North East Ambulance Service NHS
NHS Foundation Trust

Information Governance Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-3
Version Number	V05
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	22 December 2017
Date Policy Effective From	22 December 2017
Next Review Date	22 December 2020
Keywords	Personal information, sensitive information, information assets, data protection, security, Caldicott, ICO.

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
1		'NEAS' replaced with 'Trust'. All document references removed. Updated committee references. Updated in line with DNV recommendations – monitoring section.	Information Governance Manager	14 September 2014
1		It was suggested that the acronyms EIA and EIS should be expanded for clarity (to Equality Impact Assessment and Equality Impact Screening) – cannot change as this is part of the template.	Information Governance Manager	22 September 2014
1		Proof read following comment from Compliance & Risk Committee.	Information Governance Manager	16 October 2014
1		No change following review by Compliance & Risk Committee and J Baxter	Information Governance Manager	16 December 2014
3		Q-pulse numbering changed due to restructuring of the system and review date set at previous revision and table of revision amended to reflect change along with version numbers		19 January 2016
4	All	Reformatted into new template	IG Manager	Sept 2016
5	All 4 5 8 9	Full review in line with GDPR and UK Data Protection Act. Update of responsibilities. Personal data definition. Updated. Monitoring by IGWG replaced with IG Manager.	Information Governance Manager	October 2017

This page should not be longer than one single page.

Table of Contents

1. Introduction

The North East Ambulance Service NHS Foundation Trust (Trust) 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.

The Trust therefore has a responsibility to ensure that information is managed appropriately and in accordance with Information Governance (IG) requirements.

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 personal information, is managed efficiently, securely, effectively and in accordance with relevant legislation, with the objective of delivering the best possible care and service.

The Trust will establish and maintain policies and procedures to ensure compliance with requirements contained in the Data Security and Protection Toolkit.

This policy respects and complies with the applicable laws and standards including (but not limited to):

- UK Data Protection Legislation
- EU General Data protection Regulation 2016
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Department of Health Records Management: NHS Code of Practice
- Common Law Duty of Confidentiality
- Information Security Management Standard ISO 27001

2. Purpose

This policy outlines 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

This policy covers all sites and systems operating and utilised by the Trust.

The policy applies to any individual employed, in any capacity, by the Trust, and any volunteer or contractor who holds a Trust domain account.

This policy covers all aspects of information within the Trust including but not limited to:

- Patient / client / service user information
- Staff information
- Corporate information

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the confidentiality and security of patient, staff and corporate information. Implementation of, and compliance with the policy is delegated to the Director of Finance and Resources.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

The SIRO is also responsible for making sure the trust meets all legislative requirements in relation to information security.

The SIRO 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.
- 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.

4.4 Information Asset Owners (IAOs)

IAOs will be a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

IAOs have a responsibility to:

- Leading and fostering and 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 and authorising 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.

4.5 Caldicott Guardian

Director of Director of Quality and Safety (Executive Nurse) is also the Caldicott Guardian who 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.

4.6 Information Governance Manager

The Information Governance Manager is also the Trust Data Protection Officer and has responsibility for:

- Developing, maintaining and implementing this policy.
- Working with line managers and risk management leads in the investigation of potential breaches of this policy.
- Providing specialist information governance advice ensuring systems are in place to monitor, control and record compliance with EU General Data Protection Regulation.
- Leading the strategic development of policies, procedures and standards relating to information governance.
- Raising awareness and acceptance of high quality information governance standards, enabling information governance to be successfully embedded into the organisation.
- Providing assurance to the executive board that the Trust is meeting the mandatory and best practice guidelines as required for Information Governance in the following areas:-
    - Data Protection
    - Data Security and Protection Toolkit
    - Information Security
    - Records Management

4.7 Line Managers

Line managers have a responsibility to ensure all current, new and temporary staff attend induction programme and receive Mandatory Information Governance Training on an annual basis.

4.8 All staff

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 in relation to information governance.
- 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. Glossary of Terms

This policy uses the following terms:

Term	Description
Personal data	Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[1]
Information Assets	• 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.

[1] EU General Data Protection Regulation 2016

6. Policy Content

6.1 General Information Governance

The Trust will establish, maintain and review policies and procedures for the effective and secure management of all information assets and resources.

