



Information Governance Strategy

| Document Profile Box | |
|---|--|
| Document Category / Ref | QSSD 1309 |
| Version: | 0003.0 |
| Ratified by: | Governance & Risk Committee |
| Date ratified: | 20 th September 2010 |
| Name of originator / author: | Information Governance Manager |
| Name of responsible committee / individual: | Information Governance Working Group |
| Date issued: | June 2011 |
| Review date: | 1 year from issue date |
| Target audience: | Directors, Senior Managers and Heads of Department |
| Document owner: | Director of Strategy and Business Development |
| Approved by: | |

Version Control

| Version | Release Date | Author | Status | Comments |
|---------|--------------|------------|--------|---|
| 1 | 22/07/07 | N Fairless | Final | Amended work streams to even workload. |
| 2.2 | Sept 2008 | N Fairless | Final | Amended work streams, change to timescales for Information Audit (MG). |
| 2.3 | June 2010 | R Hoque | Draft | Reformatted and updated to reflect any changes. |
| 2.4 | Oct 2010 | S Hush | Draft | Amended Roles and Responsibilities subject to Governance & Risk Committee recommendations. |
| 2.5 | Feb 2011 | L Hamill | Draft | Amended in line with the IG Toolkit Version 8 requirements. |
| 3.0 | May 2011 | R Hoque | Final | Organisational Risk Structure removed due to change in structure and now held as a separate document. |

Did you print this document yourself?

Please be advised that the Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version.

Document Location

The source of the document will be found in the Trust Quality System.

Freedom of Information Act 2000 Access

This document will be available via the NEAS Publication Scheme.

Contents

| Section | Page |
|--|-------------|
| 1. Introduction | 1 |
| 2. Purpose | 1 |
| 3. Scope | 2 |
| 4. Responsibility and Accountability | 3 |
| 5. Key Policies | 4 |
| 6. Information Governance Workstreams | 5 |
| 7. Consultation, Approval and Ratification Process | 7 |
| 8. Review and Revision Arrangements | 7 |
| 9. Document Control Including Archiving Arrangements | 7 |
| 10. References | 8 |
| Appendix A: Policies and Procedures | 9 |

1. Introduction

- 1.1. Quality information and knowledge and effective use of it can lead to the provision of high quality care to patients, clients and service users. It is now recognised as being one of the most important assets of an organisation. Information is needed at all levels to support internal operations, add value to its service delivery functions and to serve as evidence of the way an organisation operates.
- 1.2. Information risk management is an essential component of information governance and is an integral part of good management practice. The intent is to embed information risk management in a practical way into business processes and functions.
- 1.3. Information risk must be managed in a robust way within work areas and not be seen as something that is the sole responsibility of IT or Information Governance (IG) staff. A structured approach is needed, building upon the existing information governance strategy and this approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.
- 1.4. The Connecting for Health Information Governance Toolkit is a framework for implementing the information governance agenda. This strategy is based on the requirements of 101.
- 1.5. The Toolkit consists of a series of evidence based requirements against which an organisation's current and planned attainment levels can be monitored. All NHS Trusts are required to complete an annual self-assessment against the Toolkit requirements the results of which will contribute to the Trusts assessment by the Healthcare Commission. The Toolkit is broken down into five initiatives:
 - Corporate Information Assurance (including Freedom of Information and Corporate Records Management)
 - Clinical Information Assurance (including Clinical Records Management and Data Quality)
 - Confidentiality and Data Protection Assurance
 - Information Security Assurance.
 - Information Governance Management

2. Purpose

- 2.1. NEAS has a duty to comply with IG, as have all public sector organisations, and as a result respond to the challenges of information rights legislation, including Freedom of Information, Data Protection and the Reuse of Public Sector Information and to also incorporate standards and best practice into everyday routine, as set out in the NHS Codes of Practice. IG is the responsibility of every employee, as everyone has a responsibility to comply with law and best practice when handling personal information.

