



MAYDEN Health
Policies and Procedures

IG02

Information Security

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	Introduction and Scope.....	1
2	Policy Aims	1
3	Policy Objectives	2
3.1	Confidentiality, Integrity and Availability	2
4	Key Duties/Security Responsibilities.....	3
4.1	The Managing Director	3
4.2	Staff.....	3
5	Information Security – Specific Current Practice.....	3
6	Office Security – Specific Current Practice.....	4
7	General Guidelines.....	4
7.1	User names and passwords	4
7.2	Computer protection	4
7.3	Using the internet	5
8	Electronic Mail Policy.....	6
8.1	Introduction	6
8.2	General Guidelines.....	6
8.3	Using Electronic Mail	7
9	User Identification and Password Security	8
10	Validity of this Policy.....	8
11	Information Management and Security Incident Reporting Procedure.....	9
11.1	How to report a security incident.....	10
11.2	Sensitive Security Incidents	10
11.3	Unintentional breaches of security.....	10
11.4	Potential Security Threat	10
11.5	Incident Resolution	11
12	Conflict with other policies and other agreements	11
13	Equality and Diversity statement.....	11

1 Introduction and Scope

This document defines the Information Security Policy for Mayden Health and covers all information (in all forms), information systems, environment and relevant people who support the organisation. This document:

- Sets out Mayden Health's policy for the security of information (especially with regard to Confidentiality, Integrity and Availability)
- Establishes the responsibilities for information security

Information is an asset, which, like other important business assets such as buildings and equipment, has a value to an organisation. Information assets can exist in many forms. Information can be printed or written on paper, stored on a computer or laptop, sent across networks, stored on tapes and diskettes, sent by fax or electronic mail or spoken either in conversations or over the telephone.

Whatever form the information takes, wherever it is held and however it is shared, it should always be appropriately protected. Management has a duty to look after, improve and account for all information assets and information systems. Management must also ensure that work can continue and that the impact of any error or threat is minimised if a security incident takes place.

Mayden Health place a very high importance on the security of information maintained and processed on behalf of the NHS, other health and social care organisations and clients. It recognises a need to segregate operational management and computer operations, and endorses this working practice where possible. It is the responsibility of all employees to comply with this policy and other relevant legislation, together with any supporting policies and procedures local to partner organisations.

2 Policy Aims

The policy aims to ensure that:

1. Computer systems are properly assessed for security
2. Confidentiality, integrity and availability are maintained
3. Staff are aware of their roles, responsibilities and accountability
4. Procedures to detect and resolve security breaches are in place

Mayden Health takes note of, and complies with, the following documents:

- Baseline NHS Security Standards as listed in NHS IM&T Standards Handbook
- BS7799 to the extent of the Scope described in the Information Security Management System (ISMS) documentation
- NHS Net Acceptable Use Policy
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990 (as amended 2006). It is an offence to take steps with intent to secure access to any programme or data held in any computer to which such person is not authorised

- Access to Health Records Act 1990
- The EC Directive on Legal Protection of Databases 1996 (Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases)
- The Caldicott Report 1997 (The Caldicott Committee: Report on the Review of Patient-Identifiable Information – December 1997)
- Data Protection Act 1998 - all staff must abide by the Data Protection Act 1998. Personal information relating to staff, suppliers, etc may only be accessed and used by staff on a need to know basis. Unauthorised disclosure of such “personal data” may result in disciplinary action and prosecution. Under the Act personal data must be:
 - obtained and processed fairly and lawfully;
 - Processed for limited purpose;
 - Adequate, relevant and not excessive;
 - Accurate;
 - Kept for no longer than necessary;
 - Processed in line with the rights of the data subject
 - Secure;
 - Not transferred to countries outside of the European Economic Area (EEA) unless they offer adequate protection

Every individual, including staff, is entitled to be informed of any personal data held on them by the Company, to access that data and to have it corrected if it is inaccurate.

- Human Rights Act (1998)
- Electronics Communications Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2001
- Regulatory and Investigatory Powers Act (RIPA)

3 Policy Objectives

3.1 Confidentiality, Integrity and Availability

The purpose of the security policy is to preserve:

- Confidentiality: Data access is confined to those with specific authority to view the data
- Integrity: All information systems operate according to specification
- Availability: Information is available when required

Employees are expected to be familiar with the internal Business Continuity, Risk and Governance policies and documents; and these should be read in conjunction with this document.

4 Key Duties/Security Responsibilities

4.1 The Managing Director

The Managing Director of Mayden Health has overall responsibility for making sure arrangements are in place for Information Security, and for assigning internal responsibility for Information Security. Furthermore, it is the responsibility of the Managing Director to ensure the overall security of Mayden Health's information and associated assets, hardware and software used by employees and, where appropriate, by third parties. This security should be consistent with legal and 'best practice' managerial requirements and obligations.