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.

All new processes, services, information systems, and other relevant information assets will require consultation with the IG Manager to ensure a robust IG assessment is carried out to identify and information or privacy risks.

The Trust will assess its performance in IG using the Data Security and Protection Toolkit to help develop and implement action plans to ensure continued improvement in this area.

The Trust 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.

6.2 Information Risk Management

The Trust will ensure the effective implementation of an information risk framework that identifies information assets and their owners.

Risk assessments will be conducted to ensure appropriate and effective security is in place for each information asset.

6.3 Openness

The Trust recognises the need to maintain an appropriate balance between openness and confidentiality in the management and use of information.

The Trust 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.

Corporate information of the Trust will be available to the public in line with the Code of Practice on Openness in the NHS and in accordance with the Freedom of Information Act 2000.

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

6.4 Disclosure of information

Patients will have access to information relating to their own health care through clear procedures for handling subject access requests.

The Trust recognises the need to share personal information with partner organisations and other agencies in line with the Data Protection Act and Caldicott principles. The Information Sharing Policy has been developed as guidance to staff to enable the Trust to meet its responsibilities regarding the appropriate use, sharing and disclosure of personal information.

6.5 Confidentiality and Data Protection Assurance

The Trust regards all personal information as confidential except where national policy or law on accountability and openness requires otherwise.

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.

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

6.6 Information Security Assurance

The Trust will undertake or commission regular audits to assess information and security arrangements in keeping with profession, legislative and statutory requirements.

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.

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

6.7 Information Quality and Assurance

The Trust 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.

IAOs will take ownership of, and seek to improve, the quality of data within their services.

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.

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

6.8 Secondary Uses Services

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

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

6.9 Transfer of Information

The Transfer of Personal Information Policy provides staff with guidance on how to transfer personal information securely in line with national and local best practice and legislative requirements, e.g. the use of safe haven fax and encryption.

7. Training Required for Compliance with this Policy

All staff to receive Mandatory Information Governance Training on an annual basis.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager,
What are you monitoring?	Compliance against the Data Security and Protection Toolkit requirements.
When will the monitoring be performed?	Bi-monthly
How are you going to monitor?	Using the online monitoring tool provided by NHS Digital.
What will happen if any shortfalls are identified?	Iidentified as risk and reported to the Information Governance Working Group
Where will the results of the monitoring be reported?	Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	Highlight reports will be progressed by the Information Security Working Group and monitored by the Finance Committee.
How will learning take place	Annual review of toolkit submission.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	**Monitoring and audit**					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Compliance with Trust policy template, format and ratification process	• Style, format and template • Explanation of terms used • Consultation process • Ratification process • Review arrangements • Control, including archiving arrangements • Associated documents • Supporting references • Monitoring section in policy	Assessing all new and reviewed policies against the guidance through presentation to relevant approval groups	Author and approval groups	Finance Committee	Ongoing	To be developed as necessary
Monitoring and reporting on Policy compliance	Meeting the requirements of each of the Data Security and Protection Toolkit requirements.	Self assessment toolkit.	Information Governance Manager	Information Governance Working Group	Bi-monthly	Monitor via Action Plans

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with:

- Information Governance Working Group
- Senior Information Risk Owner
- Caldicott Guardian

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings

12. References

This document refers to the following guidance, including national and international standards:

- UK Data Protection Legislation http://www.legislation.gov.uk/ukpga/1998/29/contents
- EU General Data Protection Regulation 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Freedom of Information Act 2000 (FOI) http://www.legislation.gov.uk/ukpga/2000/36/contents
- Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents
- Department of Health Records Management: NHS Code of Practice
- Information Security Management ISO 27001 http://www.bsigroup.com/en-GB/iso-27001-information-security/introduction-to-iso-27001/
- Caldicott National Data Guardian report https://www.gov.uk/government/organisations/national-data-guardian
- Health and Social Care Act 2010 http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

13. Associated Documentation

This policy refers to the following Trust documents:

- Information Risk Policy POL-F-IMT-6
- Information Sharing Policy POL-F-IMT- 8
- Transfer of Personal Information Policy POL-F-IMT-11