Royal Surrey County Hospital NHS
NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

Name of Policy Author:	Ruth Drewett
Name of Review/Development Body:	Information Governance Steering Group Committee
Ratification Body:	Trust Board
Date of Ratification:	April 2015
Review date:	February 2018
Reviewing Body:	Information Governance Steering Group Committee

Signed ……..
Chief Executive

Date	Review Type (please tick		Version No.	Author of Review	Title of Author	Date Ratified	Ratification Body	Page Numbers (where amended)	Line Numbers (where amended)	Details of change	
	Minor amendment	[1]Full Review								Inserted	Deleted
May 2010		✓	1	Ruth Drewett	Information Governance Manager	May 2010	Board	N/A	N/A	N/A	N/A
March 2015	✓		1.1	Ruth Drewett	Information Governance Manager	April 2015	IGSGC	N/A	N/A	N/A	N/A

[1] Where there is a full review, amendment details are not required in the version control sheet.

VERSION CONTROL SHEET

CONTENTS

1. INTRODUCTION

This policy will outline the Trust's approach to Information Governance which seeks to ensure that information held by the Trust is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care to patients. Implementation of this policy will ensure all staff comply with the law and best practice when handling personal confidential and corporate information.

2. PURPOSE

2.1 The Information Governance framework will enable the Trust to meet its legislative requirements, and ensure operational and management information is timely, robust and reliable.

2.2 The key benefits of Information Governance are to:

- Protect patients and staff information.
- Meet legislative requirements.
- Ensure comprehensive, timely and accurate information at all levels.
- Support new initiatives.
- Comply with Trust risk management procedures.
- Provide a good level of training, awareness and support to staff and patients.

2.3 In line with Department of Health (DH) Policy and to ensure the Trust is providing a consistent approach in delivering the Information Governance framework, the Trust is required to complete the annual submission of the Information Governance Toolkit (IGT). The Health and Social Care Information Centre (HSCIS) has been commissioned by DH to develop and maintain the IGT.

3. SCOPE

3.1 This policy covers all aspects of information with the organisation, including (but not limited to):

- Patient, client, service user information
- Personnel information
- Organisational information – including clinical, research, and corporate.

3.2 Information Governance covers the use and management of information in all formats, including the collecting, processing, storage, communication and disposal of information. For example (but not limited to):

- Structured record systems – paper and electronic
- Transmission of information – fax, e-mail, post, telephone and text
- Information systems purchased, developed and managed by/or on behalf of, the Trust.

3.3 This policy applies to all staff working in the Trust, including staff on assignment, placement, secondment, honorary or temporary contract arrangements. Failure to follow the requirements outlined in this policy may result in investigation and management action being taken. This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and action against other workers, which may result in the termination of an assignment, placement, secondment, honorary or temporary contract arrangement.

4. DUITIES AND RESPONSIBILITIES

4.1 Managers with the Trust are responsible for ensuring that the policy and its supporting guidance is built into local processes and that there is continuing compliance with Information Governance.

4.2 The management of Information Governance within the Trust will be as follows:

The Information Governance Steering Group Committee (IGSGC) reports to the Executive Leadership Team (ELT). The Committee will operate within the framework set out in the terms of reference for the Committee in line with powers delegated to it by the Board as required to discharge the Trust's responsibilities.

The Information Governance Steering Group Committee is made up of representatives from the Trust to cover all elements of Information Governance. The Committee will ensure a sound framework exists for handling information in a confidential and secure manner to appropriate legal, ethical and quality standards.

The Committee takes responsibility for the completion of the Information Governance Toolkit, developing annual improvement plans, monitoring compliance. The IG Toolkit sets out six assurances as follows:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

Information Governance is led by the Senior Information Risk Officer (SIRO) supported by the Trust's Information Governance Manager, and is responsible for the Information Governance Steering Group Committee - Refer to Appendix 1 for the IGSGC Terms of Reference including the representatives.

Chair: Director of Finance – (SIRO)
Deputy Chair: Director of Nursing and Patient Experience – (Caldicott Guardian)
IG Lead: Information Governance Manager

5. SUBJECT MATTER

5.1 There are clear NHS standards within Information Governance and these are known as the HORUS model. That is to say all information should be:

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

How the Trust currently complies with these standards is detailed in various existing policies covering the issues highlighted with the HORUS model and the separate components that make up Information Governance.