- 2.2. This strategy is underpinned by the Trust's IG Policy .The purpose of this strategy is to set out the strategic aims of the Trust in relation to its information and knowledge requirements and to also outline the Trust's approach and the necessary developments that will enable the Trust to deliver its aims.

3. Scope

- 3.1. The Trust has embraced the need to have a clear strategy for the management of information in response to its duty to ensure compliance with IG legislation and Codes of Practice.
- 3.2. The legislation and Codes of Practice include:
- Data Protection Act 1998 (DPA)
 - Freedom of Information Act 2000
 - The Reuse Of Public Sector Information Regulations 2005
 - Investigation of Regulatory Powers Act 2000
 - The Environmental Information Legislation 2004
 - The Confidentiality Code of Practice
 - Information Security Management
 - Records Management
 - Information Quality Assurance
 - Controls Assurance
 - Caldicott Guidelines.
- 3.3. Through implementing this strategy, the Trust will aim to comply with the above legislation and Codes of Practice by addressing the following six strategic aims.
- i. To introduce effective information management arrangements that conforms to the Department of Health standards and minimises the Trust's exposure to risk.
 - ii. To ensure relevant, accurate and quality information is used to inform all key decision making, and supports the Trust to continually demonstrate delivery, improve performance and enhance forward business planning.
 - iii. To provide ongoing assurance that all practices and procedures relating to handling and holding personal and Trust corporate information are protected, legal and conform to best and/or recommended practice whilst maintaining effective cost control.
 - iv. To provide service users, families and carers with:
 - Clear advice about how their personal information is recorded, handled, stored and shared by the Trust and its partners.
 - Information that explains their rights and how they can seek further information and how they can raise concerns.

- v. To ensure all new service development considerations include a comprehensive review of all aspects of IG arrangements to ensure that they are robust and effective.
- vi. To ensure all staff are aware and committed to their roles and responsibilities in relation to IG.

4. Responsibility and Accountability

- 4.1. There are a number of roles, resources and key bodies within the Trust which deal with IG in a variety of ways. These roles and bodies are set out and described below.
- 4.2. **The Accounting Officer** (the Chief Executive) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level and handled in a similar manner to other major risks such as financial.
- 4.3. **The Information Governance Manager**, with the support of the Information Governance Working Group (IGWG) is responsible for co-ordinating the IG work programme.
- 4.4. **The Information Governance Working Group** will have membership from senior representatives from across the organisation and will formally report to, and update the Trust Governance and Risk Committee on its progress, on a bi-monthly basis. The Group will report to the Trust Board as and when required, and at least annually to sign off the Information Governance Toolkit assessment.
- 4.5. **The Senior Information Risk Owner (SIRO)** is the Director of Strategy and Business Development, who has a responsibility to:
 - Oversee the development of an Information Risk Policy and its implementation.
 - Take ownership of risk assessment process for information risk.
 - Review and agree action in respect of identified information risks.
 - Ensure that the Trusts approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
 - Provide a focal point for the resolution and/or discussion of information risk issues.
 - Ensure the Board is adequately briefed on information risk issues.
 - Successfully complete strategic information risk management training at least annually.
- 4.6. **Senior Information Asset Officers (SIAOs)**; are directly accountable to the SIRO. There is at least one SIAO appointed to each directorate who is required to provide assurance to the SIRO that information risk is being managed effectively in relation to the assets within their directorate.
- 4.7. **Information Asset Officers (IAOs)**; report to their applicable SIAO and are required to account to the SIAO for the information risk management of the assets for which they have been assigned. The role of the IAOs is to understand:
 - What information is held.

