Heart of England NHS
NHS Foundation Trust

Information Governance Policy v 6

Document reference:	POL001
Document Type:	Policy
Version:	6
Purpose:	All staff are responsible for ensuring that information is managed in a confidential and secure manner. This document is an overarching policy encompassing the principles of Information Governance in the Trust. Staff should refer to the related Information Governance Policies and Procedures for further guidance
Responsible Directorate:	Corporate Affairs
Executive Sponsor:	Director of Corporate Affairs
Document Author:	Head of Information Governance
Approved by:	Chief Executive
Date Approved:	05 September 2016
Review Date:	30 September 2018
Related Controlled documents	• Confidentiality policy • Freedom of information policy • Incident reporting policy and procedure • Locally managed records procedure • Record keeping in healthcare records policy • Records management policy • Retention and disposal of records policy • Safe haven procedure • Data protection policy • Access to health records policy • Acceptable use of ICT • Network and IT security • Mobile computing • Information risk management policy
Relevant External Standards/ Legislation	• Records Management: NHS Code of Practice • Confidentiality: NHS Code of Practice • Information Security Management: NHS Code of Practice • Care Quality Commission fundamental standards • Information Governance Toolkit

	• Information Commissioner's Office • Monitor • Caldicott Guardian Manual • Data Protection Act 1998 • Freedom of Information Act 2000 • Public Interest Disclosure Act 1998 • Common Law of Confidentiality • Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998) • Human Rights Act 1998 • Mental Capacity Act
Target Audience:	All staff
Further information:	Available from the Information Governance team

Paper Copies of this Document

If you are reading a printed copy of this document you should check the Trust's Policy website (http://sharepoint/policies) to ensure that you are using the most current version.

Version History:

Version No.	Date of Release	Document Author	Ratified by	Date Ratified
V1.0	August 2007	Information Governance Policy	IGC	August 2007
V1.1	February 2008	Information Governance Policy	IGC	February 2008
V3.0	January 2010	Information Governance Manager	Director of Safety and Governance	January 2010
V4.0	June 2010	Information Governance Manager	Director of Safety and Governance	January 2011
V5.0	January 2013	Information Governance Manager	IGC	January 2013
V5.1	August 2016	Interim Head of Information Governance	IG Group	August 2016
V6.0	Septemb er 2016	Interim Head of Information Governance	Policy Review Group	September 2016

Summary of changes from last version:

Minor changes to bring in line with new organisational structure

Table of Contents

1. Introduction / Purpose

This policy sets out the Trust approach for the management of information. Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It is essential that the Trust protects this key asset and ensures that appropriate policies, procedures and management accountability is in place to provide a robust governance framework for information management.

This Information Governance Policy is supported by the Information Governance strategy and other policies relating to the various aspects of Information Governance including:

- Confidentiality policy
- Freedom of information policy
- Incident reporting policy and procedure
- Locally managed records procedure
- Record keeping in healthcare records policy
- Records management policy
- Retention and disposal of records policy
- Safe haven procedure
- Data protection policy
- Access to health records policy
- Acceptable use of ICT

- Network and IT security
- Mobile computing
- Information risk management policy

The purpose of this policy is to describe the arrangements for providing assurance to the Board of Directors and to the Trusts patients and public that Information Governance standards are defined and that processes are in place to monitor effective implementation of the information governance framework.

2. Policy Statement

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality care. It recognises its public accountability, but equally places importance on confidentiality of both personal information about staff and patients and commercially sensitive information. The Trust recognises the need to share patient information with other health organisations and other agencies who work in partnership to deliver care and will do so in a secure manner that is consistent with the interests of the patient and the public interest.

All staff are required to:

- ✓ Share relevant information to support the delivery of high quality patient care;
- ✓ Keep records in accordance with the record keeping policy;
- ✓ Transfer information securely;
- ✓ Complete mandatory IG training annually;
- ✓ Report and investigate incidents where compliance with IG principles have not been adhered to.

