



Information Governance Policy

Document Profile Box	
Document Category / Ref	QSSD 1313
Version:	0003.0
Ratified by:	Governance and Risk Committee
Date ratified:	17 th March 2011
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:	All staff
Document owner:	Director of Strategy & Business Development
Approved by:	

Version Control

Version	Release Date	Author	Status	Comments
0001	Feb 2008	Mark Glencorse	Approved	
0002	Apr 2009	Rahima Hoque	Draft	Reviewed to ensure the policy follows the structure identified in the Organisational-wide Policy for the Development and Management of Procedural Documents
0002	Sept 2009	Rahima Hoque	Final	Following ratification.
0002.1	Nov 2009	Rahima Hoque	Final	Document owner added to profile box.
0003.0	Dec 2010	Syma Dawson	Final	Reviewed in line with the IG Toolkit requirements of version 8

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	1
4. Definitions	2
5. Responsibility and Accountability	2
6. Legal and Professional Obligations	4
7. Principles of Information Governance	5
8. Equality and Diversity Statement	7
9. Consultation, Approval and Ratification Process	7
10. Review and Revision Arrangements	8
11. Dissemination and Implementation	8
12. Document Control Including Archiving Arrangements	8
13. Monitoring Compliance With and the Effectiveness of Procedural Documents	9
14. References	10

1. Introduction

- 1.1. The North East Ambulance Service NHS Trust (NEAS) recognises the importance of information, both in terms of healthcare management of individual patients and the efficient management of services and resources. This is because information is a vital asset that underpins the delivery of high-quality healthcare and many other key service deliverables.
- 1.2. The NEAS therefore has a responsibility to ensure that information is managed appropriately and in accordance with Information Governance (IG) requirements.
- 1.3. IG provides a framework that allows the Trust to monitor and improve the way in which it handles information. It is a means of providing assurance that information, particularly person-identifiable information, is managed efficiently, securely, effectively and in accordance with relevant legislation, with the objective of delivering the best possible care and service.
- 1.4. The NEAS will establish and maintain policies and procedures to ensure compliance with requirements contained in the IG Toolkit, monitored by Connecting for Health.
- 1.5. IG currently includes the following legislation and guidance:
 - Data Protection Act 1998
 - Freedom of Information Act 2000 (FOI)
 - Environmental Information Regulations 2004
 - Department of Health Records Management: NHS Code of Practice
 - Computer Misuse Act 1990
 - The Confidentiality Code of Practice
 - Common Law Duty of Confidentiality
 - Information Security Management BS7799

2. Purpose

- 2.1. The purpose of this document is to outline the organisation's intentions and approach to fulfilling its statutory and organisational responsibilities around information governance. It will enable staff to make informed decisions, comply with relevant legislation and help deliver the Trust's aims and objectives.

3. Scope

- 3.1. This IG policy should be adhered to by all staff employed by the NEAS and / or with a responsibility for NEAS data, which may include contractors or staff employed by other organisations but working on behalf of the NEAS.
- 3.2. This policy covers all aspects of information within the Trust including but not limited to:
 - Patient / client / service user information

- Personnel information
 - Corporate information
- 3.3. This policy covers all aspects of handling information including, but not limited to:
- Paper based and electronic record systems
 - The transmission of information via e-mail, fax, post and telephone.

4. Definitions

- 4.1. **Personal information** (sometimes referred to as person-identifiable data (PID)) is data which relates to an individual who can be identified from that information or in conjunction with any other information that is or may come under the possession of the data controller. This data can also include any expression of opinion about an individual or information provided under professional opinion. Examples of personal information includes name, address, date of birth, or any other unique identifier such as NHS Number, hospital number, national insurance number etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode etc.
- 4.2. **Sensitive information** is defined in Section 2 of the Act as data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. These data are subject to more stringent conditions on their processing when compared to personal information.
- 4.3. **Information Assets** include;
- **Personal information** e.g. content within databases, archive and back-up data, audit data, paper records
 - **Software** e.g. application and system software, development and maintenance tools
 - **Hardware** e.g. PCs, laptops, USB sticks, PDAs
 - **System / process documentation** e.g. system information and documentation, manual and training materials, business continuity plans.

