



**MAYDEN Health**  
**Policies and Procedures**

**IG06**

**Risk Management**

Information Governance

**August 2010**

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

### Current Version

<b>Responsibility of</b>	Information Governance Lead
<b>Reviewed by</b>	
<b>First Issued</b>	November 2009
<b>Last Review Date</b>	August 2010
<b>Next Review Date</b>	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 Policy Statement .....	1
1.1	The scope and role of Risk Management.....	1
1.2	Definition of Risk.....	1
1.3	Process of Risk Management.....	1
1.4	Information Security Risk Management .....	2
2	Key duties for the control of risk.....	3
2.1	Audit.....	3
2.2	The Managing Director .....	3
2.3	Staff.....	3
2.4	Associated staff.....	3
2.5	Contractors .....	4
3	Risk Management Process .....	4
3.1	New Activities .....	4
3.2	Risk (hazard) identification and description .....	4
3.3	Quantifying risk.....	5
3.4	Assessing Risk.....	6
3.5	Controlling risk.....	6
3.6	Risk registers .....	6
3.7	The recording and reporting of risks.....	7
3.8	Monitoring and review of Risk.....	7
3.9	Risk Training .....	7
4	Implementation and Review.....	7
4.1	Implementation .....	7
4.2	Review.....	7
5	Risk assessment .....	8
6	Carrying out a Risk Assessment .....	8
7	Training .....	10
8	Applicable Legislation .....	10
9	Equality and Diversity statement.....	10

---

## 1 Introduction and Policy Statement

### 1.1 The scope and role of Risk Management

It is a key organisational responsibility to identify and control all risks that might have an impact on the organisation's objectives, its staff and the people that it interacts with.

This policy identifies key aspects of Risk Management, the duties to be discharged, the way risk systems are coordinated and integrated, and explores individual risk systems.

The implementation of Risk Management is good management practice and central to the effective running of the organisation. Mayden Health will ensure that any decisions made on behalf of the organisation are taken with due consideration to the effective management of risks.

### 1.2 Definition of Risk

A risk can be defined as any circumstance that may arise and have an impact on the organisation's ability to meet its objectives. Impacts can be positive or negative, but it is inevitable that the main focus will be on those circumstances which threaten the achievements of objectives. Risks can be characterised as:

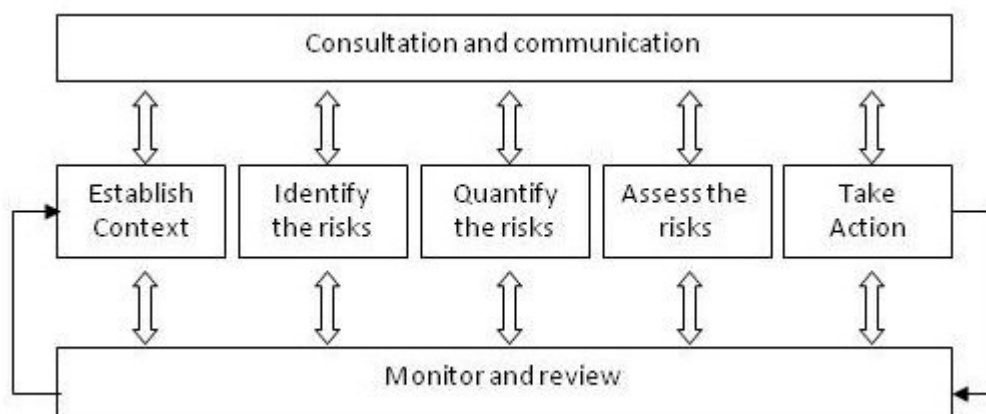
- Risks to the person (patients, staff and others)
- Risks to the reputation of the organisation
- Risks to the assets of the organisation (financial and physical)
- Risks that do not comply with the law or other requirements
- Risks to objectives

### 1.3 Process of Risk Management

The process of Risk Management can be characterised as a continuous, cyclical process whereby, at any level within an organisation, the following is carried out:

- **Establishing context:** What are the objectives to be achieved – these can include the maintenance of duties, requirements, standards etc as well as the achievement of change.
- **Identification of Risks:** What circumstances could arise that would threaten the achievement of objectives. In other words, what are the hazards?
- **Quantifying the Risks:** Two aspects are considered, and scores applied.
  - First, what would be the consequence if a risk were to materialise – what would the impact be?
  - Second, how likely is the circumstance to come about?
  - The two scores are multiplied together for an overall score.
- **Assessing the Risks:** The measures already in place to control a risk – either through reducing its impact or the likelihood of occurrence are considered. Is more control required or can the current level of risk be accepted and monitored? How does this risk compare to others? What priority for action in relation to other risks should be applied?

