



MAYDEN Health
Policies and Procedures

IG08

Lifecycle Management

Information Governance

August 2010

IG Policy Index	
IG01	Information Governance
IG02	Information Security
IG03	Personal Information Handling
IG04	Confidentiality Code of Practice
IG05	Data Quality Policy
IG06	Risk Management
IG07	Security Incident Policy
IG08	Lifecycle Management
IG09	Business Continuity Plan

Current Version

Responsibility of	Information Governance Lead
Reviewed by	
First Issued	November 2009
Last Review Date	August 2010
Next Review Date	August 2011

Version History

Version	Date	Comment	Initials	Signature
1.0	3/12/09	Initial version following wide comment	CM	
1.1	23/8/10	Update to reflect latest position and practices	CM	

Roles and Responsibilities

Information Governance Lead	Chris May
Information Security Lead	Chris Eldridge

CONTENTS

1	Policy Statement	1
2	Executive Summary.....	1
3	Introduction	1
4	Scope and definitions.....	2
5	Aims of our Records Management System.....	3
6	Roles and Responsibilities.....	4
6.1	Information Governance Lead	4
6.2	Information Governance Steering Group	4
7	Legal and Professional Obligations relating to NHS contracts.....	4
8	Safe Haven	5
9	Safe Haven Procedure.....	5
9.1	Facsimile.....	5
9.2	Letters	6
9.3	Telephone	6
9.4	Email.....	6
9.5	Electronic – via email using Microsoft protected attachment	6
9.6	Electronic – via secure upload to secure live patient site.....	7
10	Registration of Record Collections.....	7
11	Retention and Disposal Schedules	7
12	Records Management Systems Audit	7
13	Training	8
14	Review.....	8

1 Policy Statement

This Policy defines Mayden Health expectations for the management of all clinical and non-clinical records, whether internally or externally generated and in any format, from their creation to their eventual disposal. The policy and its underlying principles link closely to Mayden Health's Risk Management and Assessment policy. Both have been developed using the exemplar model on the Connecting for Health Website of the Information Governance Toolkit on :-

<https://www.igt.connectingforhealth.nhs.uk>

By adopting this policy, Mayden Health agrees to adhere to the principles and uphold the standards published by the Department of Health (DH) in its 'Records Management: NHS Code of Practice' on:-

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

2 Executive Summary

Mayden Health's records are its corporate memory, providing evidence of actions and decisions and represent a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisations 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.

This policy:

- Provides a clear and comprehensive guide on the management of all records within Mayden Health
- Includes detailed scope and definitions of these records to ensure compliance with 'Records Management: NHS Code of Practice' published by the Department of Health
- Enables staff to understand their operational and legal responsibilities for the management of all records to ensure a common approach across the organisation
- Provides clear guidance on ownership of the document, which includes responsibilities for appropriate peer review, Equity Impact Assessment and revision of the document
- Specifies the standards it complies with
- Describes how it will be distributed and shared throughout the organisation

3 Introduction

Lifecycle management of records is the process by which an organisation manages all aspects of records. It applies whether records are internally or externally generated in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.

The Records Management: NHS Code of Practice has been published by the Department of Health as a guide to the required standards 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. As Mayden Health works under contract to the NHS, Department of Health recommendations and guidelines are adhered to and represented throughout this policy.

Mayden Health's records are its corporate memory, providing evidence of actions and decisions and represent a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisation 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.

Conversely, Mayden recognises that it is sometimes inappropriate to keep certain records beyond their useful life and therefore a data retention policy is in place.

The Management Team has adopted this records management policy and is committed to the ongoing improvement of its records management functions as part of its governance agenda. It believes Mayden Health will gain a number of organisational benefits from so doing. These include:

- Better use of physical and server space;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards for Mayden Health and commissioning organisations;
- Reduced long-term costs.

The Management Team also believes its internal management processes will be improved by the greater and easier availability of information when records management is recognised as a designated corporate function.

This document sets out a framework within which staff responsible for managing Mayden Health'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.

It is the responsibility of all staff including those on temporary contracts, agency staff and students to comply with this policy.

Compliance with Mayden Health's policies is a condition of employment and breach of this policy may result in disciplinary action.

4 Scope and definitions

This policy relates to all clinical and non-clinical operational records held in any format by Mayden Health. These include:

- All administrative records (eg human resources, estates, financial and accounting records, notes associated with complaints).
- All patient health records.

Lifecycle 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. At the same time it serves the operational needs of the

organisation and preserves an appropriate historical record. The key components of records management are:

- Record creation
- Record keeping
- Record maintenance (including tracking of record movements)
- Access and disclosure
- Closure and transfer
- Appraisal
- Archiving
- Disposal

A record's 'Life Cycle' 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 in accordance with legal requirements.

Records in this policy are defined as 'recorder information, in any form, created or received and maintained by Mayden Health in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

Information is a corporate asset. Mayden Health's records are important sources of administrative, evidential and historical information. They are vital to the organisation to support its current and future operations, for the purpose of accountability, and for an awareness and understanding of its history and procedures.

5 Aims of our Records Management System

To ensure that:

- Records are available when needed – from which Mayden Health 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, the business process, 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 can be supplied in response to requests under the Freedom of Information Act 2000

- 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;
- 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 Information Governance Lead

The Information Governance Lead has overall responsibility for records management in Maiden Health. As the 'accountable officer' he is responsible for ensuring the delivery of the Information Governance Agenda. Record management is key to this, as it will ensure appropriate, accurate information is available as required.

Maiden Health has a particular responsibility for ensuring that corporately it meets its legal responsibilities, and for the adoption of internal and external (ie those of commissioning organisations) governance requirements.

