INFORMATION GOVERNANCE POLICY AND PROCEDURE

Summary

Information Governance stipulates the way in which the NHS should handle information, particularly personal and/or sensitive information such as patient and staff data. It also enables the Trust to ensure that all confidential information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care to our patients.

A range of components fall under Information Governance as it combines both Clinical Governance and Corporate Governance.

Key areas of Information Governance:
- Records Management
- Information Risk
- Information Security
- Freedom of Information Act 2000
- Data Protection Act 1998
- NHS Codes of Practice

The aim of this policy is to outline the best practice arrangements required to successfully implement and maintain Information Governance standards.

CONTENTS

1.   INTRODUCTION

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services, resources and performance management. It is therefore of paramount importance that the appropriate policies, procedures and management accountability provide a robust governance framework for information management.

The Trust Information Governance Policy has been developed as a result of the work carried out in relation to Controls Assurance Standards, Data Quality, Data Accreditation Programme, Caldicott Review, Data Protection Act 1998, Information Security and Records Management. It also includes initiatives such as the NHS Confidentiality Code of Practice and Freedom of Information Act 2000. It has also been created in line with the

Authoring Department:	Information	Version Number:	11
Author Title:	Information Governance Manager	Published Date:	05/01/2015 15:19:12
Ratified By:	IG Committee; IGRM	Review Date:	05/01/2016 15:19:12
Uncontrolled if printed			

Information Governance Toolkit (IGT), an annual assessment tool that was established by NHS Connecting for Health).

2.   PRINCIPLES OF INFORMATION GOVERNANCE

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

Equally important is the need to ensure high standards of data protection and confidentiality to safeguard personal and commercially sensitive information.

Underpinning this is the integrity need for electronic and paper information to be accurate, relevant, and available to those who need it.

Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with the relevant legislation and NHS guidance. It is the responsibility of all staff to familiarise themselves with this policy and adhere to its principles.

Further information can be obtained from: www.connectingforhealth.nhs.uk/infogov

3.   MAIN THEMES

There are four key interlinked strands to the Information Governance Policy:

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

Openness

Non-confidential information on the Trust and its services will be made available to the public through a variety of media, in line with the Trust's code of openness.

The Trust will establish and maintain 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 will be able to exercise their right to access information relating to their own health care, their options for treatment and their rights as patients.

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

Authoring Department:	Information	Version Number:	11
Author Title:	Information Governance Manager	Published Date:	05/01/2015 15:19:12
Ratified By:	IG Committee; IGRM	Review Date:	05/01/2016 15:19:12
Uncontrolled if printed			

Page 2 of 5

The Trust will have clear procedures and arrangements for handling queries from patients and the public.

Legal Compliance

The Trust regards all identifiable personal 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 identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and common law confidentiality.

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).

Information Security

The Trust will establish and maintain 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 security arrangements.

The Trust will promote effective confidentiality and security practice to its staff through policies and training.

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.

Information Quality Assurance

The Trust will establish and maintain 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 to the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

The Trust will promote information quality and effective records management through policies, procedures/user manuals and training.

Authoring Department:	Information	Version Number:	11
Author Title:	Information Governance Manager	Published Date:	05/01/2015 15:19:12
Ratified By:	IG Committee; IGRM	Review Date:	05/01/2016 15:19:12
Uncontrolled if printed			

Page 3 of 5

4.   IMPLEMENTATION

The Board level lead for Information Governance is the Chief Nurse. Reports will be submitted for consideration by the Board within the Integrated Governance and Risk Management Committee. The Trust will ensure that the strategy is implemented via the main Information Governance Policy and related policies. All policies, work programmes and action plans will be approved and monitored by the Information Governance Committee and reports will be submitted on a bi-monthly basis. The Information Governance Manager has senior level operational responsibility for this agenda, supporting the Caldicott Guardian in relation to Clinical Governance.

The Trust's Information Governance Committee has responsibility for the formulation of Information Governance policies. This group has senior level representation from all appropriate areas to ensure the Trust steers this agenda in line with current legislation.

The Information Governance Committee will receive reports from designated managers who have responsibility for dealing with all information governance requirements and will approve central returns required by the Information Governance Toolkit to the Health and Social Care Information.

The Information Governance Toolkit (IGT) will be used by the Trust to conduct baseline audit and construct action plans to ensure future compliance with this agenda. The work programmes in the individual areas will be created by adherence to the IGT standards and to the national standards appropriate to the individual field of activity.

The implementation of policies in this area will be carried out across the Trust by all involved staff and will be led by the Caldicott Guardian and supporting teams.

Training and awareness raising sessions appropriate to staff groups will be provided. This will involve the widening of existing training programmes to include new policies and initiatives, e.g. Freedom of Information. Training needs assessments will be carried out for the individual staff groups.

5.   RISK

The Trust must ensure that it operates within a robust Information Governance framework to reduce the risk of threats such as potential litigation, breach of Data Protection Act and any compromise to patient care. Risk assessments will be carried out in the individual component areas as required by the Information Governance Toolkit. Risk assessments will be undertaken as per the Risk Management Policy with additional Information Governance risk assessments performed if required. Department risk registers will be integrated alongside corporate risk registers.

6.   INFORMATION GOVERNANCE MANAGER

The Trust has appointed an Information Governance Manager who will assist in managing the Information Governance agenda. This post is line managed by the Head of Quality Assurance, who has senior level operational responsibility for the agenda and support of the Caldicott Guardian.

Authoring Department:	Information	Version Number:	11
Author Title:	Information Governance Manager	Published Date:	05/01/2015 15:19:12
Ratified By:	IG Committee; IGRM	Review Date:	05/01/2016 15:19:12
Uncontrolled if printed			

Page 4 of 5

7.   CALDICOTT GUARDIAN

The Chief Nurse is the appointed Caldicott Guardian for the Trust and has, on behalf of the Board, responsibility to act as the Guardian of patient-identifiable information.

8.   SENIOR INFORMATION RISK OFFICER (SIRO)

Each NHS Trust is now required to incorporate the new role of Senior Information Risk Officer (SIRO) into their Information Governance arrangements. It is the responsibility of the SIRO to take forward the Trust's information risk agenda and act as advocate for information risk at board level. The SIRO at The Royal Marsden is the Chief Operating Officer.

9.   REVIEW

This policy is updated annually by the Chief Nurse/Caldicott Guardian in the light of any new Guidance received.

10.   LINKED DOCUMENTS

Risk Management Policy (257)

Freedom of Information Policy and Procedures (443)

Confidentiality and the Data Protection Act Policy (277)

Consent to Examination or Treatment Policy (325)

Management of Medical Records - Policy & Procedures (459)

Computerised Case Notes Policy and Procedures for (453)

Information for Patients - Provision and Production Policy (340)

Records Management Strategy (407)

Email Usage Policy (176)

Concerns and Complaints Policy and Procedures (160)

Information Governance Assurance Management Framework (1743)

[End of Document - Do Not Delete]