5.2 The following documents should be read in conjunction with this policy as they support Information Governance:

5.2.1 Data Protection Policy – this provides guidance on how the Trust complies with issues of compliance with the Data Protection Act 1998 and its principles.

5.2.2 Code of Practice on Confidentiality Guidance – based on the "Confidentiality: NHS Code of Practice 2003", this guidance sets out how staff should maintain confidentiality of patient and Trust information. It also provides guidance on how information should be shared appropriately particularly that of a personal confidential and sensitive nature concerning patients, staff or others. With respect to such information, it is essential that the appropriate Information Sharing Protocols/Agreements are referred to and implemented

5.2.3 Freedom of Information Policy – this details how the Trust ensures that the Freedom of Information Act 2000, which came into force on 1 January 2005, is used appropriately and that relevant non-exempt and/or non-personal information is made available as required by this Act.

5.2.4 Data Quality Policy – this document details how the Trust will ensure that data is recorded accurately and is kept up to date and details other matters relating to data quality and data accreditation standards.

5.2.5 Records Management Policy – details how records should be structured, maintained, stored – life cycle management of the Trust's records.

5.2.6 Health Records Management Policy – this policy specifically details procedures around health records, including access to health records known as a Subject Access Request and references the Code of Records Management Code (Part 2) which details how long information held by the Trust should be retained. This details personal records for patients, staff and others and also covers corporate records.

5.2.7 IT Security Polices - All of these documents detail the specifics on how information systems/computer systems comply with standards of information security, such as password control, access control and risk assessment.

Network Security
Remote Access
Internet Usage and Security
Portable Computer Device
Email Use including Email Procedure

6. TRAINING

Information Governance will develop and implement a Trust wide training programme for all Trust staff to ensure awareness and compliance by all staff for all Information Governance requirements.

The Trust intranet will provide staff with detailed information and advice on all aspects of Information Governance.

All new starters to the Trust will be given Information Governance training as part of the corporate induction process.

IT Security training will take place at registration for new users, with follow-up and extra training modules for those who will be using Patient Administration Systems (OASIS, CRIS) or systems in relation to their job role, for example, Winpath.

6.1 **Contracts of Employment**
Staff contracts of employment are produced and monitored by the Human Resources department. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff and volunteers are subject to the same rules.

All employees at the Trust will be made aware of their responsibilities in connection with the Acts mentioned in this Policy through the Statement of Terms and Conditions, and targeted training sessions carried out by Managers and / or other trainers / specialists.

7. IMPLEMENTATION

Implementation has taken place but a refresh of roll out of all reviewed IG policies and guidance will take place in May 2015.

8. MONITORING COMPLIANCE, AND POLICY EFFECTIVENESS

Monitoring will be conducted by the IG Manager through the IG Spot Checks carried out across the Trust on a regular basis and reported to the Information Governance Steering Group Committee. Where non-compliance is found, a report will be sent direct to the senior manager of the area with recommendations for improvement and reported to the Caldicott Guardian.

9. REVIEW, APPROVAL / RATIFICATION AND ARCHIVING

This Policy will be reviewed every three years or more frequently if appropriate to take into account changes to legislation that may occur, and / or guidance from the Department of Health, the NHS Executive and / or the Information Commissioner.

The author or local policy officer is responsible for ensuring the archive of copies of the superseded working documents are retained in accordance with the Trust's Records Management Retention Schedule.

10. DISSEMINATION AND PUBLICATION

Dissemination of the final policy is the responsibility of the author who must ensure the policy is uploaded to the Trust's Central Library, the intranet.

Associate Directors, Business Unit, or supporting services management teams, Ward Managers and Heads of Department are responsible for distributing this policy and ensuring that all staff under their management (including bank, agency, contracted, locum and volunteers) are made aware of the policy.

11. EQUALITY IMPACT ASSESSMENT

The author of this policy has undertaken an Equality Analysis Initial Screening. No adverse impacts were identified. The Equality Analysis Initial Screening has been archived and is available via the Central Policy Officer.

Appendix 1

Royal Surrey County Hospital NHS
NHS Foundation Trust

Information Governance Steering Group Committee
Terms of Reference

1. **Constitution**

The Information Governance Steering Committee reports to the Executive Leadership Team (ELT). The Committee will operate within the framework set out in the terms of reference for the Committee in line with powers delegated to it by the Board as required to discharge the Trust's responsibilities.