- What information is added or removed from their assigned assets.
 - How information is moved / transferred.
 - Who has access to the information and why.
 - The nature and justification for information flows to and from their assigned assets.
- 4.8. **Information Asset Administrators (IAAs)**; support the IAOs in their role to effectively manage the information assets assigned to them.
- 4.9. The **Caldicott Guardian**, Director of Clinical Care and Patient Safety, has responsibility for:
- Promoting clinical governance.
 - Actively supporting work to enable information sharing where appropriate to share.
 - Advising on options for lawful and ethical processing of information.
 - Representing and championing confidentiality and information sharing requirements and issues at senior management level.
- 4.10. The **Data Protection Officer** has responsibility for:
- Implementing the Data protection work programme
 - Ensuring a senior person in each department is nominated and responsible for data protection practise within their work area.
- 4.11. IG spans the whole organisation and it is the responsibility of all staff. The development and production of other strategies covering aspects of the Trusts business have IG implications which need to be recognised and addressed. The IGWG will ensure there is adequate liaison with all Directorates. IG champions and/or departmental representatives will be critical in delivering the agenda as will those involved in information risk management.
- 4.12. Appendix B sets out the Trust's Organisational Risk Structure which includes the roles of the SIRO, SIAOs, IAOs and IAAs.

5. Key Policies

- 5.1. There are clear policies that cover the breadth of the IG agenda in line with the requirements of the NHS Operating Framework 2010/11. The relevant Trust policies include those listed below and more details on the approval / sign off of these documents can be found in Appendix A.
- Information Governance Policy
 - Confidentiality Policy and Code of Conduct
 - Data Protection Policy
 - Information Security Policy
 - Freedom of Information Policy
 - Records Management Policy

- 5.2. In addition to these policies, an Information Governance Improvement Plan has been put in place which is reviewed on a regular and updated accordingly.
- 5.3. As with all Trust policies and procedures, the above IG documents are disseminated throughout the organisation and communicated to all staff as and when they are implemented and/or amended via internal communications systems as well as during new staff induction programmes.
- 5.4. These policies are also available for all staff to access via the Trust Quality System. Staff without computer network access should contact their line manager for information on how to access policies.

6. Information Governance Workstreams

There are five workstreams that have been identified in order to manage the extensive agenda. These workstreams are:

- Confidentiality and Data Protection Assurance
- Records Management (Information Lifecycle Management)
- Staff Communications and Training
- Information Security
- Information Quality Assurance & Performance Reporting

The IGWG will assign appropriate members of the group to be the leads for a specific workstream. They will ensure that the elements involved within the workstream are up to date and fully compliant with current best practice and legislation.

6.1. Confidentiality and Data Protection Assurance

This workstream will ensure there is compliance with all aspects of the DPA and ensure confidentiality is protected in all areas of Trust practice. The main areas of work will include:

- External Communications Strategy (including Internet links, leaflets for service users, families and carers)
- Survey of service users, families and carers
- Caldicott guidelines
- Subject Access Requests
- Information Sharing Protocols
- Auditing access to confidential patient information

6.2. Records Management (Information Lifecycle Management)

This workstream will ensure the Trust has an effective Records Management Strategy in place. The main areas of work will include:

- Records Management Policy and inventory of corporate records
- Records Retention and Disposal Policy and Schedule

- Management of the Trust's Information Asset Register (IAR)
- Implementation of NHS Number
- Tiered storage
- Compliance with Freedom of Information Act

6.3. **Staff Communications and Training**

This workstream will ensure there is a clear reporting structure in place and through management action and training all staff understand IG requirements through:

- Development of IG Communications Strategy (Intranet, maintenance of a clear reporting structure)
- Staff training schedule and monitoring via the Information Governance Training Tool
- Staff induction programme and annual statutory and mandatory training

6.4. **Information Security**

6.4.1. This workstream will ensure that all data will be appropriately protected against accidental or deliberate loss as a result of human or external causes through:

- Information Security Management Policy
- Information Security Management System (ISMS)
- Risk Management
- Business Continuity and Disaster Recovery Plans
- Compliance with Security Standards ISO 17799

6.4.2. Information risk assessments are carried out in respect of information assets in line with the Information Asset Risk Assessment process and the Information Risk Policy (see Appendix A for details on these documents).