Staff should not:

- ✓ Allow personal and sentitive information to be shared inappropriately or insecurely;
- ✓ Fax information without first checking the number and confirm delivery;
- ✓ Access their own medical records, those of family and friends or any other records where they are not required to unless it is directly related to the care that they are providing;

3. Definitions

Personal information (or data)
Personal information or data means data which relate to a living individual who can be identified:
(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data
Means personal data consisting of information as to

(a) the racial or ethnic origin of the data subject,
(b) political opinions,
(c) religious beliefs or other beliefs of a similar nature,
(d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) physical or mental health or condition,
(f) sexual life,
(g) the commission or alleged commission of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

4. Policy Requirements

4.1 Information Governance Management

A separate Information Governance Strategy aims to ensure that the Trusts primary objectives of information governance are achieved.

The Trust has clear lines of accountability throughout the organisation for Information Governance that lead directly to the Board. The information governance lead for the trust is the Director of Corporate Affairs. The Head of IG is responsible for advising upon and co-ordinating an effective approach to information governance, in close collaboration with the Executive Directors. The Head of IG is responsible for day to day management of Information Governance Toolkit (IGT), Freedom of Information (FOI), Data Protection Act (DPA) and confidentiality.

APPENDIX 1 summarises the accountability framework for IG management in the Trust
APPENDIX 2 includes the Terms of Reference for the Information Governance Group

The Trust will assess its performance against the requirements of the IGT, reporting compliance to the Department of Health and the Board of Directors in line with the nationally defined timeframes. The Trust will also aim to continually improve its levels of compliance in line with the aims and objectives outlined in the Information Governance strategy.

The Trust will provide training for all staff as outlined in the Training Needs Analysis (see section 6) to provide them with the knowledge and skills require to implement the IG framework and reduce the number of incidents occurring from IG breaches.

4.2 Confidentiality and Data Protection

The Trust has a legal duty to keep all identifiable personal information relating to patients and staff confidential and secure. This obligation arises out of the common law duty of confidentiality and professional obligations. The Trust acknowledges this responsibility and all contracts including staff employment contracts and contracts with third parties will refer to this obligation.

4.3 Legal compliance

The Trust will manage all patient identifiable information in accordance with the law and duty of confidence. It will also manage information relating to staff as confidential, except where the law requires otherwise.

The Trust maintains policies to ensure compliance with the Data Protection Act, Human Rights Act, confidentiality and the Freedom of Information Act. It also has arrangements in place for ensuring the safe and secure transfer of personal and sensitive information with other agencies and partners involved in the delivery of healthcare.

4.4 Information Security

In line with the Data Protection Act (principle 7) all staff should ensure that all person-identifiable information is protected by appropriate security. In particular

- bulk transfers of any personal data must not be made unless it is absolutely necessary;
- data must be secured in transit by the use of passwords or encryption;
- Personal data should not be held on portable devices (laptops, CDs, USB sticks) unnecessarily and must be encrypted

Any instances of actual or potential breaches of confidentiality and security must be reported using the Trust's Incident Reporting policy and Risk Management policy.

4.5 Openness

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

Confidential information will be underpinned by Caldicott principles and the Data Protection Act and Freedom of Information Acts.

Patients have ready access to their information relating to their own healthcare, their options for treatment and their rights as patients to enable them to make informed choices.

Non-confidential information on the Trust and its services is available to the public through a variety of media, including the Publication Scheme in line with the Trust's Freedom of Information Policy. In the event of any queries relating to Freedom of Information staff should contact the Information Governance Manager.

The Trust publishes clear procedures and arrangements for handling requests for information from patients and the public.

4.6 Information / Data Quality Assurance

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care.

All staff have a responsibility to ensure and promote the quality of information that they obtain, record and use.

Managers should take ownership for ensuring the continuous improvement of the quality of information within their services. The Trust has clear policies and procedures in place as well as training opportunities to enable staff to achieve this.
The Trust is committed to achieving compliance with the IGT standards related to ongoing continuous improvement in the use of information.

4.7 Information Governance Toolkit

NHS Connecting for Health (CfH)[1] set standards for information governance in NHS organisations and performance is self assessed annually through the electronic submission of evidence to CfH using the Information Governance Toolkit.

The Head of IG works with the standard leads to ensure that the Trust has the systems, processes, policies and procedures in place to deliver effective information governance. The Information governance toolkit will be subject to an annual internal audit.

Compliance with the toolkit submissions will be reported to the Information Governance Group and the Board of Directors.

5. Responsibilities

[1] NHS Connecting for Health supports the NHS to deliver better, safer care to patients, via new computer systems and services, that link GPs and community services to hospitals.

