Mid Essex Hospital Services NHS
NHS Trust

Information Lifecycle Management Policy	**Type: Policy** **Register No: 08022** **Status: Public**

Developed in response to:	IG toolkit 107
Contributes to CQC Core Standard number:	C7a & C9

Consulted With	**Post/Committee/Group**	**Date**
Paul Scott	Deputy SIRO	February 2010
Dr David Blainey	Caldicott Guardian & Director of Patient Safety	February 2010
Thomas Lafferty	Associate Director: Governance & Legal	February 2010
Sharon Salthouse	General Manager, Patients Records Service	February 2010
Dave Shrimpton	IT Security Manager	February 2010
Professionally Approved By	Philippa Lowe, Deputy Chief Exec & Senior Information Risk Owner (SIRO)	February 2010

Version Number	1.0
Issuing Directorate	Corporate Services/Governance
Ratified by:	Document Ratification Group
Ratified on:	25th February 2010
Trust Executive sign off	March CMB
Implementation Date	1st March 2010
Next Review Date	January 2013
Author/Contact for Information	Liz Stewart
Policy to be followed by (target staff)	All staff
Distribution Method	Intranet, website & Staff Focus
Related Trust Policies (to be read in conjunction with)	Information Asset Management Project/Process Email Policy Retention & Destruction Schedule Document Provenance Policy Clinical Record Keeping Policy Data Quality Policy Incidents Policy

Document Review History

Review No	Reviewed by	Review Date

It is the personal responsibility of the individual referring to this document to ensure that they are viewing the latest version which will always be the document on the intranet

Index

1. Purpose of Policy

1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.

1.2 This document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

1.3 This policy meets the Trust's obligations to the Information Governance Toolkit Criteria 107.

1.4 This policy supports the Trust's obligations for Information Asset Ownership required under the Information Governance Toolkit Criteria 121

1.5 This policy reflects the NHS Records Management Code of Practice which has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

Equality & Diversity

1.6 Mid Essex Hospital Services NHS Trust is committed to the provision of a service that is fair, accessible and meets the needs of all individuals.

2. Trust Records Policy

2.1 The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations.

2.2 Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

2.3 Information (records) management, through proper control of the content, storage and volume of records, reduces vulnerability to legal challenge and promotes best value in terms of human and space resources through greater coordination of information and storage systems.

2.4 All records created in the course of the business of Mid Essex Hospital Services NHS Trust are corporate records and are public records under the terms of the Public Records Act 1958 and 1967. This includes email messages and other electronic records. Public Records must be kept in accordance with the following statutory and NHS guidelines:

- Public Records Acts 1958 and 1967
- Data Protection Act 1998
- Lord Chancellors Code of Practice under Section 46 of the Freedom of Information Act 2000
- Information Governance Toolkit
- Records Management: NHS Code of Practice
- Caldicott Review of Patient Identifiable Information, 1997
- NHSLA Risk Management Standards
- Freedom of Information Act 2000
- and any new legislation affecting records management as it arises

2.5 The Trust believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

2.6 All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: Code of Practice, in particular:

- The Public Records Act 1958
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice 2003
- And any new legislation affecting records management as it arises.

3. Scope

3.1 This policy relates to all clinical and non-clinical operational records held in any format by any member of Trust Staff. These include:

- Corporate Records – Committee papers, Trust Policies and Clinical Guidelines corporate strategies and records relating to land and buildings
- H R Records – personal files, training records, disciplinary files
- Financial & Accounting records
- Health Activity Records
- Complaint & Litigation Files
- All Health Records manual or electronic
- Emails
- Databases and registers, manual or electronic
- Back-up and archive data
- Audit data
- Electronic system information and documentation
- Operations and support procedures
- Contracts and agreements
- Business continuity plans

4. Definitions

4.1 **Records Management** is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of records management are:

- record creation
- record keeping
- record maintenance (including tracking of record management)
- access and disclosure
- closure and transfer
- appraisal
- archiving
- disposal.

4.2 **Records Lifecycle** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

4.3 **Recorded Information -** In this policy, **Records** are defined as "recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity".

4.4 **Information** is a corporate asset. The Trust's records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of the Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

5. Aims of Records Management

The aims of our Records Management System are to ensure that:

- **records are available when needed** – from which the Trust is able to form a reconstruction of activities or events that have taken place

- **records can be accessed** – records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist

- **records can be interpreted** – the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records

- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, and its integrity and authenticity can be demonstrated

- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format

- **records are secure** – from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required

- **records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and

- **staff are trained** – so that all staff are made aware of their responsibilities for record-keeping and record management.

6. Roles and Responsibilities

6.1 The Trust as a Corporate Body

6.1.1 The Trust recognises that it has a specific corporate responsibility for records management. All contracts of employment must contain record keeping standards as laid out in this policy and in guidelines produced by regulatory bodies.

6.1.2 The Trust must have robust systems and processes that ensure that records are fit for purpose, are stored securely, are readily available when needed and are destroyed in compliance with the retention and destruction schedule at the end of the cycle of each particular record.

