning and performance management. Information must be effectively managed within a robust governance framework.

It also gives assurance to the organisations and individuals we work with that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible service and to meet NHS Orkney's legal, policy and good practice responsibilities.

The Information Governance Framework must support the principles of corporate governance and public accountability with equal importance placed on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

NHS Orkney will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Scotland Information Security Policy Framework and the NHS QIS (now HIS) Healthcare Governance and Risk Management National Standards

Information Governance is a key issue for NHS Orkney and is fundamental to the effective delivery of health services, particularly as we move towards an electronic patient record.

2. Purpose

The purpose of this document is to set the high-level framework within which the NHS Orkney Board can monitor NHS Orkney's performance and compliance in information governance, and to provide an overview of responsibilities and sources of more detailed guidance for all NHS Orkney staff.

The framework also recognises the need to share information with other health organisations, with health and social care integration partners and with other agencies in a controlled manner consistent with the interests of the patient, and, in some circumstances, the public interest.

3. Scope

This framework provides guidance on the collection, analysis, storage and transmission of data within NHS Orkney. The Information Governance Group

will be responsible for monitoring the implementation of the Information Governance policy and for developing any action plans to develop policies and procedures resulting from the implementation of the framework.

The policy applies to all the business information received, created or held by NHS Orkney, including, but not restricted to:

- Research and policy information
- Operational and financial information
- Personal information relating to patients and public, health practitioners, trainees and employees
- Organisational and corporate governance information

The policy applies to all the formats of information held by NHS Orkney, including, but not restricted to:

- Structured database records;
- Unstructured documents held on computer network drives, hard drives (PC or laptop), or removable media such as memory sticks, CD-ROMs, hard disks, and other similar media;
- E-mail held on current and 'archive' systems;
- Information published on the internet, blog or intranet by NHS Orkney;
- Printed or hand written on paper, white boards etc.;
- Paper records held on file;
- Microfilm, microfiche and electronically-scanned documents;
- Working documents, regardless of format, held by NHS Orkney staff or its contractors;
- Information held outside NHS Orkney premises or systems on our behalf;
- NHS Orkney business information held at home by NHS Orkney employees engaged in home/flexible working;
- Sent by e-mail, facsimile (fax) or other communications method;
- Presented on slides, overhead projectors, using visual or audio media;
- Digital dictation and voice mail;
- Spoken during telephone calls and meetings or conveyed by any other method.

4. Policy linkages

Effective information governance is a key part of NHS Orkney's compliance with NHS Quality Improvement Scotland (NHS QIS) Standards for Clinical Governance & Risk Management (October 2005).

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

The Essential Criteria from the relevant Standards informed the Information Governance Standards which have been used to structure the substantive content of this Policy (sections 5 to 11). Reporting against the Information Governance Standards toolkit is no longer required by Scottish Government.

The NHSS Information Security Policy Framework (June 2015) replaced both the NHSS Information Security Policy (2006) and the NHSS Information Assurance Strategy (2011-2015)

http://www.ehealth.nhs.scot/wp-content/uploads/sites/7/2015/07/IG3-Introduction-NHSS-Information-Security-Policy-April-2015.pdf

The Information Security Policy Framework is a vital part of a wider package of measures in the Information Governance Improvement Plan 2015-2017 (ranging from improvements to national scrutiny to developing better guidance for information sharing). In turn, the total package of information governance work underpins all the NHSS strategies.

The Public Records (Scotland) Act (2011) requires authorities to submit a record management plan to be agreed by the national Keeper of Records.

Continuous improvements in Information Governance will also be key to NHS Orkney meeting the 'Efficiency and governance improvements' performance indicators under the HEAT targets set by the Scottish Executive in Delivering for Health.

5. Information Governance Responsibilities

The Director of Public Health has delegated board-level responsibility for Information Governance and is responsible for this policy, its implementation and monitoring. This policy will be agreed by the Quality and Improvement Committee (QIC). Monitoring its implementation will be delegated to the Information Governance Group who will approve and monitor an Information Governance Implementation Plan.

NHS Orkney is obliged to abide by all relevant Scottish, UK and European Union Legislation. The requirement to comply with this legislation shall be devolved to employees and contractors of NHS Orkney, who will be held personally accountable for any breaches of information security for which they are held responsible.

As the Executive Lead for Information Governance, the Director of Public Health has a key responsibility to feed issues relating to the governance of information into policy and strategy development.

