Mid Essex Hospital Services NHS Trust

Information Governance Strategy	**Type** **Corporate/Strategic** **Register Number** **07012** **Status** **Public**

Developed in response to:	Information Governance Toolkit Best practice guidance
Contributes to CQC Outcome	20

Consulted With	**Post/Committee/Group**	**Date**
Kate Thompson	Head of IT	Sept 2015
Barry Stannard	IT Operations Manager	Sept 2015
Richard Chapman	Deputy Director of Business Performance & Planning	Sept 2015
All members	Information Governance Group	March 2016
Professionally Approved by	Martin Callingham Chief Information Officer / SIRO	March 2016

Version Number	3.0
Issuing Directorate	Informatics
Ratified by:	DRAG Chairmans Action
Ratified on:	21st March 2016
Trust Executive Sign Off Date	April 2016
Implementation Date	22nd March 2016
Next Review Date	February 2019
Author/Contact for Information	Bhavesh Khetia
Policy to be followed by (target staff)	All staff, contractors and affiliates
Distribution Method	Intranet, Website
Related Trust Policies (to be read in conjunction with)	All Information Governance Policies All IT Security Policies Risk Management Strategy

Document Review History

Review No	**Reviewed by**	**Review Date**
1.0	D Shrimpton	November 2012
2.0	D Shrimpton	March 2013
3.0	Bhavesh Khetia	March 2016

Index

1.0 Purpose

1.1 It is the purpose of this policy to demonstrate:

- The importance of information governance to the Trust
- The importance of setting information governance standards so that patients can be assured of the Trust's commitment to protect their information, record it accurately and to share it appropriately
- A commitment to comply with, or work towards, achieving all national and local information governance standards
- That the Trust will, through its information governance work plans be seeking to demonstrate year on year improvement

2.0 Policy Statement

2.1 The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information governance plays a key part in supporting clinical governance, service planning and performance management.

2.2 Information governance also gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible patient care.

2.3 The Trust will establish, review, adapt and maintain policies and procedures to ensure compliance with requirements contained in the Health and Social Care Information Centre's (HSCIC) Information Governance Toolkit (IGT).

2.4 The Trust has a comprehensive range of policies supporting the information governance agenda, as set out in Appendix 1.

3.0 Scope

3.1 This document reflects all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel information
- Organisational information

3.2 This document reflects 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 All information systems purchased, developed and managed by, or on behalf of, the organisation and any individual directly employed or otherwise by the organisation.

4.0 Principles

4.1 Openness

- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information
- Information will be defined and where appropriate kept confidential, underpinning the Caldicott Principles and the regulations outlined in the Data Protection Act 1998
- Non-confidential information about the Trust and its services will be available to the public through a variety of means, in line with the Trust's code of openness. The Trust will comply with the Freedom of Information Act 2000
- Patients will have controlled access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience
- The Trust regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory framework will be achieved, monitored and maintained
- 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 and procedures to ensure compliance with the Data Protection Act 1998, the Human Rights Act 1998, the Common Law Duty of Confidentiality and the Freedom of Information Act 2000
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness in line with the requirements of the IGT will provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity, will be undertaken to determine appropriate, effective and affordable information governance controls are in place

4.2 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- Audits will be undertaken or commissioned to assess information and IT security arrangements
- The Trust's Incident Reporting system will be used to report, monitor and investigate all breaches of confidentiality and information security

4.3 Information Quality Assurance

- The Trust will establish and maintain policies for information quality assurance and the effective management of records

- Audits will be undertaken or commissioned of the Trust’s quality of data and records management arrangements
- Divisional/General Managers will be expected to take ownership of, and seek to improve, the quality of data within their services
- Wherever possible, information quality will be assured at the point of collection
- The Trust will promote data quality through policies, procedures/user manual and training

5. Responsibilities

5.1 The Chief Executive, as Accountable Officer, has overall accountability and responsibility for Information Governance within the Trust. They are required to provide assurance, through the Statement of Internal Control, that all risks to the Trust, including those relating to information governance, are effectively managed and mitigated.

5.2 The Information Governance Group is responsible for overseeing Information Governance issues; ensuring that policies are developed, with standards set and communicated. The Group authorises the IGT returns and agrees the Information Governance work plans.

5.3 The Senior Information Risk Officer (SIRO) is expected to understand how the strategic business goals of the Trust may be impacted by information risks. The SIRO will act as an advocate for information risk on the Trust Board of Directors and in internal discussions, and will provide written advice to the Accounting Officer on the content of their Annual Governance Statement (AGS) with regards to information risk.

5.4 The SIRO will be supported by the Caldicott Guardian, the Chief Information Officer (who may also be the SIRO), the Information Governance Manager and the Trust’s lead for risk management.

5.5 The Information Governance Manager is responsible for overseeing day-to-day information governance issues, developing and maintaining policies, standards, procedures and guidance, and overseeing the Trust’s submission for the IGT annual assessment.

5.6 Relevant Operational Management are responsible for ensuring that the strategy and its supporting policies are built into local processes and that there is on-going compliance.

5.7 Departmental managers and the Human Resources Department are responsible for ensuring that regular Information Governance training and updates are provided for all staff.