It is important that all levels of IT security are communicated to all employees and that sufficient training is in place.

4.2 Staff

All staff are responsible for information security and therefore must understand and comply with this policy and the supporting policies available. It is the duty of each employee who uses or has access to information to be aware of and abide by the procedures and arrangements concerning the secure use and protection of information.

Staff will be provided with the necessary guidance, awareness and, where appropriate, training in relation to all applications, systems and networks they have access to; and staff will adhere to and abide by the rules controlling applications, systems and networks.

All personnel or agents acting for the organisation have a duty to:

- Safeguard hardware, software and information in their care
- Prevent the introduction of malicious software on the organisation's IT system
- Report any suspected or actual breaches in security

5 Information Security – Specific Current Practice

Access into Mayden Health's applications and data is through two routes; via the internet or via the NHS secure N3 network. Access to the internal files, intranet and the hc2d.co.uk data is through a router, and access to client applications and data is either through VPN or through the N3 on a one-way connection only. Data mirrors exist on both servers, so there is contingency if one were to be affected or suffer from a reduction in performance. There is currently no application mirror; however there is a plan to install an additional pair of servers, reflecting the data and application information for each original server. Future plans are in place to add in an additional application and data mirror on an offsite server. On completion of all actions stated above, 4 data mirrors will be in place, offering significant contingency against loss of data or reduced performance. This cluster of servers allows for 'load sharing', and thus in itself reduces the possibility of loss of server performance.

If an application were to fail completely, requiring a hardware/software rebuild, Mayden Health aims to resume the service within four days. Back up data is held at an offsite data centre and data is

sent to this data centre on a daily basis. This data would be used to reconstitute the database – in most cases right up to the last few seconds before the failure.

There is a server in the Mayden Health office, which is backed up to the offsite server each night. This information is also backed up on a hard drive and stored on a PC outside of the office environment. Thus if something were to happen to the server in the office, there are two other means of accessing the data.

6 Office Security – Specific Current Practice

The security of the Mayden Health's office is of paramount importance to the organisation. The office is locked and alarmed, with a 20 second allowance period to enter the alarm code. Details of the alarm code are restricted, and whilst the alarm system is not connected to the Police, it does satisfy the insurance requirements. Windows are secured with screw locks. There are two means of entering the building, and more specifically the server room; through the front door and through a garage which is situated to the rear of the building. Whilst the front door is single entry, the server room requires access through a further set of locked doors once in the building. Access to the server room via the garage requires entry through a further additional 2 locked doors once having entered the building.

There is no patient identifiable or sensitive information on the server that is stored within the office area. All folders that are retained on the office server are password protected, and staff are required to audit the information they store on the server on a monthly basis to ensure that they are not storing patient identifiable data.

The Mayden Health email system is run from the offsite server as opposed to the server in Mayden Health's office. It is a highly secure system which is password protected. Emails are deleted from this main server once they have been moved into Outlook.

7 General Guidelines

7.1 User names and passwords

Each user is responsible for maintaining the security of their individual login and password. Staff must not share their user name(s) or password(s) with anyone. The choice of passwords should comply with industry best practice. Passwords must be changed on a regular basis (between 30 and 90 days depending on the specific system). If a breach of security is recorded under a specific staff login, that member of staff may be deemed responsible for the breach and disciplinary action may be taken.

7.2 Computer protection

Do not leave a computer logged on and unattended. If a computer is left logged on and unprotected, another person can access the internet in your name. Ensure that password protected screen savers or other mechanisms prevent the use of your identity by a third party.

All software should be licensed and from a legitimate source.

Anti-virus software and security applications should be set on auto-update or manually updated weekly.

7.3 Using the internet

7.3.1 *Acceptable use of the internet*

The internet is to be used for work related purposes, for example to help with research for work, to access useful work related sites, for professional development and training or to obtain information related to work.

Limited personal use of the internet is allowed providing it does not interfere with your work, nor expose the organisation to any expense or liability. If this privilege is abused your manager may limit access to work related sites only. You are required to act in accordance with your manager's guidelines.

7.3.2 *Unacceptable use of the internet*

You are not allowed to access, display or download any material that is liable to offend. Material liable to offend includes hostile text or images related to gender, ethnicity, race, sex, sexual orientation, age, religious or political convictions and disability.

You must not use the internet, to attempt any unauthorised access to resources (hacking). Nor are you allowed to access hacker websites as some sites contain traps, which may trigger malicious programmes when an internet page is accessed.

