

Directorate of Performance Assurance

INFORMATION GOVERNANCE POLICY

Reference:	DCP074
Version:	2.5
This version issued:	27/03/15
Result of last review:	Minor changes
Date approved by owner (if applicable):	N/A
Date approved:	09/02/15
Approving body:	Information Governance Committee
Date for review:	March, 2018
Owner:	Wendy Booth, Director of Performance Assurance
Document type:	Policy
Number of pages:	9 (including front sheet)
Author / Contact:	Jill Mill, Head of Risk Management

Northern Lincolnshire and Goole NHS Foundation Trust actively seeks to promote equality of opportunity. The Trust seeks to ensure that no employee, service user, or member of the public is unlawfully discriminated against for any reason, including the "protected characteristics" as defined in the Equality Act 2010. These principles will be expected to be upheld by all who act on behalf of the Trust, with respect to all aspects of Equality.

Contents

Section	Page
1.0 Purpose.....	3
2.0 Policy Principles.....	3
3.0 Area	3
4.0 Duties.....	4
5.0 Openness.....	5
6.0 Legal Compliance	5
7.0 Information Security	6
8.0 Information Quality Assurance	6
9.0 Monitoring Compliance and Effectiveness	6
10.0 Associated Documents	7
11.0 References.....	7
12.0 Definitions	7
13.0 Consultation	7
14.0 Dissemination	7
15.0 Communication	8
16.0 Equality Act (2010).....	8
Appendix A - Information Governance Roles and Responsibilities	9

1.0 Purpose

- 1.1 The aim of this policy is to provide the employees of Northern Lincolnshire and Goole NHS Foundation Trust with a simple framework through which the elements of Information Governance will be met.
- 1.2 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.
- 1.3 It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

2.0 Policy Principles

- 2.1 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 personal information about patients and staff and commercially sensitive information.
- 2.2 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.
- 2.3 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 clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.
- 2.4 There are 4 key interlinked strands to the information governance policy:
- Openness, transparency and trace-ability
 - Legal compliance
 - Information security
 - Quality assurance

3.0 Area

- 3.1 The policy covers all aspects of information within the organisation, including but not limited to:
- Patient/Client/Service user information
 - Personnel information
 - Organisational information

3.2 This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems – paper and electronic
- Transmission of information – fax, e-mail, post and telephone

3.3 This policy covers all information systems purchased, developed and managed by on behalf of the organisation, and any individual directly employed or otherwise by the organisation.

4.0 Duties

4.1 The roles and responsibilities are detailed in appendix A.

4.2 Chief Executive

The Chief Executive has overall accountability for ensuring that there are appropriate arrangements are in place for governing of all information processed within the Trust.

4.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is the Trust Information Governance Lead and is tasked with the responsibility for information risk at board level. The SIRO is responsible for ensuring that the organisational information risk is properly identified, managed and that the appropriate assurance mechanisms exist.

4.4 Caldicott Guardian

The Head of Governance is the designated Caldicott Guardian with responsibility for providing the organisation with advice on agreeing and policies governing the confidential management and movement of identifiable information and images within and beyond the Trust. The Caldicott Guardian is the Trust lead for the Confidentiality and Data Protection Assurance and signs off the agenda annually. The Caldicott Guardian is responsible for advising on appropriate sharing of personal identifiable information throughout the organisation and is lead for the Confidentiality and Data Protection Assurance Agenda in the Information Governance Toolkit.

4.5 Trust Information Security Officer

The designated Information Security Officer is the Deputy Director of Information and Information Technology and has the responsibility for maintaining information security within the organisation. The information security officer is also tasked with the responsibility of leading the Information Security Agenda.

4.6 All Managers

All managers are responsible for ensuring that their staff are adequately trained and conform to the Information Governance Policy and this associated strategy.

4.7 All Staff

All staff have a responsibility to adhere to all information governance standards which is written in the duty of confidence statement and as per their terms of employment.

5.0 Openness

- 5.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- 5.2 Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act. Non-confidential information on the Trust and its services will be available to the public through a variety of media, including its internet based Publication Scheme, in line with the Trust's code of openness.
- 5.3 The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- 5.4 Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- 5.5 Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- 5.6 The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- 5.7 The Trust will have clear procedures and arrangements for handling queries from patients and the public.
- 5.8 Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.
- 5.9 Information Governance training including awareness and understanding of Caldicott principles, confidentiality, information security and data protection will be mandatory for all staff.

6.0 Legal Compliance

- 6.1 The Trust regards all identifiable personal information relating to patients as confidential.
- 6.2 The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- 6.3 The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- 6.4 The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and common law confidentiality.
- 6.5 The Trust will establish and maintain 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, Crime and Disorder Act, Protection of Children Act).

7.0 Information Security

- 7.1** The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- 7.2** In the event of the transfer of personal information to countries outside of the UK, this will be undertaken in accordance with the Data Protection Act 1998 and Department of Health guidelines.
- 7.3** The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- 7.4** The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training.
- 7.5** The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

8.0 Information Quality Assurance

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

9.0 Monitoring Compliance and Effectiveness

- 9.1** The Deputy Director of Clinical and Quality Assurance and Assistant Trust Secretary will chair an Information Governance Committee, meeting at least bi-monthly and reporting to the Trust Governance Committee (a sub-committee of the Board), which will monitor compliance with, and review this policy on a 3 yearly basis.
- 9.2** The Information Governance Committee is responsible for overseeing day to day information governance issues; developing and maintaining policies, procedures and guidance, coordinating Information Governance in the Trust and raising awareness of Information Governance.

9.3 The Information Governance Committee will receive regular reports on the implementation of the Information Governance Toolkit annual self-assessment and associated action plans giving auditable evidence of the Trust's compliance with the Information Governance Agenda.

10.0 Associated Documents

10.1 Freedom of Information Individual Access Policy.

10.2 Confidentiality Policy.

10.3 Information Security Policy.

10.4 Health Records Management Policy & Strategy.

10.5 Data Quality Policy.

10.6 Destruction and Retention Policy - Clinical Health Records.

10.7 Non-Clinical (Corporate) Records Management Policy.

10.8 Data Protection & Personal Information Fair Processing Policy.

11.0 References

11.1 Department of Health (2003) Confidentiality: NHS Code of Practice.

11.2 Connecting For Health – Information Governance Toolkit.

11.3 The Data Protection Act (1998).

11.4 Freedom of Information Act (2000).

12.0 Definitions

Information Governance Toolkit – This is an online self-assessment tool, where the Trust is obligated to demonstrate compliance with standards required by Connecting for Health on an annual basis.

13.0 Consultation

Information Governance Committee.

14.0 Dissemination

This policy will be disseminated to all staff via the intranet.

15.0 Communication

Information Governance Newsletters will be produced regularly including an annual update for all staff. Newsletters will be disseminated via Trust intranet and via line managers for staff who do not have regular access to intranet pages.

16.0 Equality Act (2010)

- 16.1** In accordance with the Equality Act (2010), the Trust will make reasonable adjustments to the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Trust will endeavour to develop an environment within which individuals feel able to disclose any disability or condition which may have a long term and substantial effect on their ability to carry out their normal day to day activities.
- 16.2** The Trust will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Trust's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010).

**The electronic master copy of this document is held by Document Control,
Directorate of Performance Assurance, NL&G NHS Foundation Trust.**

Appendix A

Information Governance Roles and Responsibilities

