North East Ambulance Service NHS
NHS Foundation Trust

Information Sharing Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-8
Version Number	02
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director – Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	15 February 2018
Date Policy Effective From	08 March 2018
Next Review Date	08 March 2021
Keywords	Secure, transfer, Information Sharing Agreement, ISA, person identifiable information, data transfer, confidential information sharing

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
2	All	Document reviewed and refreshed in line with GDPR	IG Officer	Nov 2017
2	All	• Full review in line with GDPR and UK Data Protection Act. • Section 9 Monitoring by IGWG replaced with IG Manager.	IG Manager	Jan 2018

This page should not be longer than one single page.

Table of Contents

1. Introduction

This Information Sharing Policy sets out the requirements for staff when sharing personal information within the NHS and between the NHS and other bodies.

Information sharing can take the form of:

- A reciprocal exchange of data.
- One or more organisations providing data to a third party or parties.
- Several organisations pooling information and making it available to each other.
- Several organisations pooling information and making it available to a third party or parties.
- Exceptional, one-off disclosures of data in unexpected or emergency situations.

The key statutory requirement for NHS compliance with personal information sharing is the Data Protection Act (DPA) and EU General Data Protection Regulation 2016 (GDPR). They provide a broad framework of general standards that have to be met and considered while managing (including but not limited to collecting, processing, storing and deleting) all personal information in conjunction with other legal obligations.

The Trust will comply with the following legislation and other legislation as appropriate:

- General Data Protection Regulation 2016
- The Data Protection Act
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Computer Misuse Act (1990)
- Human Rights Act (1998)
- Investigatory Powers Act 2016
- Freedom of Information Act 2000
- Fraud Act 2006
- Crime and Disorder Act (1998)
- Health and Social Care Act 2015

2. Purpose

Information sharing is the key to the Government’s goal of delivering better, more effective public services. It is particularly important to enable early intervention and prevention, safeguarding and public protection. It is important that the public are confident that their personal information is being kept safe and secure and that staff maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that staff are able to share information appropriately as part of their day-to-day work with appropriate safeguards.

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

This policy does not apply to information that does not fall within the scope of the DPA or GDPR.

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 and staff 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 sharing.

4.4 Director of Quality and Safety (Executive Nurse)

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.

4.5 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.

The IAO is responsible putting in place sharing agreements with 3rd parties.

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.
- Provide support to IAOs in completing sharing agreements and privacy impact assessments.
- Reviewing information sharing agreements and keeping a register of sharing agreements.
- Ensuring privacy notices are kept up to date.

4.7 All staff

All staff have a responsibility to:

- Adhere to this policy where there is a need to share information with external organisations.
- Adhere to the relevant legislation in relation to information sharing.
- Raise any concerns in relation to information sharing with their line manager or the Information Governance Manager.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Anonymised information	Information that cannot identify an individual.
Direct Care	Clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals
Data Protection Impact Assessment (DPIA)	A process which helps to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.
Information Asset Owner	Senior individual involved in the provision of service. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the Senior Information

Term	Description
	Risk Owner (SIRO) on the security and use of those assets.
Information Asset (IA) and register	Are identifiable and definable assets owned or contracted by an organisation which are valuable to the organisation. The register will likely include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data.
Information Sharing Agreement (ISA)	A set of common rules binding on all the organisations involved in a data sharing initiative. It is not contractually binding but is used to set good practice standards that the parties need to meet in order to fulfil any duty of care which exists in relation to the regular/routine sharing of personal information.
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 to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.[1]
Routine flows	Any flows or transfers of information that are undertaken on a regular basis; 'regular' in this context could be as infrequently as once a year.

6. Policy Content

6.1 Sharing personal information with other organisations

This policy covers two main types of information sharing:

- Systematic - routine information sharing where the same data sets are shared between the same organisations for an established purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.
- Ad hoc - one-off decisions to share information for any of a range of purposes. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation. All ad-hoc or one-off sharing decisions must be carefully considered and documented.

