Information Governance Policies and Procedures 2012

ISMS14

Personal Information Handling Policy

ISMS Policy Index	
ISMS01	Information Governance Policy Statement
ISMS02	Information Security Policy
ISMS03	Risk Management Policy
ISMS04	Internal Audit Plan
ISMS05	Information Security Risk Assessment Policy
ISMS06	Business Continuity Plan
ISMS07	Clear Desk and Screen Policy
ISMS08	Email Security/Acceptable Use Policy
ISMS09	Laptop Security Policy
ISMS10	Outsourcing Security Policy
ISMS11	Physical Access Policy
ISMS12	Lifecycle Management Policy
ISMS13	Confidentiality Code of Practice
ISMS14	**Personal Information Handling Policy**
ISMS15	Router Security Policy
ISMS16	Patient safety assessment on health software

Current Version

Responsibility of	Information Governance Lead
Reviewed by	IG Group
First Issued	16 March 2011
Last Review Date	October 2011
Next Review Date	October 2011

Version History

Version	Date	Comment	Initials	Signature
		Draft	CE	
	16/3/11	Draft ISMS 2011	PE	
	13/7/11	Draft QA	ASD	
2.0	1/10/11	Issued to company for comment	ASD	
2.1	Dec 11	Updated for issues arising from company-wide review	ASD	
3.0	25/1/12	Latest version release incorporating changes from review by all staff October 2011	ASD	

Roles and Responsibilities	
Information Governance Lead	Chris May
Information Security Lead	Steve Exley
Patient Data Governance	Chris Eldridge
Company and Employee Data Governance	Alison Sturgess-Durden

CONTENTS

1 Scope and Purpose

Mayden 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 as well as patient identifiable data (please refer to Appendix 7 of the DOH Report on the Review of PI data, http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf.). Mayden 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 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.

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

The policy applies to all personal information held by Mayden 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*.

This policy outlines Mayden'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.

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

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 Information Security and Business Continuity policies.

2 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's ability to process personal information.
- To ensure compliance with legislation, guidance and standards relating to the handling of personal information.

3 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 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.

Where necessary, employees will undergo necessary vetting procedures to have access to and handle sensitive data. References are taken up for all recruits. Staff are only given access to personal data once they have passed through their induction and probation periods and we are confident they are competent to work on live data securely.

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

Personal information will be held securely, 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 by electronic means 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 subject's 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 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 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 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.

4 Management of Patient Data

For analysis work, patient data is requested with as few identifiable fields provided as possible unless they are specifically required. Mayden always requests 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 does 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 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 a secure VPN.

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

- By using a secure website (encrypted in both directions) created by Mayden, where the client can upload the patient level data, and Mayden 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. Mayden also has a web based dropbox on the N3 network for larger files.
- By directing Mayden to a secure website where they are able to download the data
- By sending a password protected CD or USB key to the Mayden office, via recorded delivery
- By emailing the data in a Truecrypt encrypted file as an attachment with the password phoned through to the intended recipient.
- Mobile devices should really just be considered as small computers and data treated the same as we would a laptop.

If company data is accessed using a mobile device such as a smart phone or tablet then the device needs to be appropriately secured. A minimum 4 digit pin should be setup where 10 failed attempts would wipe the phone, preferably with a GPS tracking app setup. A screen lock should be setup with an appropriate lock time of 5 minutes or less. Data files on the phone should be encrypted using an appropriate method. "Jailbreaking" devices should not be encouraged, and a device which has been "Jailbroken" should not be used to secure company data.

Data should not be stored on any removable media without it being suitably encrypted.

5 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 subset export of the database 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.

All laptops or desktops disposed of by Mayden have their hard drive destroyed by the IG team.

6 Management of Client Data

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

Refer also to section 4 concerning clients' proprietary and commercially confidential information.

Data used and stored concerning users of the Mayden website is governed by the terms of the website privacy statement available at www.mayden.co.uk.

7 Management of Employee Data

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

8 Protection of Data from Loss, Damage or Inappropriate Access

Further procedures for mitigating the impact of loss, damage or inappropriate access to restricted data are detailed in ISMS02 Information Security, Section: Office Security. The following should be adhered to in light of the procedures set out in ISMS02

An additional copy of each dataset is always retained by Mayden, either through back up or through the retention of the original data source. As a minimum, data is backed up each night, thus the risk of loss or damaged data is restricted to at most, 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 which is itself backed up to a remote server in Box.
- At a designated offsite data centre, transferred by a secure VPN 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 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 Managing 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.

In the event of data loss or corruption, Mayden will comply with its obligations set out in any contract between itself and the client in question, including the stipulations of any Security Addendum to the contract.

9 Ensuring the Reliability of Data

Mayden undertakes two main functions when working with datasets:

- The production of bespoke information systems for clients to upload and manage patient level data.
- The completion of analysis based on patient level data.

When producing information systems for clients, Mayden 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 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 with by their clients is robust.

Mayden 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. This will test the outcomes of specific formulas to ensure the expected results are seen.

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

10 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 quarterly basis to assess employees' compliance and understanding of this policy.

11 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 into disrepute.
- Any purpose which is not in accordance with the employee's 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.

12 Legislation

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

12.1 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.

12.2 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 and 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 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.

13 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'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 may be terminated. The contract may also be terminated if the employee is an employee of a contractor.

14 Policy Compliance

14.1 Relationship to other policies and agreements

This policy is one part of Mayden's overall Information Security Management System (ISMS) document set. It should be read and adhered to in conjunction with the other policies making up the ISMS document set (**ISMS01-ISMS15**).

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, in relation to any matters of Information Governance, then the terms of this policy shall take precedence.

14.2 Awareness and training

All employees are expected to read and comply with the terms of this policy. This policy will be brought to the attention of all employees each time it is revised and reissued. All new members of staff are expected to read this policy as part of their induction. A copy will be placed on the Mayden intranet for easy reference. A quarterly checklist will be completed by all members of staff to confirm they are complying with key elements of Mayden's ISMS documentation.

All staff will be given necessary training to support their compliance with this policy.

14.3 Enforcement

Compliance across Mayden will be monitored via the internal audit programme as set out in **ISMS04**.

Mayden works to maintain a culture within Mayden where information governance and information security are taken seriously, and where there is openness and honesty in the reporting of issues, risks, near misses and incidents whenever they are identified and whoever identifies them.

A 'no blame' approach has been adopted to help promote this culture. Where an employee finds that they, or another member of staff, are acting in violation of this policy, they are expected to report the matter to their line manager who will log the issue, and be responsible for agreeing an appropriate course of action in conjunction with the Information Governance Group. Action will always be proportionate, constructive, and taken with a view to educating and developing staff and improving Mayden systems and processes. The same procedure will be adopted where compliance issues are identified via the internal audit process.

In the case of persistent, gross and/or deliberate failure to comply with information governance policies, then Mayden's capability and disciplinary procedures may need to be initiated as set out in the Employee Handbook.

14.4 Review

This policy will be reviewed when necessary (eg as a result of an incident or near miss or change in legislation), but at least annually as a minimum.

14.5 Equality and Diversity statement

This document complies with Mayden's Equal Opportunities statement as set out in the Employee Handbook.