



MAYDEN Health
Policies and Procedures

IG03

Personal Information Handling

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	Scope and Purpose.....	1
2	Policy Objectives	1
3	Introduction	2
4	Processing Personal Information	2
5	Management of Patient Data	3
6	Retention of Patient Data	4
7	Management of Client Data.....	4
8	Management of Employee Data	5
9	Protection of Data from Loss, Damage or Inappropriate Access.....	5
10	Ensuring the Reliability of Data.....	5
11	Training	6
12	Inappropriate and Unacceptable Use	6
13	Legislation	7
14	Non-compliance with the Legislation and Policy	8
15	Implementation and Review.....	8
15.1	Implementation	8
15.2	Review.....	8
16	Equality and Diversity statement.....	9

1 Scope and Purpose

This Policy outlines Mayden Health's approach to accessing Personalised Patient Data, Anonimised Patient Data, Client Data and Employee Data, in accordance with The Data Protection Act 1998.

This Policy will be communicated to all employees. All users must confirm in writing that they have read and understood these documents. This Policy will be published to employees through the intranet and a hard copy will be available at Mayden Health's office base.

The Policy applies to all personal information held by Mayden Health irrespective of ownership. In line with the Data Protection Act, personal information is defined for the purposes of this policy as being *anything that can be traced back to a living human being*.

The Policy also applies to all contractors and agencies operating on behalf of Mayden Health. For the purpose of this Policy the term 'employee' covers all of these groups.

This Policy outlines Mayden Health's approach to ensuring all employees effectively process and manage personal information within set standards, to protect the privacy of individuals, and to comply with the principles and requirements of the Data Protection Act 1998 and other legislation. The Policy tells employees how to handle personal information about patients, clients and employees within the company.

This Policy should be complied with for personal information relating to all individuals, whether deceased or living.

This Policy should be read in conjunction with The Information Governance, Information Security and Business Continuity policies.

2 Policy Objectives

The purposes of the Personal Information Handling Policy are:

- To promote the effective, consistent and legal, processing of personal information by defining a personal information policy
- To ensure all employees are aware of their responsibilities in relation to the processing of personal information and to the law surrounding its use
- To ensure all employees are aware of the consequences of the misuse or abuse of personal information
- To establish and maintain trust and confidence in Mayden Health's ability to process personal information
- To ensure compliance with legislation, guidance and standards relating to the handling of personal information

3 Introduction

Mayden Health needs to collect and use certain types of information about patients and clients in order to perform its functions. This also includes information on current, past and prospective employees, suppliers, clients, customers, service users and others with whom it communicates. Mayden Health is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of the Government.

Mayden Health regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining the confidence of clients. It is essential that it treats personal information lawfully and correctly.

The Purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals. It regulates the processing of personal information including the obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal information and gives rights to those whose information is being processed.

4 Processing Personal Information

The processing of personal information is defined as encompassing everything that we do with personal information including the sharing, transferring or disclosing of personal information to another organisation or internally.

Personal Data held on behalf of clients (eg patient data) should only be processed in accordance with instructions from the appropriate client (which may be specific instructions or instructions of a general nature or as otherwise notified) and should only be processed to the extent, and in such a manner, as necessary for provision of the services or as required by law.

Personal information must be processed in accordance with the eight principles under the Data Protection Act 1998 unless a court order applies.

Employees must respect personal information that they have access to and treat it in the manner in which they would expect their personal details to be treated.

Employees must have regard and respect for the privacy of customers and clients and employees and process personal information accordingly.

No employee has an automatic right to access all or any personal information held by Mayden Health by virtue of their position or the fact that they are employed by the organisation. Access to personal information must be accepted by all, to be on a need and right to know basis only.

Personal information should be deleted and disposed of safely and securely as appropriate.

Personal information will be held securely, and accessible only by those with a need and a right to know. Managers are responsible for ensuring that personal information is surrounded by appropriate security (ie relevant to the sensitivity of the personal information).

Personal information must not be transmitted externally electronically without appropriate security.

Personal information will not be passed on to any third party unless in highly exceptional circumstances where:

- permission or consent is obtained
- the organisation requesting the information has a legal right to the information (eg the police investigating a crime) via a S29 or Personal Data Access Request form.
- it is a requirement of law
- to comply with a court order
- we believe it is clearly in the subjects own interest upon discussion of justification with the relevant client(s)
- we believe it is in the overall public interest and in a particular instance this is judged to outweigh the other considerations

In the case of personal data held on behalf of clients (eg patient data) the ownership of the data resides with the client – not Mayden – and data will only be released to any external authority at the express instruction of the client who may or may not be subject to the circumstances listed above.

At the point of collection the subject of the personal information will be informed, if reasonable, of the purposes for which the information will be processed and any other relevant details regarding this processing. This responsibility may be upheld by the NHS if the personal information relates to patients.