5. Responsibility and Accountability

- 5.1. **All staff** have a responsibility to:
- Adhere to the IG Policy and all other IG related policies, procedures, including the Confidentiality Code of Conduct.
 - Adhere to the relevant legislation, particularly those listed under point 1.5.
 - Undertake IG training that is appropriate to their role.
 - Raise any concerns in relation to IG with their line manager or the IG Manager.
- 5.2. **Line managers** have a responsibility to:

- Ensure all current, new and temporary staff are instructed of their IG responsibilities and made aware of the IG Policy in addition to other IG related policies and procedures.
- Ensure staff receive IG training that is appropriate for their role.
- Investigate and take relevant action on any potential breaches of this policy supported by Risk Management and the Information Governance Working Group (IGWG) in line with existing procedures.

5.3. **The Information Governance Working Group (IGWG)** has a responsibility to:

- Develop and maintain the IG agenda across the NEAS.
- Monitor progress against the IG Toolkit.
- Ensure policies and procedures are developed, implemented and reviewed appropriately.
- Develop standards and guidance relevant to IG.
- Promote awareness of IG issues.
- Ensure IG risks and incidents are identified, logged, actioned and monitored routinely.

The IGWG has a membership from senior representatives across the organisation and formerly reports to the Governance & Risk Committee, which reports into the Trust Board.

5.4. 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 as well as issues at senior management level.

5.5. The **Information Governance Manager** has responsibility for:

- Implementing the IG agenda whilst coordinating the IG work programme
- Developing and maintaining IG policies and procedures to provide staff with direction and guidance on how to comply with IG requirements
- Raising awareness and promoting IG throughout the NEAS
- Work closely with the Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) to ensure information risk is managed effectively within the organisation

5.6. The **Senior Information Risk Owner**, Directory of Strategy and Business Development, 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 alongside IAOs and IAAs

- 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

5.7. The **Information Asset Owners** have a responsibility to:

- Leading and fostering an information security culture which values, protects and uses information for the success of the organisation and benefit of its patients.
- Knowing what information compromises or is associated with the asset, what enters and leaves it and why
- Knowing who has access to the asset, whether system or information, and why, and ensuring access is monitored
- Understanding and addressing risk to the asset, whether system or information, and why
- Ensure the asset is used for the public good, including requests for access from others
- Notifying the IGWG of any changes to existing assets and ensuring that new information assets are added to the asset register and any redundant assets removed.

6. Legal and Professional Obligations

- 6.1. The Trust regards all person-identifiable and sensitive information as defined under section 4 of this policy as confidential information.
- 6.2. Information that can be accessed under the Freedom of Information Act 2000 will be made available through a variety of media and in line with the Trust's FOI Publication Scheme.
- 6.3. The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000, the Data Protection Act 1998 and other relevant legislation relating to the security and use of both personal and non personal information.
- 6.4. The Trust will ensure that any transfers of personal information outside of the UK, and particularly outside the European Economic Area (EEA), are only done so when adequate level of protection exists and security measures are satisfied within the receiving country.
- 6.5. The Trust will establish and maintain policies for the controlled and appropriate sharing of personal information with other agencies (i.e. Information Sharing Agreements), taking into account relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).
- 6.6. The Trust will undertake or commission regular audits to assess its compliance with legal requirements.

