

The Newcastle upon Tyne Hospitals NHS Foundation Trust

Information Governance Policy

Effective: March 2011

Review: March 2013

1. Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

The policy applies to The Newcastle upon Tyne Hospitals NHS Foundation Trust (the Trust), to all people who work in the Trust, including employees, honorary contract holders, researchers, trainees, clinical observers and other contractors or individuals involved in patient care and covers e-mail and messaging systems used or accessed through Trust computers and servers if these systems are under the jurisdiction and/or ownership of the Trust.

A List of relevant Trust policies is included in Appendix A (IG Framework)

2. Principles

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personally identifiable information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

2.1. Openness

- Non-confidential information about the Trust and its services should be available to the public through a variety of media, in line with the Department of Health Code of Openness.
- The Trust maintains policies to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Trust has clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust has clear procedures and arrangements for handling queries from patients and the public.

2.2. Legal Compliance

- The Trust regards all personally identifiable information relating to patients as confidential.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust regards all personally identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust has in place policies to ensure compliance with the Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998 and the common law of confidentiality.
- The Trust has established policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act 2008, Crime and Disorder Act 1998, Protection of Children Act 1999).

2.3. Information Security

- The Trust has policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust promotes effective confidentiality and security practice to its staff through policies, procedures and training.
- The Trust has in place explicit incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.

2.4. Information Quality Assurance

- The Trust has established and maintains policies and procedures for information quality assurance and the effective management of records.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards are set through clear and consistent definition of data items, in accordance with national standards.
- The Trust promotes information quality and effective records management through policies, procedures/user manuals and training.

3. Responsibilities

The Trust Information Governance Framework, outlining roles and responsibilities is attached as Appendix A to this policy.

It is the role of the Information Governance Committee to define the Trust's policy in respect of Information Governance, taking into account legal and NHS requirements. The Board of Directors is responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Information Governance Working Group is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Trust and raising awareness of Information Governance.

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

4. Contact Point

Questions about this policy may be directed to the Senior Information Governance Officer.

5. Audit and Monitoring

Trust compliance with this policy is ongoing as part of the Information Governance Toolkit requirements and submissions.

6. Disciplinary process

Any breach of this policy may lead to action under the Trust [Disciplinary Policy/Procedure](#).

7. Review

The Head of Information Security and Governance, Senior Information Risk Owner (Trust Secretary) and the Caldicott Guardian (Medical Director) are responsible for the review and amendment of this policy. The policy will be reviewed and refreshed as required at least every two years.

Policy author: Senior Information Governance Officer.

The Newcastle upon Tyne Hospitals NHS Foundation Trust Information Governance Framework

This document outlines the Trust's structure for the management and reporting of Information Governance.

Key Personnel

- IG Lead and Head of Information Governance and IT Security – Richard Oliver
- Senior Information Risk Owner (SIRO) and Trust Secretary – Steven Reed
- Medical Director and Caldicott Guardian – Dr Tim Walls
- Privacy Officer – Lorraine Gray.
- Senior Information Governance Officer – Fay O'Sullivan

Key Policies

- Over-arching IG Policy (This Policy)
- Data Protection Act 1998/Confidentiality Policy
- Organisation Information Security Policy
- Information Lifecycle Management Policy
- Corporate Governance Policy
- Registration Authority (RA) Policy
- Reporting and Management of Serious Untoward Incidents.
- Freedom of Information and Environmental Information Regulations Policy
- Confidentiality and Security Policy
- Risk Management Strategy

Key Information Governance Bodies

IG Committee: Reporting to Board of Directors. Membership from Clinical Departments, Human Resources, Finance, Data Quality, Patient Relations and Risk.

IG Working Group: Reporting to committee and with responsibilities for toolkit returns and actions. All departments represented.

ISSB: Information Systems Strategy Board

CRAC: Clinical Records Advisory Committee

CGARD: Clinical Governance and Risk Department

Resources

IG Lead - Responsibility for all governance issues and legal requirements.

SIRO - Information Risk Manager for the organisation.

Caldicott Guardian - Board level sponsor for all Patient Information within the Organisation

Privacy Officer - Responsible for patient level alerts or incidents.

Senior Information Governance Officer - Management of evidence for toolkit and submissions.

Governance Framework

Information systems are recorded within the Trust Service catalogue and Information Asset owners identified within the catalogue.

The IG Lead and Senior Information Governance Officer assist the Caldicott Guardian with the day to day handling of Caldicott approval requests.

Training and Guidance

Information Governance training for all staff is mandated through the IG Training Tool.

Staff sign confidentiality code of conduct and acceptable use declaration.

All Policies are available to all staff.

Incident reporting and risk management policies and Training are provided.

THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST
IMPACT ASSESSMENT – SCREENING FORM A

This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Policy Title:	Information Governance Policy	Policy Author:	Richard Oliver
		Yes/No?	You must provide evidence to support your response:
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	This policy re-iterates the NHS policy on data transfer.
	• Ethnic origins (including gypsies and travellers)	No	Ditto
	• Nationality	No	Ditto
	• Gender	No	Ditto
	• Culture	No	Ditto
	• Religion or belief	No	Ditto
	• Sexual orientation including lesbian, gay and bisexual people	No	Ditto
	• Age	No	Ditto
	• Disability – learning difficulties, physical disability, sensory impairment and mental health problems.	No	Ditto
2.	Is there any evidence that some groups are affected differently?	No	Ditto
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?		
4(a).	Is the impact of the policy/guidance likely to be negative? (If "yes", please answer sections 4(b) to 4(d)).	No	Ditto
4(b).	If so can the impact be avoided?		
4(c).	What alternatives are there to achieving the policy/guidance without the impact?		
4(d).	Can we reduce the impact by taking different action?		

Comments:	Action Plan due (or Not Applicable): Not Applicable.
------------------	--

Name and Designation of Person responsible for completion of this form: Richard Oliver Head of Information Security & Governance.....Date:.....18 Feb 2011.....

Names & Designations of those involved in the impact assessment screening process:.....Steven Read Chairman IG Committee – Tim Walls Caldicott Guardian.....

(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified on this form, please refer to the Policy Author identified above, together