6.4.3. All staff are also required to adhere to the Policy for Incident Reporting and Investigation and report any and all information security incidents and suspected incidents accordingly using the NEAS07 form. Again, details regarding the Policy for Incident Reporting and Investigation can be found at Appendix A.

6.5. **Information Quality Assurance & Performance Reporting**

This workstream will ensure all data held is accurate, timely and fit for purpose, easily available to those who need it and there is effective monitoring of all Information Governance activity, also complying with external IG performance requirements. These workstreams are:

- Data accreditation and information management standards (Management and Clinical Audits will also be used to identify good practice and opportunities for improvement)
- Development of coding standards in the advent of Payment by Results
- IG breaches and incident reporting
- IG Toolkit Self-Assessment
- IG review schedule and performance framework (including Annual Health Check)

- Compliance with Audit Commission's Data Quality Standards

6.6. **National developments**

The IGWG will keep the Trust up to date with all related national developments including release of new legislation and/or Codes of Practice.

6.7. **Risks associated with non-implementation of Information Governance**

6.7.1. The purpose of this strategy is to identify and eliminate, reduce or mitigate the risks relating to inadequate Information Governance. There are a number of risks to the Trust which can be classified under the following headings:

- Legal action – non compliance with Data Protection, Common Law, Human Rights and Freedom of Information legislation.
- Adverse publicity, resulting in loss of public trust/confidence in the organisation.
- Contribution to clinical or corporate negligence due to information failure.
- Impact on future activity – reduced or no access to Connecting for Health
- Financial Impact – the Information Commissioner's Office as at 6 April 2010, now has the power to impose fines of up to £500,000 as a penalty for serious breaches of the Data Protection Act.

6.7.2. There will be close alignment of this strategy with the Trust's Risk Management Policy. A full information risk assessment will be carried out.

7. **Consultation, Approval and Ratification Process**

7.1. **Consultation**

7.1.1. This document has been produced by the author on behalf of the IGWG. This group was consulted upon and their comments added to the document as appropriate.

7.2. **Approval and Ratification**

7.2.1. The Governance and Risk Committee is the committee with the authority for the approval and ratification of this document.

7.2.2. The IGWG has carried out a full and proper consultation and has considered the content of the document in terms of current best practice, guidelines, legislation and mandatory and statutory requirements, in considering the document for approval the committee also took into account the results of the recommendations of the EIA.

8. **Review and Revision Arrangements**

8.1. The document will be reviewed every 2 years or when appropriate after changes in legislation or guidance. The document owner will be responsible for this review.

9. **Document Control Including Archiving Arrangements**

9.1. **Register / Library of Procedural Documents**

All documents shall be held within the Trust Quality System and will be managed in line with quality standards.

9.2. **Archiving arrangement**

Archiving of documents will be in line with the Records Management Policy.

10. References

- Department of Health NHS IG Guidance on Legal and Professional Obligations.
- NHS Connecting for Health IG Toolkit <https://www.igt.connectingforhealth.nhs.uk/>.

Appendix A: Policies and Procedures

| Policy Name | Date Issued | Date Approved / ratified | Approved / ratified by? |
|---|-------------|--------------------------|---|
| Information Governance Policy | June 2011 | March 2011 | Governance & Risk Committee |
| Confidentiality Policy and Code of Conduct | 31/10/2009 | 15/09/2009 | Policy Review Group Joint Consultation Committee |
| Data Protection Policy | 31/10/2009 | 15/09/2009 | Policy Review Group Joint Consultation Committee |
| Information Security Policy | 31/10/2009 | 24/09/2009 | Trust Board |
| Freedom of Information Policy | Jan 2011 | Oct 2010 | Trust Board |
| Records Management Policy | Jan 2011 | Jan 2011 | Trust Board |
| Information Risk Policy | Aug 2010 | 25/03/2010 | Policy Review Group Governance & Risk Committee Trust Board |
| Policy for Incident Reporting and Investigation | July 2009 | Sept 2008 | Health & Safety Committee |