7. Principles of Information Governance

7.1. General Information Governance

- 7.1.1. The NEAS will establish, maintain and review policies and procedures for the effective and secure management of all information assets and resources.
- 7.1.2. All staff will receive IG training that is appropriate for their role; a training needs analysis will be conducted to consider different staff roles and the level of IG training that is required.
- 7.1.3. Regular reviews and audits will be carried out to identify good practice and opportunities for improvement. Staff surveys will also be utilised as a means of evaluating staff awareness and compliance around IG.
- 7.1.4. All new processes, services, information systems, and other relevant information assets will require consultation from the IG working group in line with the Trust's policy GEN 269.
- 7.1.5. The NEAS will assess its performance in IG using the IG Toolkit to help develop and implement action plans to ensure continued improvement in this area.
- 7.1.6. The NEAS will identify third parties (key contractors, sub-contractors, partners or support organisations) gaining access to confidential information and will ensure formal contractual arrangements include compliance with IG requirements.

7.2. Information Risk Management

- 7.2.1. The NEAS will ensure the effective implementation of an information risk framework that identifies information assets and their owners.
- 7.2.2. Risk assessments will be conducted to ensure appropriate and effective security is in place for each information asset.
- 7.2.3. Staff will be informed on policies and procedures that provide guidance for reporting IG breaches and incidents in line with the Trust's Information Risk Policy.

7.3. Openness

- 7.3.1. The Trust recognises the need to maintain an appropriate balance between openness and confidentiality in the management and use of information.
- 7.3.2. The NEAS fully acknowledges its obligation to be publicly accountable; however, the Trust also places importance on the confidentiality and safeguarding of personal information relating to staff and patients and commercially sensitive information.
- 7.3.3. Corporate information of the NEAS will be available to the public in line with the NHS code of openness and in accordance with the Freedom of Information Act 2000
- 7.3.4. The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- 7.3.5. Awareness and understanding of all staff, with regard to their responsibilities when handling information, will be assessed and appropriate training and guidance provided as necessary.
- 7.3.6. Patients will have access to information relating to their own health care through Trust publications, and there will be clear procedures for handling subject access requests.

7.3.7. The NEAS recognises the need to share personal information with partner organisations and other agencies in line with the Data Protection Act and Caldicott principles. The NEAS will help contribute to the implementation of the North East Information Sharing Guidelines and associated Information Sharing Agreement.

7.4. **Confidentiality and Data Protection Assurance**

7.4.1. The NEAS regards all person-identifiable information as confidential except where national policy or law on accountability and openness requires otherwise.

7.4.2. IG awareness and understanding of all staff will be assessed via staff surveys and spot checks; follow up action will be taken as a result of the findings e.g. refresher IG training provided.

7.4.3. Effective arrangements will be put in place to ensure confidentiality and security of personal and other sensitive information.

7.4.4. All staff will be informed around the disclosure of person-identifiable information and the consequences should an information security breach occur e.g. ICO powers to fine up to £500,000.

7.5. **Information Security Assurance**

7.5.1. The Trust will undertake or commission regular audits to assess information and security arrangements in keeping with profession, legislative and statutory requirements such as the NHS Information Security Code of Practice.

7.5.2. A review of all information flows will be conducted followed by a risk assessment for each data flow; those at a high risk of an information security breach will be mitigated. Processes will be established to regularly review data flows so information risk and security is managed effectively.

7.5.3. The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training.

7.5.4. The Trust's incident reporting system will be used to report, monitor and investigate all breaches of confidentiality and security.

7.6. **Information Quality & Assurance**

7.6.1. The NEAS recognises that accurate, timely and relevant information is essential to deliver high quality healthcare. As a result, the Trust will establish and maintain policies for information quality assurance and the effective management of records.

7.6.2. The appointment of Records Management Officers (RMOs) will take ownership of, and seek to improve, the quality of data within their services.

7.6.3. There is a commitment with improving records management for care purposes in keeping with profession, legislative and statutory records management requirements such as the NHS Records Management Code of Practice.

7.6.4. The integrity and reliability of information will be monitored and maintained to ensure that it is consistent and appropriate for the purposes intended.

7.7. Secondary Uses Services

7.7.1. There is a commitment to developing quality data to support non direct care related purposes (planning, commissioning, public health, finance).