Chief Executive
The Chief Executive has delegated responsibility to the Director of Corporate Affairs for implementation and review of this policy.

Director of Corporate Affairs
The Director of Corporate Affairs is the executive responsible for Information Governance within the Trust.

Caldicott Guardian
The Associate Medical Director undertakes the role of Caldicott Guardian. S/he has particular responsibility for ensuring the appropriate disclosure of patient information and where required will become directly involved with the decision to disclose or withhold information.

SIRO
The key responsibilities of the SIRO are to:

- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework;
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control;
- Review and agree action in respect of identified information risks;
- Ensure that the organisation's 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.

All Directors, Heads of Service and Managers
All Directors, Heads of Service and Managers will be responsible for ensuring that this policy is communicated and implemented within their area of responsibility and that the principles and standards which constitute good Information Governance are adopted and are followed on a day to day basis.

Head of Information Governance
The Head of IG has day to day responsibility for advising upon and co-ordinating information governance in conjunction with other relevant personnel. The Trust Information Governance Manager will provide reports to the Director of Corporate Affairs as required, detailing any risk issues. She/he will be responsible for providing reports to the Information Governance Group.

All staff and Contractors

All staff should be aware of their own personal responsibilities for Information Governance and compliance with the law. Contractors are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these. The Information Governance Team is the point of contact for any information governance issues.

Information Governance Group
The Information Governance Group is responsible for overseeing day to day information governance issues, developing and maintaining information governance related policies, standards, procedures and guidance; coordinating information governance in the Trust and raising awareness of information governance and confidentiality issues. It provides assurance to Board of Directors via the Director of Corporate Affairs.

6. Training

All Information Governance training is to be completed on an annual basis in line with the Information Governance Toolkit (95% target). Information governance training is **provided via the Trusts mandatory training programme** Completion of specialist training on the Health & Social Care Information Centre's website is required for specific job roles within the Trust. All the required training is included in the Training Needs Analysis below:-

	Introduction to IG/IG Refresher	Access to Health Records Management	Risk Management for SIROs and IAOs	Records Management in the NHS	Caldicott Training
All Staff	✓				
SAR Co-Ordinators	✓	✓		✓	
IAOs	✓		✓	✓	
IAAs	✓		✓	✓	
SIRO	✓		✓	✓	
Deputy SIRO	✓		✓	✓	
Caldicott Guardian	✓		✓	✓	✓
Deputy Caldicott Guardian	✓		✓	✓	✓

7. Monitoring and Review Matrix

This document will be reviewed on an annual basis, or sooner in the light of organisational, legislative or other changes.

Minimum Requirement	Frequency	Process for Monitoring e.g. audit	Evidence	Responsible Individual	Responsible Committee for action plan monitoring
IG Work Programme Progress	Bi-Monthly	IG Toolkit	Minutes	Head of IG	Information Governance Group
Incident Analysis	Bi-monthly	DATIX	Minutes	IG Officer	Information Governance Group
Uptake of IG Training	Bi-Monthly	Verbal update with a final report in March	Minutes and Final Report	IG Officer	Information Governance
IG Toolkit Annual Assessment	Annually for final sign-off	IG Toolkit	Assessment	Head of IG	Information Governance Group

8. References

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2013 and ISO/IEC 27001: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To share or not to share? The Information Governance Review (also known as the Caldicott 2 Review).
- Information: To share or not to share - Government Response to the Caldicott 2 Review

APPENDIX 1

BOARD OF DIRECTORS

Accountable for ensuring that the Trust has a robust IG framework in place. The Director of Corporate Affairs is the Exec with Board responsibility for IG.

⇧

CHIEF EXECUTIVES GROUP AND CEO PERFORMANCE MEETINGS WITH DIVISIONS

⇧

INFORMATION GOVERNANCE GROUP

Its responsibility is to ensure an appropriate infrastructure is implemented to monitor, maintain and improve all elements of Information Governance

APPENDIX 2

Heart of England NHS
NHS Foundation Trust

Information Governance Group Terms of Reference

Approved by: Director of Corporate Affairs September 2016

Review date: September 2017

Purpose

To ensure an appropriate infrastructure is implemented to monitor, maintain and improve all elements of Information Governance across the Trust.