Information may be shared in the following ways (subject to patient consent):

- To manage healthcare within the NHS;
- Auditing NHS accounts and services;
- Investigating complaints, incidents and legal claims;
- Reviewing care to ensure it is of the highest standards;

[1] EU General Data Protection Regulation 2016

- Preparing data for performance management;
- Research and Development;
- Teaching and training of healthcare professionals;
- Where information is required by statute or court order;
- In the public interest in order to protect the health or safety of patients, their families or the wider community.
- Ensure that commissioning meets the current and future care meets the needs of service users;

6.2 General considerations for information sharing

- Could the objective be achieved without sharing the data or by anonymising it? It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- What information needs to be shared? You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives.

- Who requires access to the shared personal data? You should employ 'need to know' principles, meaning individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- When should it be shared? Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

- How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- How can we check the sharing is achieving its objectives? You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- How are individuals made aware of the information sharing? Consider what to tell the individuals concerned. Is their consent needed? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the individual's rights are respected and can be exercised e.g. how can they access the information held once shared?

- What risk to the individual and/or the organisation does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

.

6.3 Information Sharing Agreement

Information sharing agreements are one way of ensuring that those organisations involved in information sharing have considered all the potential information governance issues around this sharing and are adhering to the current legal framework.

Not having an information sharing agreement does not mean that information cannot be shared. As long as information sharing is being carried out legally, information sharing can occur. This approach is supported by the Information Commissioners Office. It is not a useful tool for managing the ad hoc information sharing which all practitioners find necessary.

6.4 When is an Information Sharing Agreement required?

Any routine sharing of information for direct care purpose do not need Information Sharing Agreements. However, an agreement should be considered for sharing for non-care purpose e.g. for purposes including commissioning, healthcare development, improving NHS resource efficiency etc. This is because the purposes for sharing need to be defined and limited, and additional requirements such as recorded informed consent or evidence of support under section 251 of the NHS Act 2006 (formerly section 60 of the Health & Social Care Act 2001), may be required to enable lawful sharing.

6.5 Data Privacy Impact Assessments (DPIA)

Before entering into any data sharing agreement, a Data Privacy Impact Assessment (DPIA) should be carried out in order to assess the benefits the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects such as an erosion of personal privacy or the likelihood of damage or distress to data subjects.

Information Governance Manager will be able to advice further on conducting a DPIA.

6.6 Bodies with which we normally share information

- Hospitals and other care providers.
- Local authorities and social care providers.
- Police, coroners and Court.

6.7 NHS Protect

NHS Protect operates under the authority of the Secretary of State for Health Directions on Countering Fraud in the NHS. This direction places specific duties upon the Trust to make available to NHS Protect any files or data as required in the pursuance of its counter fraud function. In addition, it has statutory powers conferred by the NHS Act 2006 that require the production of any documents containing information relevant to the exercise of any of its functions, further advice can be sought from the Local Counter fraud team.

6.8 Emergency Planning

The DPA does not prevent organisations from sharing personal data in emergency response situations, but the type of information likely to be shared should be considered in the form of an ISA, factoring in the risk of not sharing data under such circumstances.

6.9 Complaints

A complaint from a data subject or their representative about information shared will be investigated first by the organisation(s) that are party to the information sharing. The Trust will assume responsibility for communications with the complainant in the first instance. More information on the procedure is available in the Complaints Policy.

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?	Where systematic sharing of information is taking place, as reported by the information flows, there an up to date ISA in place and DPIA. Data protection breaches are checked against the information flows.
When will the monitoring be performed?	When incidents occur.
How are you going to monitor?	Incidents reports against the information flows.
What will happen if any shortfalls are identified?	Identify any risks in the information flow.
Where will the results of the monitoring be reported?	Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	Assessment of the risk with the IAO and report back to the working group.
How will learning take place	Recommendations from the working group and identifying any additional training.

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**
	Information sharing register is up to date Number of data sharing incidents	Via Ulysses reports.	Information Governance Manager.	Information Governance Working Group.	When incidents occur.	Learning will be via the action plans and monitored by Information Governance Manager.

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

- Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
- General Data Protection Regulation2016
- 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:

- Secure Transfer of Information Policy POL-F-IMT-11
- Information Governance Policy POL-F-IMT-3
- Complaints Policy
- Safeguarding Policy
- Data Protection Impact Assessment Guidance
- Information Sharing Agreement

14. Appendices

14.1 Information Sharing Agreement

Information%20Sharing%20Agreement%