CONFIDENTIALITY MARKING

AGENDA ITEM NO:

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 24 MARCH 2011

Title:	**INFORMATION GOVERNANCE POLICY**
Responsible Director:	David Burbridge, Director Corporate Affairs
Contact:	David Burbridge, Director Corporate Affairs

Purpose:	To seek the Board of Directors' approval for the Information Governance Policy.
Confidentiality Level & Reason:	n/a
Medium Term Plan Ref:	n/a
Key Issues Summary:	This policy sets out the principles and framework for Information Governance within the Trust
Recommendations:	The Board of Directors is asked to consider and if thought fit, approve the Information Governance Policy.

Signed:	**Date:** 24 March 2011

CONFIDENTIALITY MARKING

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS
THURSDAY 24 MARCH 2011

INFORMATION GOVERNANCE POLICY

PRESENTED BY DIRECTOR OF CORPORATE AFFAIRS

1. Introduction

This policy sets out the principles and framework for the management of Information to ensure that personal and corporate information is dealt with legally, securely, effectively and efficiently to deliver the best possible care and to comply with Data Protection principles

2. Review

It has been developed in consultation with all members of the Information Governance Group.

3. Framework

3.1. This policy sets out the high level framework for Information Governance within the Trust.

3.2. This Policy focuses on the following four guiding principles:

3.2.1. Openness
3.2.2. Legal Compliance
3.2.3. Information Security
3.2.4. Information Quality Assurance

3.3 The aim of the policy is to ensure the Trust maintains a robust Information Governance framework, in accordance with Department of Health Standards, so that all information under its control is:

- Held securely and confidentially, as appropriate;
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

4. Implementation and Monitoring

4.1 All staff will receive information governance training as part of their induction and at regular intervals in accordance with the mandatory Training Policy. The training will include an assessment of their understanding.

4.2 Training compliance will be monitored by the Senior Manager Information Governance and reported to the Information Governance Group.

4.3 The Trust shall carry out an annual assessment against the Information Governance Toolkit. The process underpinning this assessment and the outcome will be overseen by IGG and reported to the Audit Committee.

4.4 Specific monitoring and audit requirements are set out in the associated policies.

5. Recommendation

The PRG reviewed this policy, considered it compliant with the Policy for the Development and Management of Controlled Documents and recommends that it is approved.

David Burbridge
Director of Corporate Affairs

CONTROLLED DOCUMENT

University Hospitals Birmingham NHS
NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE:	
This Document supports:	
Controlled Document Number:	477
Version Number:	
Controlled Document Sponsor:	Director of Corporate Affairs
Controlled Document Lead:	Senior Manager Information Governance
Approved By:	Board of Directors
On:	
Review Date:	[3 yrs]
Distribution: • Essential Reading for: • Information for:	 All Directors, Senior Managers and Department Heads All Staff

Contents

1. Policy statement

1.1. The key aim of the Information Governance Policy (this Policy) is to give assurance to the Trust and individuals that personal and corporate information is dealt with legally, securely, effectively and efficiently to deliver the best possible care and to comply with Data Protection principles.

1.2. This aim will be achieved by maintaining a robust Information Governance framework, in accordance with Department of Health Standards, so that all information under its control is:

- Held securely and confidentially, as appropriate;
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully.

2. Scope

2.1. This Policy applies to all types of information held by the Trust regardless of the media/format in which it is held and the content of such information. This includes, but is not limited to:

- Patient, client, service user information
- Staff, contractor, volunteer information
- Organisational information

2.2. This Policy further applies to all aspects of processing information, including, but not limited to;

- Receipt, creation and/or storage of information and record systems – paper and electronic
- Use of information, including accessing and disclosing
- Transmission or transfer of information, by various methods, including, but not limited to: fax, email, post, telephone, hand delivery
- Destruction or permanent preservation of information

2.3. This Policy is to be adhered to by anyone processing information for or on behalf of the Trust, including employees formally employed by the Trust or on an honorary contract, volunteers, governors, contractors, students, locum staff and agency staff.

3. Framework

3.1. This policy sets out the high level framework for Information Governance within the Trust. Specific aspects of Information Governance are dealt with in more detail in the following operational policies:

3.1.1. Record Management and Information Lifecycle Management Policy
3.1.2. Data Quality Policy
3.1.3. Information Security Policy
3.1.4. Email Policy
3.1.5. Access Control Policy
3.1.6. Freedom of Information Policy
3.1.7. Freedom of Information Policy
3.1.8. Data Protection Policy

3.2. Additional requirements and procedures are contained in procedural documents and guidelines, the key ones of which are set out in Section 8: Associated Policy and Procedural Documentation. Trust-wide procedural documents shall be approved by the DCA. Local procedural documents (i.e. documents applicable to specific departments or areas) shall be approved by the manager of the area/department concerned.