6.2 Information Governance and Security Steering Group

The Company's Information Governance and Security Steering Group is responsible for ensuring that this policy is implemented and that records management systems and processes are developed, coordinated, monitored, audited and reviewed. This group meets on a monthly basis and a review of its effectiveness is undertaken by the entire Maiden Health team annually.

7 Legal and Professional Obligations relating to NHS contracts

All NHS records are Public Records under the Public Records Acts. Maiden Health will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS 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

And any current or future legislation affecting records management as it arises.

8 Safe Haven

Mayden Health will ensure that access to confidential information is strictly controlled to minimise the risk of unauthorised access to this information, whether accidental or deliberate.

Mayden Health will implement Safe Haven procedures to safeguard confidential information flowing to, within and from the organisation so that all such information exchanged passes between Safe Haven contact points.

All Mayden Health employees transmitting confidential information must identify and use their relevant Safe Haven contact points and inform their recipients of these Safe Haven procedures to ensure compliance.

Mayden Health will ensure that all members of staff are aware of the existence of the Safe Haven principles and the policies and procedures surrounding it.

Please remember to contact the recipient before safe haven material is faxed to ensure that the information is sent to the correct address.

9 Safe Haven Procedure

9.1 Facsimile

Staff must ensure that whenever practicable confidential information is transmitted using the Secure Fax procedure.

- Where it is not practicable for information to be routed in this way, staff must be aware of any other local documented protocols (either derived through Mayden Health or the commissioning organisation). They should take responsibility both for adhering to them and for drawing the attention of peers and managers to the standards that apply and any associated risks.
- Staff in service areas using fax machines that do not comply with Secure Fax principles but are used for sending and receiving confidential information should consider the security of this and add this concern to the Risk Register.
- Staff should contact the recipient before transmitting the fax to ensure that the confidential information is being sent to the right point.
- Staff receiving faxes sent via Secure Fax contact points should check for the arrival of such faxes frequently and remove them from the fax in-tray within a maximum of 24 hours.
- If sending a fax that relates to an NHS contract or contains patient identifiable data, display the following disclaimer at the bottom of each fax:

IMPORTANT CONFIDENTIALITY/SECURITY: This facsimile is confidential and may be subject to public disclosure under the NHS Code of Openness or the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this fax and any reply cannot be guaranteed. It is intended only for the addressee(s) stated above. If you are not an addressee you should not disclose, copy, circulate or in any way use the information contained in this transmission. If you have received this transmission in error, please notify the sender immediately and then destroy it. Thank you.

- Do not send faxes that contain sensitive information unless specifically requested to do so and first checking that the receiving fax is in a safe haven.
- Please take care when dialling the fax number to ensure accuracy.
- Staff should familiarise themselves with the Caldicott Principles to protect themselves and their clients, as follows:
 - Principle 1 Justify the purpose(s) for using confidential information
 - Principle 2 Only use it when absolutely necessary
 - Principle 3 Use the minimum that is required
 - Principle 4 Access should be on a strict need-to-know basis
 - Principle 5 Everyone must understand their responsibilities
 - Principle 6 Understand and comply with the law

9.2 Letters

- Please send patient identifiable information through the relevant internal/external postal system using the confidential letter envelopes applicable to the appropriate commissioner organisation wherever practicable.
- If not practicable, please mark the envelope SAFE HAVEN – CONFIDENTIAL: RETURN TO SENDER IF UNDELIVERED. Ensure the sender's address is legible.

9.3 Telephone

- Confirm the identity of the other party prior to discussing confidential issues or divulging confidential details. [Protocol needed]

9.4 Email

Patient identifiable data should not be sent by email unless via an approved secure method.

9.5 Electronic – via email using Microsoft protected attachment

Patient identifiable data can be sent by email in an encrypted attachment. The following method is approved but only as 'acceptable practice' as Microsoft email is not a secure transmission process.

- Create a source file (Word usually but could be Excel) to contain the required confidential information.
- Save the document as 'Save as'; highlight on the word 'Tools' (find it on the top tool bar) left click and it will show a drop down list: select 'Options' then 'Security options'; select 'Password to open' and type in this box a password that you must remember; select o.k.; on next screen select 'Save'.
- Create a new e-mail in the normal way and type a clear subject header.
- Write whatever non-confidential text you wish but make sure you advise your recipient to a) contact you for the password and b) remove the attachment from their e-mail once they have opened it.

- Ensure that you finish this email with your signature showing a clear contact number that enables the recipient to get hold of you on the day.
- When your recipient contacts you, confirm their identity and tell them the password so that they can read the file containing the confidential information.

9.6 Electronic – via secure upload to secure live patient site

For transfers of patient identifiable data to/from a client with a live patient management system, the most secure method of transfer is to upload/download data files as an attachment to a dummy patient record. This can be retained against the dummy record indefinitely or as a temporary store.

10 Registration of Record Collections

Mayden Health will establish and maintain mechanisms through which staff can register the records they are maintaining.

The inventory of record collections will facilitate:-

- The classification of records into series; and
- The recording of the responsibility of individuals creating records.

This inventory will form a records register and the register will be reviewed annually.

11 Retention and Disposal Schedules

It is a fundamental requirement that all of Mayden Health's 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 to the Company's business functions.

12 Records Management Systems Audit

The Company will regularly audit its records management practices for compliance with this framework. The audit will:

- Identify areas of operation that are covered by the Company's policies and identify which procedures and/or guidance should comply with the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance;
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of control and adjustment to related procedure

The results of audits will be reported to the team by the Information Governance Lead.

13 Training

All Mayden Health staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance.

14 Review

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are introduced).