6.2 Chief Executive

The Chief Executive has overall responsibility for records management in the Trust. As accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required. However the responsibility is delegated to the Senior Information Risk Owner (SIRO)

6.3 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

6.4 **Senior Information Risk Owner (SIRO)**

6.4.1 The SIRO is an Executive Board member who is responsible for identifying and managing the information risks to the organisation and for ensuring the availability of an Information Asset Register.

6.4.2 The SIRO will have oversight of the organisation's information security incident reporting and response arrangements. The SIRO will be supported in their role by one or more Information Asset Owners who have assigned responsibility for the information assets of the organisation.

6.4.3 In the event of an Serious Untoward Incident occurring that relates to patient information the SIRO will work in tandem with the Caldicott Guardian.

6.4 Information Asset Owners (IAO)

6.4.1 IAOs are senior managers in the Trust, normally a level down from Executive Director, or they can be heads of specific services.

6.4.2 IAOs must be aware of the information that is held and administered within the division or department for which they are responsible and will be held accountable for its security, currency, and appropriate disposal.

6.4.3 IAOs are directly responsible to the SIRO in the discharge of their responsibilities irrespective of their normal line management.

6.4.4 IAOs must ensure that they do not retain information any longer than they are required to do so and must be familiar with the time limits set out in the Retention & Destruction Schedule.

6.5 Information Asset Administrators (IAA)

6.5.1 IAAs will be individuals who have day to day control of information assets.

6.5.2 The main function is to complete Information Asset Registration forms for all items current and archived as per the list under 2.1 and make sure that all subsequent changes to the asset i.e. disposal, are recorded.

6.5.3 An IAA can also be an IAO.

6.5.4 Every shared drive or shared database must have an administrator.

6.5.5 There can only be one administrator for each asset irrespective of the numbers of users of the asset.

6.4 **General Manager – Patients Records Service**

6.4.1 The General Manager is responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up

guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

6.5 **The Corporate Governance Group**

6.5.1 The Corporate Governance Group (CGG) will be the overarching group for information management. The minutes of the CGG are submitted to the Trust Audit Committee.

6.5.2 The Medical Records Group is responsible to the CGG and for ensuring that all major information risk and information security issues are routinely reported to it.

6.7 **All Staff**

6.7.1 All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any guidance subsequently produced.

6.7.2 All records created must be set according to a clear indexing system, be dated and where appropriate version controlled.

7. Trust Records Database

7.1 The Trust will establish the Information Asset Register (IAR)

7.2 The IAR will be searchable to enable each IAO to produce a report showing all the information assets recorded by their IAAs. This report would always be the up to date register attributed to that particular IAO.

7.3 The Trust has as part of its Information Governance Agenda has set up Trust-wide Data Mapping accessible directly from the intranet. The purpose of data mapping is to record all sensitive information that is flowing in or out of the Trust. An information governance risk assessment will take place if any transfers that are not deemed as safe.

8. Retention and Disposal

8.1 It is a fundamental requirement that all Trust records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance of the Trust's business functions.

8.2 The Trust has adopted the retention periods set out in the Records Management: NHS Code of Practice Schedule D and the searchable database for staff reference is on the intranet.

9. Security of Sensitive Information

9.1 Any incident or near miss relating to a breach in the security regarding use, storage, transportation or handling of records must be reported using the Trust's incident reporting framework and the Incidents Policy..

9.2 All breaches of confidentiality or information security will be deemed as a Serious Untoward Incident and be reported to the Information Governance Group.

9.3 The Trust's Caldicott Guardian must be informed immediately of any loss or misplacement of any document that is used to record patient information, including diaries, laptops, datasticks or any Trust business. Any loss will be managed as a Serious Untoward Incident and investigated and reported in accordance with the Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents (DH Jan 2010)

9.4 Staff must seek permission from the Information Governance Manager before sending unsecured patient data out of the Trust if the transfer has not been risk assessed as part of the data mapping exercise.

9.5 All information assets must be securely and appropriately protected

9.6 Staff must ensure that:

- they do not retain patient identifiable information (PII) on C Drives or on unprotected portable media – refer to Encryption Policy
- Sensitive information is not sent either in the title, the body or as attachment out of the trust if it is not password protected, but preferably encrypted

10. Training

10.1 Staff need to have an understanding of:

- What they should record
- Why they are recording it and how it will be used
- How to validate the information with the patient or against other records – so staff are recording the correct data
- How to update information and add in information from other sources
- The correction of errors – so staff know how to correct errors and how to report errors if they find them

10.2 This training will take place either as part of local induction, close observation of others or at aformal training session. The latter particularly applies when it relates to the use of an electronic clinical system.

13.3 General Information Governance awareness will be provided to all staff at induction and at mandatory training days and in the future via on line e-learning.

13.4 Staff with medical records responsibilities will receive appropriate training and can refer to their Medical Records Procedures Manual.

11. Audit

11.1 The SIRO will include Information Asset risk information gained from the IAOs, other relevant staff and from the incident reporting framework, to the Statement of Internal Controls.

11.2 All incidences of inappropriate sharing of personal identifiable information will be reported to the Corporate Governance Group chaired by the SIRO.

12. References

Data Protection Act 1998
NHS Records Management Code of Practice (revised)
Information Governance Toolkit 107