An Information Governance Report including proposed key actions for the coming year will be submitted to the Quality and Improvement Committee (QIC) annually.

The Director of Finance as the Senior Information Risk Owner (SIRO) has responsibility reviewing the Board's information security management system at planned intervals to ensure its continuing suitability and effectiveness (in conjunction with the executive management team), establishing a Board-level information security management system (ISMS), and ensuring that the Board-level information security policy aligns to the NHSS information security policy framework.

The day-to-day co-ordination of Information Governance issues will be delegated to the Health Intelligence and Clinical Governance Manager. The responsibilities of the Health Intelligence and Clinical Governance Manager will include, but not limited to:

- Recommending for approval, by the Information Governance Group or QIC, related policies and procedures.
- Recommending for approval by the Information Governance Group or QIC, an annual report on information governance and related key actions for the next year.
- To support the Information Governance Group to coordinate and monitor the Information Governance Policy across NHS Orkney.

The Health Intelligence and Clinical Governance Manager will report to the Director of Public Health. The Health Intelligence and Clinical Governance Manager will coordinate liaison with appropriate organisational departments as work streams require.

The Head of eHealth and IT will be responsible for ensuring that Board information security objectives are aligned with the NHSS eHealth Strategy and for producing reports such as Fairwarning reports to the DPH and IG Datix reports to the IG Group.

NHS Orkney has in place a comprehensive range of policies supporting the Information Governance agenda which are subject to ongoing review and improvement; reference must be made to these alongside this policy. Legal and professional guidance will be sought where appropriate.

Risk assessment, in conjunction with overall priority planning of organisational activity, will be undertaken to determine appropriate effective

and proportionate information governance controls are in place. Information governance issues will be captured within the Corporate Risk Register and the related reporting framework.

The Director of Finance is the Senior Information Risk Officer (SIRO)for NHS Orkney

6. Confidentiality

NHS Orkney regards all identifiable personal information relating to health practitioners, employees and patients as confidential. Compliance with the relevant legal and regulatory framework will be achieved, monitored and maintained.

NHS Orkney will maintain policies and procedures to ensure compliance with the Data Protection Act 1998 (see below), The Human Rights Act 1998, the common law duty of confidentiality, NHS Orkney's duty of care and the Freedom of Information (Scotland) Act 2002 (see below).

The Director of Public Health is the NHS Orkney Caldicott Guardian and has overall responsibility for the governance of confidential patient information and for the implementation of the component parts of this information governance framework.

Information Governance is an essential part of our business continuity planning and risk management processes and will be explicitly referred to in any strategies and plans. Breaches of confidentiality are reported through NHS Orkney's reporting system so that lessons can be learned from any incidents.

The responsibilities of all staff for Confidentiality are set out in employment contracts and the Policies and Procedures:

http://nhsnews02:1200/db/share/humanresources/Policies%20and%20Procedures/.

Breaches fall within the Disciplinary Policy and Procedures:

http://nhsnews02:1200/db/share/humanresources/Policies%20and%20Procedures/.

The rights of staff to report legitimate concerns will be protected in line with the NHS Orkney policy on whistle-blowing.
http://nhsnews02:1200/db/share/humanresources/Policies%20and%20Procedures/.

Responsibilities for Confidentiality will also form part of all contractual relationships with external organisations and all staff and stakeholders will be made aware of confidentiality requirements. All those on whom NHS Orkney holds personal information will be made aware of the uses to which the information may be used.

Incidents involving breaches of confidentiality and information security will be reported to the official designated in the Information Security Breach procedures. (See Information Security Policy)

http://nhsnews02:1200/traction/permalink/IT1660

Serious breaches will also be reported to the Information Commissioners Office (ICO). The Commissioners Officer will then decide if an official enquiry needs to be undertaken

7. Freedom of Information (FOI)

The Freedom of Information Act (Scotland) 2002 enables any person to obtain information held by Scottish public authorities, including NHS Orkney. This is a legal right and will ensure that all people swiftly receive information to which they are entitled. NHS Orkney will seek to be as open as possible, both in pro-actively providing information to the wider community and in responding positively to requests for information. As well as meeting our statutory responsibilities, NHS Orkney considers openness a vital component of our commitment to Patient Focus and Public Involvement (PFPI). NHS Orkney has a nominated FOI Lead with appropriate support and qualifications. The FOI Lead co-ordinates mechanisms to ensure NHS Orkney' statutory obligations are met.