The internet should not be used for browsing, downloading and/or posting (as appropriate) any of the following:

- Content that expresses personal views about subjects unrelated to and inappropriate for a productive workplace.
- Accessing sites that relate to or provide information on criminal or terrorist activity; and/or
- Accessing sites whose prime function is to provide offensive material. Posting, downloading or viewing pornography (ie material that depicts erotic behaviour and is intended to cause sexual excitement) may constitute a criminal offence and is likely to be viewed as gross misconduct warranting summary dismissal.
- Downloading of music, audio and video, not related to work.
- Any breach may be treated as a disciplinary offence, which could ultimately lead to dismissal or criminal prosecution.

7.3.3 *Unintentional breaches of security*

If you accidentally find yourself connected to a site, which contains unacceptable material, you must disconnect from the site immediately and inform your manager.

7.3.4 *Downloading of files and material from the internet*

If you have authority to download files the following rules apply:

- It is a breach of security to download files which disable the network or which have the purpose of compromising the integrity and security of the networks and file servers.
- To intentionally introduce files which cause computer problems could be prosecutable under the Misuse of Computers Act 1990 (as amended 2006).
- Where permitted, file downloads must be done in accordance with laws that protect copyright, designs and patents. Some materials on the internet are copyright works or trademarks belonging to third parties. You must not print or download or in any way attempt to reproduce or disseminate any document or material from the Internet unless you are sure that it is not protected by copyright or trade mark law.

7.3.5 *Joining chat rooms and news group*

If you join a chat group or news group related to your work, you are expected to conduct yourself in a professional manner. Be courteous and inoffensive. Unless you are authorised to do so, you are not permitted to write or present views on behalf of Mayden Health.

8 Electronic Mail Policy

8.1 Introduction

This electronic mail policy forms part of the overall Information Security Policy.

By signing to say that you have read and understood this policy, you have agreed to the electronic mail policy and the code of conduct as described in this document. Failure to comply may result in disciplinary action, which could ultimately lead to dismissal or criminal prosecution.

The purpose of this policy is to clearly explain what is:

- acceptable and
- unacceptable use of electronic mail

8.2 General Guidelines

8.2.1 *User names and passwords*

Each user is responsible for maintaining the security of their individual login and password. Staff must not share their user name or password with anyone. Passwords must be changed on a regular basis.

8.2.2 *Computer protection*

Do not leave a computer logged on and unattended. If a computer is left logged on and unprotected another person can send and receive messages in your name. Ensure that password protected screen savers or other mechanisms prevent the use of your identity by a third party.

8.3 Using Electronic Mail

8.3.1 *Acceptable use of electronic mail*

Electronic mail (email) is to be used for work related purposes. Limited personal use of email is allowed provided it does not interfere with your work nor expose the organisation to any expense or liability. Your manager may stop you from using email for personal use if you abuse this privilege. You are required to act in accordance with your manager's guidelines.

8.3.2 *Unacceptable use of the electronic mail*

You are not allowed to email material that is liable to offend. Material that is liable to offend includes hostile text or images related to gender, ethnicity, race, sex, sexual orientation, age, religious or political convictions and disability. You are not allowed to email material that has a criminal or terrorist content. You are not allowed to send or participate in the dissemination of chain or joke emails. Any breach may be treated as a disciplinary offence, which could ultimately lead to dismissal or criminal prosecution.

8.3.3 *Attachments*

Do not send large attachments unless absolutely necessary. Where drives are shared, indicate the location of the document in the email so that the recipient can find the document. If you do send attachments you need to consider whether the document needs a copyright statement.

8.3.4 *Advertising*

The email system is not intended for commercial or personal advertising.

8.3.5 *Virus protection and detection*

All computers are protected with anti-virus software. However, this only works for a known virus. If you receive an email from an unknown source, think before you open the email. [Review]

The latest version of anti-virus definitions and software (from an industry accepted anti-virus software vendor) must be used to check for, contain the spread of and minimise the impact of malicious software from the ICT Environment.

8.3.6 *Hoax emails*

If you receive an email that you think is from a suspicious source delete it. Email is not the only method of communication and if you mistakenly delete a legitimate, the source will no doubt re-contact you.

8.3.7 *Email content*

Email is treated by a court of law in the same way as spoken or written statements. You must therefore take care with the contents of your email as the contents may form a legally binding document.

8.3.8 Confidentiality clause

A confidentiality clause is automatically inserted into externally sent emails in case they are mistakenly sent to the wrong recipient. This is not visible to the sender at the point of sending.
[Review]

8.3.9 Distribution lists

Email distribution lists should only contain addressees who are appropriate recipients of the email content. Email should not be sent out to a large number of people unless essential as you could be wasting people's time and causing possible disruption to services. Do not ask for acknowledgements from distribution lists.

When using lists 'BCC' should be used instead of 'To' or 'CC' to protect the addresses of those on the list.

8.3.10 House keeping

Each mailbox has a storage limit and you should delete both received and sent email messages on a regular basis. If an email needs to be kept for future reference, save it electronically into an appropriate personal or shared drive.