5.8 All staff, whether permanent, temporary, contracted or volunteers are responsible for ensuring that they are aware of the requirements incumbent upon them, and for ensuring that they comply with these on a day to day basis.

5.9 The procurement department is responsible for ensuring that an information governance requirement is built into Trust contracts for purchasing goods and services.

6.0 Year on Year Improvement Plan and Assessment

6.1 An assessment of compliance with requirements, within the IGT, will be undertaken each year. Annual reports and proposed Action/development plans will be presented to the Trust's Information Governance Group for approval prior to submission to the IGT. The requirements are grouped into the following initiatives:

- Information Governance Management
- Confidentiality & Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance (includes Freedom of Information)

7.0 Information Governance Management

7.1 Information governance management across the organisation will be co-ordinated by the Information Governance Group. The membership of this group will comprise:

- The Senior Information Risk Owner (SIRO)
- Chief Information Officer (CIO)
- The Caldicott Guardian
- The Information Governance Manager (IGM)
- The IT Security Manager
- The Registration Authority Manager (Covers HR)
- The Health Records Manager
- The Head of Clinical Coding & Data Quality
- Head of Governance (or Representative)

7.2 The Information Governance Group is the decision making body for all issues relating to information governance. This is supported by two sub groups:

- Data Quality Group
- Medical Records Group

7.3 It will also act as the reporting body for the following sub groups on an “as required” basis:

- Registration Authority Sub-Group
- Document Ratification Group (DRAG)

7.4 The Terms of Reference of the Information Governance Group and the Sub-Groups will be published separately.

7.5 The Information Governance Group will report to the Informatics Steering Group who in turn report to the Patient Safety and Quality Committee.

8.0 Training

8.1 All staff should attend, as part of their induction, a training session on Information Governance. Top–up training will be provided; this can be requested by an individual wanting personal development or arranged at the discretion of a manager.

8.2 A rolling programme of annual Information Governance e-learning has been introduced for all staff.

8.3 All staff attending their mandatory update training will have an Information Governance session included and this will either be a face to face classroom sessions or taken as e-learning as per 8.2.

9.0 Communication

9.1 This document will be published on the Trust's intranet, internet and notified to staff via available communication channels.

9.2 The author will notify all heads of services who will be responsible for ensuring that the document is cascaded throughout their work areas.

9.3 Heads of services may be audited to ensure compliance with 9.2.

10. Audit & Monitoring

10.1 The results of the IGT returns will be considered the results of this Strategy.

11.0 References

Data Protection Act 1998
Freedom of Information Act 2000
Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
Computer Misuse Act 1990
Copyright, designs and patents Act 1988 (as amended by the Copyright Computer programs regulations 1992)
Human Rights Act 1998
Crime and Disorder Act 1998
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000

Appendix 1

List of Trust Policies relevant to Information Governance

Register No	Name	What's it about?
07012	Information Governance Strategy	This is the overarching policy under which all other policies refer. This document will tell you the direction of the trust but not give specific task guidance
09045	Information Security Management Strategy	This is the overarching policy under which all IT security and IT specific policies refer. This document will tell you the direction of the trust but not give specific task guidance
04084	Records Management Strategy	This is the overarching policy under which all records related policies and procedures refer. This document will tell you the direction of the trust but not give specific task guidance
07011	Confidentiality & Data Protection Policy	This is the key document that relates to all aspects of confidentiality and how the Trust will met its obligations under the Data Protection Act
07026	Sharing Patient Information	Key document that sets out the rules for sharing patient information outside the Trust and a Data Sharing Agreement (Appendix 1)
08088	Acceptable Use of IT	This is the key document that relates to safe computer usage
08075	Workstation Security	How to work safely at your computer
09036	Password Policy	Management of passwords
07042	Email Policy	Staff responsibilities about the use of email
08064	Encryption Policy	All mobile media must be encrypted including laptops, memory sticks. Trust information can only leave the trust on media that is encrypted
09021	Remote Working	Rules for secure working with IT for staff who are either mobile or working outside of the trust e.g. at home
10055	Sending Patient Identifiable information out of the UK	This policy relates specifically to the Data Protection Act and its Principles and the policy sets out the rules for managing this in the trust
08042	Document Provenance Policy	This sets out the rules and standards for all trust policies, clinical and non-clinical
08022	Information Lifecycle Policy	The Trust's first policy relating to trust records management
10123	Information Asset Policy	Sets out the responsibilities of Information Asset Owners and Information Asset Administrators to the SIRO for the correct recording of information assets onto the trust database

04085	Archiving Policy	Relates mainly to the archiving of Medical Records – staff must also need to know about the Retention & Disposal schedule that sets out the rules for how long trust documents needs to be retained
04086	Access to Records Policy	The rules and procedures for meeting DPA Subject Access Requests and requests from other agencies including the Police for duplicate health records
07015	Coding Policy	The management of medical coding
08086	Clinical Record Keeping	The required procedures for clinical record keeping
05103	Case Note Tracking Policy	The rules concerning the tracking of medical records and specifically how each movement of each record must be recorded on PAS
06019	Data Quality Policy	The trust policy for achieving data quality relating to patient activity
09031	Registration Authority	The rules around smartcards
07014	Freedom of Information	Reflects the FOI Act and includes the trust process for the appropriate management of the Freedom of Information requests it receives