



MAYDEN Health
Policies and Procedures

IG04

Confidentiality Code of Practice

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	1
2	Confidentiality Agreement.....	1
3	Responsibilities and Training	1
4	Disclosure of Information	2
4.1	Disclosure of Information in the Public Interest.....	2
5	Security and Disposal of Confidential Information	2
6	General Principles of Confidentiality	3
6.1	Anonymity	3
6.2	Careless Talk.....	3
6.3	Public Domain	3
7	Termination of Employment.....	3
8	Legislation	4
9	Data Protection Act 1998.....	4

1 Policy

It is the responsibility of Mayden Health, including its Managers, Directors and employees to identify, determine and protect oral or written information which is regarded as confidential.

Employees of Mayden Health are in a position whereby they will receive, handle or be aware of confidential information. They have a duty to their Employer to protect against the wrongful disclosure of confidential information.

2 Confidentiality Agreement

Each employee will be required to sign to state that they have read and understood this confidentiality Code of Practice.

The following are examples of information which are considered to be confidential:

- a) Any information which relates directly or indirectly to the condition, care and treatment of patients.
- b) Any other information about a patient.
- c) Any information about an employee of the Company.
- d) Any other information that you receive, handle or become aware of which is confidential to our business. Such information may include, but not be limited to:
 - Operational policies and procedures
 - Information relating to our fees/charging structure, which is not made generally available.
 - Financial management Information
 - Plans, reports and other material that is of a general, financial, commercial or strategic nature, the disclosure of which could damage the Company

The above examples do not cover all possibilities and any other material classified, known, or believed to be confidential will be considered as relevant to this policy.

This policy is consistent with the General Medical Councils Ethical policy, and is also in line with the requirements of the Data Protection Act 1998, the Human Rights Act 1998 and the common law.

Again, if employees are unsure as to whether a person is entitled to receive confidential information, then their primary duty is to assume that they are not entitled; then check with the immediate line manager.

3 Responsibilities and Training

All staff must understand their responsibilities regarding confidential information and be vigilant for breaches, or potential breaches, of the security of information written or otherwise.

Confidentiality awareness training is the responsibility of Mayden Health, and forms a part of the induction of new staff and should be undertaken on an ongoing basis at staff meetings and away days. The dangers of casual, work related conversations being held in public areas within a client (healthcare or otherwise) environment or within the local communities should be stressed.

Managers are also responsible for monitoring compliance with this policy and for taking appropriate action in the event of a breach.

4 Disclosure of Information

Employees are required not to give any information either on or off company premises to newspaper, magazine, TV or radio reporters or photographers by telephone or in person. Any such enquiries should be directed to the Deputy Managing Director.

The fact that information has already been disclosed in the media does not mean that an employee may disclose or confirm such information.

Under no circumstances whatsoever should information be given orally or in writing to any party not directly connected to the Company without the express approval of the line manager.

The over-riding duty and obligation of employees is to safeguard the interests of the Company. No other member of staff can ever instruct an employee to disregard this policy.

If, at any time, an employee discloses any information, which is confidential, to any unauthorised person or entity then these actions may be subject to a disciplinary enquiry. They may also possibly face prosecution under the Data Protection Act 1998 or other relevant legislation.

4.1 Disclosure of Information in the Public Interest

The company takes the issue of malpractice or wrong doing in any form very seriously and therefore seeks to ensure staff, acting in good faith, who genuinely believe that malpractice is evident, are able to disclose the information to the senior management of the Company without fear of detriment or victimisation, in accordance with the Public Interest Disclosure Act 1998 (the Act).

5 Security and Disposal of Confidential Information

Confidential documents should be shut / locked away at night and kept securely during the day.

Where paper-based confidential information is to be disposed of, then it must be shredded or incinerated.

Our **Personal Data Handling** policy sets out the procedures for the disposal of confidential patient data held on our servers.

In addition, our security checklist ensures that employees:

- regularly check the relevant folders on the office server and confirm that all confidential data has been removed where it is no longer required, or has been uploaded to a secure area on our network in case it is required at some future date, or that is being worked on or backed up temporarily and is being stored in a TrueCrypt vault.
- must check their PCs for confidential data and confirm there are none present other than those that are currently being worked on.

6 General Principles of Confidentiality

Access to files containing medical information or other confidential information should be limited to those individuals who have a proper reason for needing it. They should be able to justify the purpose(s) for using patient identifiable information in the first instance.

Once a file has been accessed, the user should read only what is relevant to the job in hand.

This principle applies without regard to rank or position.

6.1 Anonymity

Patient identifiable information should only be used when absolutely necessary and only the minimum required. Where possible, employees should follow Mayden Health's policy of issuing unique identifiers to identify patients, and convert date of births into age brackets.

6.2 Careless Talk

Casual, work related conversations held in public areas, particularly within healthcare environments, are strongly discouraged and will not be tolerated. Any member of staff who casually discusses confidential details of identifiable individuals with anyone will be in breach of this confidentiality code / policy and may risk disciplinary action. There is also the possibility of prosecution under the Data Protection Act 1998 or other relevant legislation.

6.3 Public Domain

Information should be treated as confidential if the owner of such information takes steps to ensure its secrecy, eg ex directory telephone number, or if it has been disclosed to Mayden Health on the understanding that it should remain confidential.

Any information that is already publicly available may no longer be confidential. However, the fact that information has already been disclosed in the media does not mean that an employee may disclose or confirm such information.

NB If you are in any doubt do not disclose.

7 Termination of Employment

It is the responsibility of the line manager to discuss this policy with the departing member of staff and agree what material should be returned. Such material should not be copied for retention after employment has ended.

On leaving the Company, it is the duty of each employee to return any such material in their possession, at home or at work, to their line manager before their last day of employment.

These restrictions also apply after the termination of employment and will only cease to apply if information has come into the public domain lawfully via the proper channels.

8 Legislation

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

The Caldicott Report – “Protecting & Using Patient Information”

The NHS Caldicott Report 1997 sets 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.

Do not 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.

9 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 purpose
- 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.