7.7.2. There is a commitment to improving data quality through the use of local and national benchmarking.

8. Equality and Diversity Statement

8.1. The Trust is committed to providing equality of opportunity, not only in its employment practices but also in the services for which it is responsible. As such, this document has been screened, and if necessary an EIA has been carried out on this document, to identify any potential discriminatory impact.

8.2. If relevant, recommendations from the assessment have been incorporated into the document and have been considered by the approving committee. The Trust also values and respects the diversity of its employees and the communities it serves. In applying this policy, the Trust will have due regard for the need to:

- Eliminate unlawful discrimination.
- Promote equality of opportunity.
- Provide for good relations between people of diverse groups.
- For further information on this, please contact the Equality and Diversity Department.

9. Consultation, Approval and Ratification Process

9.1. Consultation

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

9.2. Approval and ratification

9.2.1. The Trust Policy Review Group is the committee with the authority for the review of this document. The Governance and Risk Committee have responsibility for ratification of this policy

9.2.2. 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.

10. Review and Revision Arrangements

10.1. The document will be reviewed at least annually or when appropriate after changes in legislation or guidance. The document owner will be responsible for this review.

11. Dissemination and Implementation

11.1. Dissemination

11.1.1. This policy is 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.

11.1.2. All staff will be notified of new or revised documents via internal communications systems.

11.1.3. This document will also be included in the Publication Scheme for NEAS in compliance with the FOI Act 2000.

11.2. Implementation

11.2.1. This policy will be implemented in the following ways:

- Regular communications to staff on new policies and procedures through IG Circulars.
- Regular audit of information governance (IG) processes undertaken in line with policies and procedures in key areas i.e. records management, confidentiality, information security, FOI and data quality.
- Monitoring through the Information Governance Toolkit (IGT).

11.3. Training

11.3.1. IG training will be incorporated into the Trust's Statutory and Mandatory training and will be delivered using the IG Training Tool; an online system that has been provided by Connecting for Health. Additional training can be requested at the discretion of a manager, or by an individual wanting personal development along with mandatory yearly update training.

11.3.2. Further guidance and information relating to IG issues will be distributed periodically via various media including the intranet site, 'The Pulse' (monthly service journal) and via email.

12. Document Control Including Archiving Arrangements

12.1. Register / library of procedural documents

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

12.2. Archiving arrangement

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

13. Monitoring Compliance With and the Effectiveness of Procedural Documents

13.1. Process for monitoring compliance

13.1.1. All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for IG.

13.1.2. Failure to follow this policy and related IG policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

13.1.3. Different methods will be used for monitoring different aspects of IG including:

- Monitoring of IG processes through the IG Toolkit.
- Audit of information flows to ensure confidential information is being transferred securely.

13.2. Standards and Key Performance Indicators

There are a number of national standards and requirements relating to IG.

13.2.1. IG Toolkit (IGT)

The IGT is an evidence-based performance tool produced by Connecting for Health which contains a series of requirements for different NHS organisations. Each requirement draws together legal obligations in addition to central guidance. The NEAS currently has 35 national requirements which require a minimum of level 2 compliance for each. The final submission for every toolkit version is the 31st March, the results of which will contribute to the assessment undertaken by the Healthcare Commission.

13.2.2. Standards for Better Healthcare

- The Department of Health's standards for better health include 24 core standards that all NHS healthcare providers in England should achieve, and 13 developmental standards that they should be working towards achieving.
- These core and developmental standards cover all aspects of healthcare, including the safety of patients, clinical effectiveness and cost effectiveness.
- Specific standards are of relevance to IG which covers consent for use of patient / service user information, confidentiality of patient / service user information, records management and information sharing protocols.

13.2.3. NHS Litigation Authority

- The NHSLA Risk Management Standard for Ambulance Trusts applies to all Ambulance Trusts and designed to address organisational, clinical, and non-clinical / health and safety risks.
- Parts of the Clinical Care standard are of relevance to IG, including patient / service user identification and quality of written and electronic clinical records.

14. References

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