8.3.11 Non-delivery report, delivery reports and receipt reports

If a message is not delivered, you will receive a non-delivery report. This will normally identify the cause of non-delivery such as incorrect address, unavailable end system, etc. Look at this information first before raising a request for support, as you may just need to correct the address.

Delivery reports indicate that the email has been successfully sent and will only be returned if the sender has requested it.

Receipt notifications indicate that the recipient has opened the email. However, recipient reports are not guaranteed and often require recipient consent. Remember that the recipient may not have read or acted upon the email, as a personal assistant or administrator may have read the email on behalf of the recipient.

Delivery reports or read receipt notifications should only be used when you need positive confirmation that a message has been received and read.

9 User Identification and Password Security

It is the users' responsibility to ensure that their user identification and password are kept secure.

10 Validity of this Policy

This Information Security Policy and all supporting policies will be reviewed annually. Supporting policies will also be reviewed when required, taking into account new systems, new ways of working as well as new government initiatives and directives.

11 Information Management and Security Incident Reporting Procedure

This Information Management and Security Incident Reporting Procedure forms part of the overall Information Security Policy.

Incident reporting plays a major role in helping the organisation maintain a secure working environment. It helps protect the confidentiality, integrity and availability of the information and systems accessed. Trend analysis of reported incidents enables the organisation to highlight areas of weakness and, if necessary, take appropriate action to reduce specific threats and vulnerabilities.

All staff members have a responsibility to report security incidents whether deliberate or accidental.

This procedure also covers reporting security weaknesses and software malfunctions.

A security incident is defined as: Any actual or potential breach of security, which may comprise the confidentiality, integrity or availability of information.

The term security incident covers a wide range of events, which can vary considerably, and it is therefore not possible to detail every single event. However, the following list gives examples of types of security incidents that should be reported:

- Disclosure of confidential information to an unauthorised person
 - The accidental or deliberate sending of a confidential email to an unauthorised person
- Password compromise
 - An unauthorised person has gained access to your account or attempted to gain access using your password
 - You suspect that other people in the organisation are misusing passwords
- Hacking attempt
 - There has been a deliberate attempt to gain unauthorised access to information
 - You have reason to believe unauthorised persons are using or attempting to use IT systems
- Virus attack
 - You suspect a virus has entered the network or company's IT infrastructure
- Physical security breach
 - You have evidence, or suspect that unauthorised persons have gained or attempted to gain access to premises or secure areas
- Theft or loss of information or equipment
- Unlicensed software
 - The installation or distribution of unlicensed or unauthorised software
- Gaining of information by deception (social engineering)
 - Gaining of eg passwords, patient identifiable information, personal addresses, by unauthorised persons posing as engineers, relatives, doctors, etc, using e-mail or via telephone

- Inappropriate use of email
- Examples include the sending or receipt of fraudulent emails requesting cash or services, chain mail, hoaxes, offensive or threatening mail, bulk mail (bombarding people with unwanted email).
- Inappropriate use of the internet

This includes but is not limited to, activities such as:

- the possession, viewing, downloading, or transmission of any offensive material;
- advertising or operating home business from the workplace;
- use of web sites to access or downloads unauthorised software, images or documentation

This list is not exhaustive and staff must ensure they report any incident that has or may result in:

- Disclosure of confidential information to an unauthorised person
- The integrity of information being put at risk
- The availability of information or information systems being affected.

11.1 How to report a security incident

All security incidents should be reported in the first instance to your line manager. [Review]

11.2 Sensitive Security Incidents

It is recognised that some incidents can be sensitive especially if colleagues or managers may be incriminated. It is important that the person reporting the incident receives absolute protection and guarantee of confidentiality even in the event of a false alarm.

11.3 Unintentional breaches of security

If an individual unintentionally causes a breach of security eg, accidentally accessing an inappropriate website, they should inform their line manager immediately. The reporting procedure detailed above will still be followed. If management are satisfied that the breach is accidental no disciplinary action will need to be taken.

11.4 Potential Security Threat

Staff are required to report any observed or suspected potential security incident eg:

- Individuals having unlimited attempts to guess a password
- Passwords stored as readable text files which can be viewed by unauthorised individuals
- System administration privileges given to individuals who do not require them

Staff must not attempt to prove a suspected potential security incident as this might be interpreted as a potential misuse of the system. Instead the weakness must be reported to their own line manager.

11.5 Incident Resolution

Once the incident has been dealt with and closed, the individual who reported the incident should be notified of the resolution.

12 Conflict with other policies and other agreements

If there is any conflict between the terms and conditions of this Policy and those of any supporting policy; or any employment contract or other agreement, then the terms of this Policy shall take precedence.

13 Equality and Diversity statement

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