Mayden Health will promote good practice in the sharing of information with its partners, government agencies and departments and other public and private sector organisations and will obtain written consent from the client in order to transfer any personal data to any sub-contractors for provision of the services.

The quality and accuracy of personal information should be relevant to the purpose for which it is to be used.

Complaints regarding the handling or processing of personal information should be referred to the Deputy Managing Director.

The rights of the data subjects as defined by the Data Protection Act 1998 and specifically their right of access to their own personal information will be complied with fully and given appropriate respect and priority.

5 Management of Patient Data

For analysis work, patient data is requested with as minimal identifiable fields provided as possible unless they are specifically required. Mayden Health always request that patients' names and addresses are removed from the data sets provided, postcodes are converted into area wards with the postcode fields then being deleted, PAS or Hospital Numbers are converted into unique patient ID numbers, and dates of birth are converted into age bands, with the date of birth fields then being deleted. Mayden Health do not analyse patient lines relating to HIV/AIDS treatment episodes or

lines relating to the termination of pregnancy. Patient information relating to the above is automatically deleted prior to any analysis being undertaken on the dataset.

The above process always applies unless there is a specific analytical need or request from the client to retain data fields. If Mayden Health is required to import patient data into a bespoke patient management tool then there is often a requirement to migrate all data fields into the system. In these instances, once the migration has been completed the original data set is destroyed. There is no requirement to keep patient level data stored within the office environment as data is transferred to a dedicated offsite data centre, via an MPLS secure line.

Procedures relating to the handling of patient information also incorporate the receipt of data from Mayden Health's clients. Patient level data can be sent to Mayden Health primarily through 4 main channels:

- By sending a password protected CD or USB key to the Mayden Health office, via recorded delivery
- By emailing the data in a password protected zip file, encrypted where possible
- By directing Mayden Health to a secure website where they are able to download the data
- By using a secure website (encrypted in both directions) created by Mayden Health, where the client can upload the patient level data, and Mayden Health can then securely download the data from this website. For patient management systems, this is usually achieved by uploading the data file to a dummy patient as an attachment.

6 Retention of Patient Data

Should the contract between the client and Mayden be terminated for any reason, Mayden will liaise with the client to facilitate the safe transfer of confidential patient data to the client. Our preference is to release this data as a database copy in case the service is required to be resumed at some point in the future. However, other data formats can be provided.

Once the safe transfer of data has been completed and verified, Mayden will delete – as far as is practicable – all copies of the client's patient data from its systems, including master and slave databases. Some bit-level backup data may be retained where it is difficult to extract it from other data but this will gradually diminish in line with the normal back-up rotation cycle.

In any case, unless specifically requested by the client, Mayden will remove all patient identifiable data from its systems within three months of service termination.

7 Management of Client Data

Mayden Heath has its own intranet system where entry is password protected and the URL is only available to employees of the company. All client level information is stored within this intranet system, including contact details. Access to the client address book requires an additional password entry. Work contact details only are retained for clients. Home phone numbers are only recorded and used with the client's permission.

8 Management of Employee Data

As with client information, only the work contact details of employees are made available to anyone outside of Mayden Health. However, for HR purposes, employee personal information is retained, and the home contact details for each employee are stored on the secure intranet system.

9 Protection of Data from Loss, Damage or Inappropriate Access

An additional copy of each dataset is always produced by Mayden Health; either through back up or through the retention of the original data source. Data is backed up each night; thus the risk of loss or damaged data is restricted to one day only, as data saved the previous day can be retrieved.

Data can be backed up and stored in three separate locations:

- At the office server on a secure network
- At a designated offsite data centre, transferred by a secure MPLS connection
- On a hard drive which is then backed up on a separate PC at an external location

All datasets, systems and analysis are password protected twice and firewalls have been successfully setup to ensure that access is only granted from a recognised IP address. This ensures that data can only be accessed by eligible employees.

Almost all employees now use a laptop PC and it is expected that these will be taken off-site. Staff are encouraged to take their laptops home to remove the temptation for thieves. For this reason, the following rules apply with respect to personal data held on laptop computers:

- All laptops should be password protected at login.
- Personal data held on a laptop should be kept to a minimum (usually in Outlook and linked to received emails); the primary location for personal data held by Mayden Health is on-line on the intranet.
- Personal data held on behalf of clients should only be present on employee laptops for the time that they are being worked on; otherwise they should be transferred to a TrueCrypt file on the office server.
- Personal data held on behalf of clients should only be worked on at the Mayden office and should not be taken off the premises except with the express permission of the Director.
- Once the data has been processed/analysed it should be deleted if no longer needed; otherwise patient data should be uploaded and kept as an attachment to a dummy patient in the secure live environment.

Regular audits will be performed by all staff to ensure that laptops are free of unnecessary personal data and especially of patient data that is no longer required.