2. **Membership**

Chair: Director of Finance – (SIRO)
Deputy Chair: Director of Nursing and Patient Experience – (Caldicott Guardian)
Information Governance Manager
Deputy Medical Director
Associate Director of HR
Company Secretary
Head of Information Services
Healthcare Records Manager
Speciality Manager for Outpatients
Informatics/IT Representative
Head of Clinical Risk
Head of Non-Clinical Risk
Head of Communications
Patients 1st Clinical Lead

Optional
Legal Services Manager
Estates (Soft Facilities Management)

The decisions of the Committee shall not be upheld without ratification unless quorate. Quoracy will be achieved when a minimum of four members in addition to the Caldicott Guardian or the Chair are present.

3. **Frequency**

Meetings shall normally be held every two months and not less than six times a year. The planned duration will be 1.5 - 2 hours. The IG Forum Working Groups will be expected to report improvements to the Committee on a regular basis determined by their plans.

4. **Quorum**

Meetings shall be considered quorate if the Caldicott Guardian and/or SIRO and four members are present.

5. **Terms of Authority**

The Chief Executive has overall responsibility for information governance, including responsibility for ensuring the implementation of Caldicott requirements, controls assurance and risk management.

The Caldicott Guardian for the Trust has overall responsibility for compliance with Caldicott and Data Protection.

The SIRO for the Trust has overall responsibility for the Trust's information risk.

The Chair of the Committee is delegated with responsibility for ensuring the implementation of policies and procedures within the Trust that adhere to Caldicott principles and fulfil the requirements of the Data Protection Act.

The Information Governance Steering Group Committee is established to provide a lead for Information Governance strategic direction and to take forward operational/practical issues.

6. Overview and Scope

Information Governance currently encompasses the following initiatives or work areas:

.

- Data Protection Act 1998
- Freedom of Information Act 2000
- Information Sharing
- The Confidentiality Code of Practice
- Information Security Management
- Records Management
- Information Quality Assurance & Data Quality
- Information Security

The Committee is responsible for ensuring that the Trust meets all legal and other requirements in these areas, and for developing a strategy of implementation, updating policies as appropriate and ensuring that a comprehensive programme of training in these areas is available to staff.

7. Objectives

The Committee shall:

- Support the provision of high quality care by promoting the effective and appropriate use of information.
- Develop, support and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- Oversee the use of the Information Governance Toolkit and to finalise the Hospital's annual electronic submission before sending to the Trust Board for sign off.
- Agree and develop an IG work programme that includes improvement planning.
- Develop and review the Information Governance policy and strategy on an annual basis, or in response to new legislation or national guidance as required.
- Monitor the issues relating to Information Governance identified through incident reporting and recommend actions.
- Ensure that the relevant requirements of the NHSLA risk management programme and the requirements of Standards for Better Health are fulfilled.
- Review the Royal Surrey County Hospital's Publication Scheme annually and monitor applications under the Freedom of Information Act.
- Review the Royal Surrey County Hospital's annual notification under the Data Protection Act 1998 to ensure it fully covers all Trust use of information and to review procedures for meeting subject access requests.
- Ensure initiatives relevant to Information Governance are co-ordinated and communicated to staff across the hospital.
- Identify training and development requirements in priority areas and support effective implementation of recommendations.
- Liaise with other Trust committees undertaking work in this area to ensure all Information Governance requirements are met.
- Ensure appropriate monitoring of actions, implementation of policy and assure the Board that effective processes are place for Information Governance.

- Consider any breaches of IT Security or Confidentiality and learn from these.
- Act in an advisory capacity to clinicians and management to ensure appropriate review of new processes or systems which will involve a new use or significantly change the way in which personal data is handled.
- Review and approve the development of IG related policies including, but not limited to, Records Management, Data Quality and use of NHS Number, IM&T security.
- To ensure that the Trust undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.

8. **Accountability**

The minutes of the Information Governance Steering Group Committee meetings shall be formally recorded and submitted to Executive Leadership Team.

The Committee shall report on:

- Annual Management audits and improvement plans
- Information Governance Toolkit submissions and any other Information Assurance submissions made to an external body, such as NHS England, Health & Social Care Information.

9. **Review of Effectiveness**

On a quarterly basis the Committee shall monitor its effectiveness as follows:

- Ensuring its objectives, accountability and reporting arrangements are effective and meet the Committee's requirements
- The programming and implementation of any action plans
- Membership and attendance record
- Reporting arrangements for any Sub-Committees
- Quorum requirements

Agreed by the Board: ……..

Date: …….