3.3. This Policy focuses on the following four guiding principles:

3.3.1. Openness
3.3.2. Legal Compliance
3.3.3. Information Security
3.3.4. Information Quality Assurance

3.4. Openness

The Trust will ensure that:

3.4.1. Patients/relatives/carers are kept informed as set out in the Being Open Procedure and Patient Information Policy and its associated procedures;

3.4.2. Non-confidential and corporate information about the Trust and its services is easily accessible through a variety of media, in line with the Freedom of Information Act 2000 and the Trust's Publication Scheme;

3.4.3. Clear procedures and arrangements are in place for handling requests for information in accordance with the Freedom of Information Act 2000 (see Freedom of Information Policy);

3.4.4. Policies and Procedures are in place for patients to be informed about the use of their personal information and to have access to information relating to their health care under the Data Protection Act 1998 or Access to Health Records Act 1990 (see Data Protection Policy);

3.4.5. Procedures are in place for staff to have access to their personal records under the Data Protection Act 1998.

3.5. Legal Compliance

The Trust will ensure that:

3.5.1. Policies and procedures to ensure compliance with the Data Protection Act 1998, the Access to Health Records Act 1990, the Freedom of Information Act 2000, the Human Rights Act 1998, the common law duty of confidentiality, Department of Health's Code of Practice on Records Management, and other appropriate legislation and regulation and all associated guidance are in place and maintained;

3.5.2. All person identifiable information relating to patients and staff is regarded as confidential except where national policy on accountability and openness requires otherwise;

3.5.3. Non-confidential Information classed as being for the benefit of the general public is accurate, up to date and easily accessible to patients and the public;

3.5.4. When personal information is shared with other individuals and/or organisations appropriate information sharing protocols are in place.

3.6. Information Security

The Trust will ensure that all information will be treated in accordance with the following three principles:

3.6.1. **Confidentiality:** Information must be secured against unauthorised access or disclosure.

3.6.2. **Integrity:** Information must be safeguarded against unauthorised modification and must be valid, accurate and complete.

3.6.3. **Availability:** Information must be accessible to authorised users at all times when they need it.

Further details are contained in the Information Security Policy and Procedure.

3.7. Information Quality

3.7.1. Information Quality relates to the completeness, accuracy, relevancy, accessibility and timeliness of all information generated by the Trust.

3.7.2. To achieve information quality the Trust will ensure that information is processed in accordance with the Trust's Records and Information Lifecycle Management Policy and Strategy and its associated guidance documents for corporate and health records and the Data Quality Policy.

4 Duties

4 .1 Chief Executive

The Chief Executive has overall responsibility for information governance within the Trust. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information governance is key to this as it will ensure the appropriate use of information.

4.2 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. He/she is responsible for ensuring patient identifiable information is used and shared in an appropriate and secure manner. The Trust's Executive Medical Director will be the Trust's Caldicott Guardian.

4.3 Director of Corporate Affairs

The Director of Corporate Affairs is responsible for the overall development and maintenance of information governance throughout the Trust, in particular for promoting compliance with this Policy in such a way as to ensure the correct use of personal and corporate information and to lead on information risk with the Trust. The Director of Corporate Affairs is the Trust's Senior Information Risk Owner.

4.4 Senior Manager Information Governance

The Senior Manager Information Governance is responsible for promoting a culture of good information governance within the Trust and developing and maintaining policies, procedures and protocols in compliance with this policy and strategy and in accordance with good practice.

4.5 Information Asset Owners

Information Asset owners are responsible for:

- Providing assurance that information risk is managed effectively in relation to information assets that they are responsible for
- Identifying and documenting all information assets they own
- Taking ownership of their local asset control, risk assessment and management processes for the information assets they own
- Providing support to the Senior Information Risk Owner to maintain awareness of risks to information assets
- Ensuring that staff are aware of and comply with information governance and record management standards for the effective use of information assets

4.6 Information Asset Administrators

Information Asset Administrators are the operational staff responsible for the day to day control and use of one or more information assets, in particular they:

- Ensure that policies and procedures are followed;
- Recognise actual or potential security incidents;
- Consult their Information Asset Owners on incident management; and
- Ensure that Information Asset Registers are accurate and up to date

4.7 All staff

It is the responsibility of all staff to adhere to the principles set out in this document and any related policy/ procedure to help maintain the availability, effectiveness, security and confidentiality of information.

5. Implementation and Monitoring

5.1 All staff will receive information governance training as part of their induction and at regular intervals in accordance with the mandatory Training Policy. The training will include an assessment of their understanding.

5.2 Training compliance will be monitored by the Senior Manager Information Governance and reported to the Information Governance Group.

5.3 The Trust shall carry out an annual assessment against the Information Governance Toolkit. The process underpinning this assessment and the outcome will be overseen by IGG and reported to the Audit Committee.

5.4 Specific monitoring and audit requirements are set out in the associated policies.

6. References

The Trust's Information Governance arrangements take into account statutory arrangements and good practice, including:

- Data Protection Act 1998;
- Department of Health: Confidentiality Code of Practice 2003;
- International Information Security Standard ISO/IEC 27002:2007 (formerly(17799:2005);
- Department of Health: Information Security Code of Practice;
- Department of Health Records Management Code of Practice
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004
- Caldicott Principles (from the Caldicott Committee Report on the Review
- The NHS Care Records Service (NHS CRS)
- Access to Health Records Act 1990
- Common Law duty of confidentiality
- Connecting for Health Information Governance Toolkit Requirements

7. Associated Policy and Procedural Documentation

- Record Management and Information Lifecycle Management Policy
- Health Records Procedure
- Corporate Records Procedure
- Data Quality Policy
- Record Registration Guidelines
- Information Security Policy
- Email Policy
- Access Control Policy
- Access to Health Procedure
- Freedom of Information Policy
- IT Disaster Recovery Plan
- Emergency Preparedness and Business Continuity Policy
- IT Disaster Recovery Plan
- Freedom of Information Policy
- Data Protection Policy
- Information Asset Procedure
- Guidance for Classification Marking of NHS Information
- Record Registration Guidelines
- Policy for the Prevention and Management of Incidents Including Serious Incidents