10 Ensuring the Reliability of Data

Mayden Health undertakes two main functions when working with datasets:

- a) The production of bespoke information systems for clients to upload and manage patient level data

- b) The completion of analysis based on patient level data

When producing information systems for clients, Mayden Health is not responsible for the quality of data that the client uploads into the system. The client should ensure that the quality of the data they upload into the system is robust. However, where possible, software driven checks are put into place to alert the user (data uploader) to duplication in entry and incorrect formatting of information in each specific field.

When completing analysis for clients, Mayden Health takes responsibility for ensuring that the accuracy of the analysis is correct. However, this again is subject to the proviso that the quality of the data they have been provided by their clients is robust.

Mayden Health undertakes random manual quality checks against software outcomes to ensure the accuracy of the software programmes. Furthermore it is standard practice to incorporate a 'Data Quality' tab at the front of each analytical spreadsheet compiled by Mayden Health. This will test the outcomes of specific formulas to ensure the expected results are seen.

Mayden Health recognises the importance of data quality and the need to consistently review and improve quality checking processes; and to formulise adopted protocols where appropriate.

11 Training

The Managing Director is responsible for ensuring that all employees receive Personal Information Handling training appropriate to their responsibilities for personal information and their access to personal information.

The employee checklist will be utilised on a monthly basis to assess employee's compliance and understanding of this policy.

12 Inappropriate and Unacceptable Use

Unacceptable use includes:

- Unauthorised access of personal information
- Unauthorised disclosure of personal information
- Unauthorised use of personal information (eg not for reason given to subject)
- Non adherence to the organisation's information-sharing protocols

Employee or client personal information must not be used for:

- Any illegal purpose;
- Any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring Mayden Health into disrepute;
- Any purpose which is not in accordance with the employees role or job description

This is not an exhaustive list.

Employees are required to notify the Managing Director if they become aware, or suspect that personal information is being misused or handled inappropriately.

13 Legislation

The following legislations should be considered when using and sharing personal data;

The Caldicott Report – “Protecting & Using Patient Information”

Within the NHS the Caldicott Report 1997 set out a number of recommendations to improve the way the NHS and its partner organisations handle and protect personal, identifiable information. The Committee identified and established the following 6 key principles:

Justify the purpose

Every proposed use or transfer of personal identifiable information within or from an organisation should be clearly defined and scrutinised with continuing uses regularly reviewed by an appropriate guardian.

Don't use personal identifiable information unless it is absolutely necessary

Personal identifiable information items shall not be used unless there is no alternative.

Use the minimum necessary personal identifiable information

Where use of personal identifiable information is considered to be essential, each individual item of personal information should be justified with the aim of reducing identity.

Access to personal identifiable information should be on a strict need to know basis

Only those individuals who need access to personal identifiable information should have access to it and they should only have access to the personal information items that they need to see.

Everyone should be aware of their responsibilities

Actions should be taken to ensure that all staff who handle personal identifiable information are aware of their responsibilities and obligations to respect confidentiality.

Understand and comply with the law

Every use of personal identifiable information must be lawful.

Data Protection Act 1998

The purpose of the Act is to prevent personal information being used for purposes other than that for which it has been collected for and states that data should be:

- Obtained and processed fairly and lawfully
- Obtained for one or more specified purposes
- Accurate and where possible kept up to date

- Kept for no longer than is necessary
- Processed in accordance with the rights of the data subject
- Stored using appropriate measures against accidental loss or destruction or damage to personal data
- Data should not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects.

The Act works in two ways, giving individuals certain rights whilst requiring those who record and use personal information on computer or manual records to be open about their use and to follow proper practices.

The Act refers to “personal data” which means data that relates to an identifiable living individual, and “sensitive personal data”. This is any personal data that includes the subject’s racial origin, political or religious beliefs, trade union membership, physical and mental health or condition, sexual life, the commissioning of an offence or any proceedings relating to an offence.

Any data collected should always be with the informed consent of that individual or their representative (ie on the NHS commissioner or provider), and it is always advisable to give a full explanation to an individual of the purposes for using their personal information.

Mayden Health acknowledges that their clients are subject to the requirements of the Department of Constitutional Affairs, and the Code of Practice for Government Information, FOIA and the Environmental Information Regulations and shall assist and Co operate with the client to enable them to comply with its information disclosure obligations.

14 Non-compliance with the Legislation and Policy

All employees must be aware of their own obligations with regard to the disclosure and the processing of personal information.

Employees not complying with this Policy or legislation will be dealt with under Mayden Health’s Disciplinary Procedure. Non-compliance may be deemed an act of gross misconduct. In the event of non-compliance by an agency worker or casual worker, his/her work with Mayden Health may be terminated. The contract may also be terminated if the employee is an employee of a contractor.

15 Implementation and Review

15.1 Implementation

This policy will be distributed to all employees with an accompanying letter setting out any individual responsibilities as required.

15.2 Review

This policy and procedure will be reviewed annually, or sooner as required.

16 Equality and Diversity statement

This document complies with Maiden Health's Equality and Diversity statement.