Membership

- Director of Corporate Affairs (Group Chairman)
- Head of Corporate Risk and Compliance (Group Deputy Chairman)
- Head of Information Governance
- Information Governance Officer
- Director of ICT
- Information Systems Security Specialist
- Caldicott Guardian
- Deputy Chief Nurse
- Health records manager
- Divisional operational representatives
- Lead nurse - Safeguarding
- Data Quality Lead
- HR Business partner

Other staff and specialist advisers will be invited on an ad hoc basis to discuss particular topics, where appropriate.

Secretary

The IG administration assistant will be secretary to the group. They will attend all the meetings and provide appropriate support to the group chair and members. Their duties will include:-

- Agreement of the agenda with the chair, collation and circulation of papers;
- Minuting the proceedings and resolutions of all meetings of the group including recording the names of those present and in attendance - minutes shall be circulated promptly to all Members of the group; and

- Keeping a record of matters arising and issues to be carried forward.

Quorum

The Group will be quorate when a minimum of 6 members are present, including at least one (1) from each of the following three categories:

- Chairman or Deputy Chairman
- Caldicott Guardian or Deputy Caldicott Guardian or SIRO or Deputy SIRO
- Representative from ICT

Deputies with full delegated authority count toward the quorum. Deputies must be approved by the Chair prior to the meeting unless there are exceptional circumstances in which case they may be approved at the meeting.

Non-members who are not deputies may be invited to attend by the Chair

Frequency of Meetings

The Group meets bi-monthly. All members are expected to attend or send deputies who have full delegated powers. Where a member has an action to report on but cannot attend the meeting a written summary must be provided to the Head of Information Governance in accordance with the given deadline in order to ensure that the group remains updated on progress.

Notice of Meetings

Meeting dates will be arranged on an annual basis. Members of the group will be expected to attend a minimum of four meetings per year in person.

Minutes of Meetings

Agendas and briefing papers will be prepared and circulated one week in advance of the meeting allowing members time to give them due consideration.

Group meetings will be minuted with the minutes being circulated within two weeks of the meeting allowing members time to make progress on the agreed actions.

External Considerations

Information Governance Toolkit, CQC Regulations, Information Commissioners Office, Health and Social Care Information Centre and Information Legislation (in particular common law, DPA 1998, FOIA 2000, Access to Medical Records Act 1990,).

Accountability and Scheme of Delegation

The Information Governance Group is chaired by the Director of Corporate Affairs and is accountable to the Chief Executives Assurance Group. The Information Governance Group will promote effective Information Governance, maintain a framework to ensure legal compliance and promote local responsibility and accountability. This is the specialist group where key decisions are taken regarding Information Governance, the security of information and data and confidentiality.

Responsibilities

- The Information Governance Group will oversee and monitor a programme of risk management activities in relation to its specialist responsibilities. This will include a risk identification, review, management and progress/action monitoring.

- To provide direction or initiatives relating to confidentiality, data protection, information disclosure & information security.
- To advise the Executive team on all aspects of Information Governance, strategic and operational.
- To develop, implement and monitor an overarching Information Governance Strategy for the Trust and present to the Board, as required.
- To advise the Board of the existence of new external legislation and guidance which will have significant impact on the Trust.
- To oversee the development and implementation of a programme of work to achieve compliance with the Information Governance Toolkit and approve and sign off the final submission.
- To approve Information Governance related policies and monitor implementation.
- To monitor the investigation of IG Serious Incidents Requiring Investigation (SIRI) in accordance with required protocol.
- To provide specific guidance on Data Protection and Freedom of Information matters.
- To provide the Trust with assurance and guidance in relation to compliance with external regulatory requirements

Accountability and Reporting

- The IG group will provide a quarterly assurance report to the Board of Directors

- The IG group may request information from other operational groups on an ad hoc basis.

- Risks and concerns identified by the sub-groups that arise in between meetings will be escalated directly to the Chair or Vice Chair to ensure timely action/resolution.

The Group receives regular reports as detailed below;

Description	Responsibility	Frequency
Requests for Information and Information Disclosure: Status Report	Information Governance Officer	Quarterly
Incident Management and Information Security Incidents: Status Report	Information Governance Officer	Quarterly
Information Governance Toolkit: Progress report	Head of Information Governance	Bi-monthly
Report from ICT on information security issues	Information Systems Security Speciality	Bi-monthly
ICO Correspondence	IG Officer	Bi-monthly

Other Matters

The IG Group Terms of Reference will be reviewed annually