NHS Orkney has made a commitment to both patients and staff to be as open and transparent as possible in the way that it works. The Director of Nursing, Midwifery and AHP is the nominated Executive Lead for the FOI programme of work and on behalf of NHS Orkney will ensure compliance with the requirements of the Act.

8. Records Management

The Board Secretary is responsible for the implementation of the Board's administrative records management. This includes the management of storage, disposal and retention policies/procedures for all administrative records.

The Clinical Administration Manager is responsible for overseeing the management of all clinical records across Secondary Care. The Primary care Manager has responsibility for overseeing the management of all clinical records across Primary Care. A working sub-group of the Information Governance Group will be formed when necessary to review existing patients' records policies and procedures to ensure they comply with the required Information Governance standards and any revised guidance from the Scottish Government Health Department (SGHD) on the retention and disposal of health records.

NHS Orkney recognises effective records management as being a key component of Information Governance and of our accountability and efficient service delivery. NHS Orkney will have a Records Management policy in place, agreed by the Information Governance Group, supported by appropriate procedures and technology. The policy identifies the Director of Public Health as the Senior Manager with responsibility for the Records Management Policy and Implementation Plan. Appropriate information and training will be provided to all staff.

NHS Orkney will manage the closure, retention and disposal of records, regardless of format, with reference to all available NHS Scotland guidance, such as NHS HDL (2006) 28, and in line with the Code of Practice on Records Management under section 61 of the Freedom of Information (Scotland) Act 2002. NHS Orkney will work towards the standards of records management set out in the International Standard ISO15489.

(See Records Management Policy and the Procedure for the Retention, Storage and Disposal of Records.)

http://nhstraction01:1200/db/attachments/management/2393/1/Records%20Management%20Policy%20February%202015.docx

http://nhstraction01:8080/traction#/single&proj=Management&edate=all&normaledate=all*1%2d1&stickyparams=normaledate,sort&sort=2&rec=2325

9. Patient Records and Caldicott

The Caldicott Guardian plays a key role in ensuring that NHS Orkney satisfies the highest practical standards for handling patient-identifiable information.

The Director of Public Health is nominated as Caldicott Guardian and NHS Orkney will observe the Caldicott principles where applicable (see MEL (19)1999). The Caldicott Guardian will also use the associated guidance in the manual for NHS Scotland Caldicott Guardians (2011).

Data Protection

NHS Orkney holds personal data relating to patients receiving care, and NHS Orkney employees. NHS Orkney fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998. NHS Orkney will:

- observe fully conditions regarding the fair collection and use of information (as defined under the 1st Principle)
- meet its legal obligations to specify the purposes for which information is used (as defined under the 2nd Principle)

- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements (as defined under the 3rd Principle)
- ensure the quality of information used (as defined under 4th Principle)
- apply strict checks to determine the length of time information is held (as defined under the 5th Principle)
- ensure that the rights of people about whom information is held can be fully exercised under the Act, including the rights to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances and; the right to correct, rectify, block or erase information which is inaccurate. (as defined under the 6th Principle)
- take appropriate technical and organisational security measures to safeguard personal information (as defined under the 7th Principle)
- ensure that personal information is not transferred outside the European Economic Area without suitable safeguards (as defined under the 8th Principle)

The Head of eHealth and IT is the nominated Data Protection Officer with appropriate skills and support, who ensures that a full, correct and up-to-date notification is lodged in its name with the Information Commissioner as required by the Data Protection Act 1998 (MEL(17)2000). This Officer's advice must be sought when any new information system is being designed to ensure the system's compliance with Data Protection requirements.

The IT Manager is the nominated Information Security Officer

All those on whom NHS Orkney holds personal data will be effectively informed of their rights in relation to the use of their personal data. All contractual arrangements will include the appropriate requirements for confidentiality, data protection, freedom of information and information security.

(See Information Security Policy)
http://nhsnews02:1200/traction/permalink/IT1660

10. Information Security Management

NHS Orkney will establish, implement maintain and continually improve an information security management system.

All NHS Orkney's major information assets will be accounted for in an Information Asset Register and have a nominated owner to ensure appropriate protection is maintained. Stakeholders will be involved in the development of information systems and information management

arrangements will link effectively to educational and research governance arrangements.

NHS Orkney will at all times comply with its responsibilities to protect the Intellectual Property Rights of third parties. The Health Intelligence and Clinical Governance Manager will provide guidance where required, seeking legal advice as necessary.NHS Orkney will maintain an Information Security Policy which nominates an appropriate Information Security Officer who will actively lead initiatives to improve information security and confidentiality. NHS Orkney will establish and maintain policies for effective and secure management of its information assets and resources in line with national policy and advice, for example as set out in NHS HDL (2006) 41.

NHS Orkney will maintain an Information Asset Register, assigning ownership of each major information/data set, its business justification and access restrictions.

All NHS Orkney staff will have defined and documented information access rights and their responsibilities for information security will be stated in employment contracts and in guidance documents. Business requirements for access control will be defined and documented. NHS Orkney will have procedures to prevent unauthorised access, damage or interference to business premises and information. NHS Orkney will follow standards to reduce the risks of human error, theft, fraud or misuse of information or facilities.

Audits will be undertaken or commissioned to assess information and IT security arrangements. NHS Orkney's incident reporting system will be used to report, monitor and investigate breaches of confidentiality and security. The availability of information systems will be preserved through the operation of clearly defined backup procedures and business continuity plans.

All computers, network communications and operations owned or used by NHS Orkney will be managed, operated and maintained in a secure manner and to recognised security standards. All responsibilities for operational procedures are documented and all alterations to procedures will be subject for formal change control procedures. Any new information system developments will be developed and implemented in a secure manner to preserve the confidentiality, integrity and availability of NHS Orkney systems, and with appropriate privacy impact assessments.

In order to measure the impact of NHS Orkney Information Governance Policy and associated procedures, staff will report to the Health Intelligence and Clinical Governance Manager any incident that places patient confidentiality or the confidentiality, security, integrity or availability of NHS Orkney information at risk (via the Datix reporting system or directly).

All NHS Orkney equipment containing information storage media will be checked to ensure that any sensitive data and licensed software have been

removed or overwritten prior to disposal. Where information is passed to other organisations, this will be done securely.

(See Information Security Policy)
http://nhsnews02:1200/traction/permalink/IT1660

11. Data Quality

As NHS Orkney deals directly with patient clinical data, we are subject to the clinical data quality standards and clinical coding issues which apply to other NHS Boards. NHS Orkney also recognises that high quality data is critical to clinical care, accurate decision making, sound performance management and accountability. NHS Orkney will take proportionate measures to ensure the quality of business critical data.

NHS Orkney will proactively identify its critical datasets which will be managed to the relevant data standards. These will have system audit trails, where appropriate linking data entered to specific individuals responsible for that data.

Internal and external audit and other quality assurance review processes will examine and underpin data quality in these critical areas. Where possible and proportionate, information quality will be assured at the point of collection.

Managers are expected to take ownership of, and seek to improve, the quality of data within their services. Internal and external audit will provide an independent check for data quality.

Relevant data quality standards and checks will be an integral part of all role-specific training in NHS Orkney.

12. References

International Standards Organisation	ISO27001 Information Security Management http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
Department for Health (UK)	MEL(19)1999 Caldicott Guardians http://www.sehd.scot.nhs.uk/mels/1999_19.doc
Scottish Government	Caldicott Guardians: Principles into Practice http://www.scotland.gov.uk/Publications/2011/01/31115153/10
International Standards Organisation	ISO15489 Records Management Standards
Scottish Government	Records Management Code of Practice

	http://www.scotland.gov.uk/Publications/2010/04/20142935/0
Scottish Government	Public Records (Scotland) Act 2011 http://www.scotland.gov.uk/Publications/2012/02/1995
NHS National Services Scotland	IT Security Guidance http://www.security.scot.nhs.uk
HealthCare Improvement Scotland	Standards for Clinical Governance & Risk Management. http://www.nhshealthquality.org/nhsqis/files/CGRM_CSF_Oct05.pdf
Scottish Government	Freedom of Information (Scotland) Act 2002 http://www.legislation.gov.uk/asp/2002/13/contents
Office of Public Sector Information	Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
Scottish Government	NHS HDL (2006) 28 The Management, Retention and Disposal of Administrative Records http://www.sehd.scot.nhs.uk/mels/HDL2006_28.pdf
Scottish Government	Scottish Accord on the Sharing of Personal Information (SASPI)
Scottish Government	eHealth Guidance http://www.ehealth.scot.nhs.uk/information-governance/
Scottish Government	Health and Social Care Information Sharing – A strategic Framework 2014-2020 http://www.scotland.gov.uk/Publications/2015/02/2900/0
Information Commissioners Office	https://ico.org.uk/for-organisations/health/