- **Taking action:** If additional action is required to control risk, then specific measures must be identified and implemented.
- **Monitoring and review:** Risks must be monitored to ensure that actions taken have been successful in reducing the risk to an acceptable level and progress reviewed at all levels of the organisation.
- **Consultation and communication:** It is essential that information about risk is communicated effectively, up, down and across the organisation and where appropriate to stakeholders outside the organisation.



*From Australian/New Zealand standard AS/NZS 4360:1999*

Once a risk has been identified and assessed, there are a number of options available to control the risk, as follows:

- **Elimination:** the activity which leads to the risk is eliminated
- **Export:** the activity is carried out outside the organisation, with another organisation bearing the risk
- **Risk treatment:** suitable controls are implemented which reduce the impact or likelihood of the risk
- **Insurance:** arrangements are made to reduce the financial impact of the risk
- **Acceptance:** the risk is accepted and monitored and the consequences managed as part of normal business

#### 1.4 Information Security Risk Management

Mayden Health relies on well managed information systems. Therefore all information should be managed to prevent misuse or inappropriate disclosure. Information security risks must be on the corporate risk register and be managed accordingly. Where an information security risk is identified, the scoring of its impact/consequence must be informed by the relevant rows in the risk consequence table as set out in Appendix 1. Further, specific information on Information Security can be found in the Information Security Policy.

## **2 Key duties for the control of risk**

### **2.1 Audit**

Mayden Health will ensure that an annual external audit and review of governance, risk management and internal control across the whole organisation's activities will take place, with recommendations implemented and reviewed frequently.

### **2.2 The Managing Director**

The Managing Director of Mayden Health has overall responsibility for all resources; implementing and operating internal risk control systems, and ensuring the quality and safety of the services provided by Mayden Health.

The Managing Director should ensure that a corporate risk register is maintained, reviewed and updated regularly. Furthermore, the Managing Director is responsible for ensuring all formal necessary "risk assessments" are carried out and that risks are controlled by implementing, operating and contributing to the appropriate risk control systems set out in the overarching organisation's policies.

It is important that all levels of risk information are communicated to all employees and that sufficient risk training is in place to enable employees to:

- Identify and report adverse events and risks
- Undertake their roles safely and effectively.

### **2.3 Staff**

Staff have a duty to comply with all arrangements for Risk Management, including the identification and reporting of adverse events and hazards according to their competence and where appropriate, professional duties.

Staff should also take part in an appraisal and development process that enables personal review of risk responsibility and undergo any training required. This includes completion of the monthly employee checklist.

Furthermore, it is important that staff have a positive and proactive attitude to matters of risk.

### **2.4 Associated staff**

Staff working for other employers but working alongside Mayden Health on the organisation's premises have a duty to comply with arrangements for Risk Management, including the identification and reporting of adverse events and hazards according to their competence and where appropriate, professional duties.

## 2.5 Contractors

All contractors working on Mayden Health’s premises must comply with specified contractual obligations with regard to risk, procedures for working on premises and any local Health and Safety requirements.

## 3 Risk Management Process

### 3.1 New Activities

When new activities are contemplated, planned for or implemented, it will be important that associated risks are identified and managed effectively.

Responsibility for identifying and managing the risks of change and new activities lies with the person(s) responsible for the changes.

Risk identification and control must form part of any arrangements to initiate, plan for or implement change or new activities.

### 3.2 Risk (hazard) identification and description

#### 3.2.1 Identification

The identification of Hazards (circumstances with the potential to cause harm) is both a reactive and proactive process. Not only must the process involve the analysis of what has happened already, but it must also involve the identification of what could happen in the future. This is shown in the table below:

	Source: Inside the organisation	Source: Outside the organisation
What has happened (historic)	Complaints, incidents, audits, claims, operational and financial data, reflective practice, team discussion, induction, appraisal, policy review, self inspection, HR process outcomes.	Performance review, inspections, national initiatives, safety alerts, national audit.
What could happen (prospective)	Risk assessments (specific and generic), internal advice, guidance, plans & objectives, discussions with staff, sources of shared learning.	National Bodies, safety alerts, external consultation, national/local targets.

#### 3.2.2 Describing a risk

The risk description for each entry of the Risk Register should be clear, unambiguous and represent an actual risk rather than a control weakness or statement. The description should include an event or trigger and its consequences, for example:

- Poor contract performance leads to financial penalty (amount)
- Loss of confidential data leads to national reputational damage

### 3.3 Quantifying risk

#### 3.3.1 Likelihood

The likelihood (or probability) of the risk materialising must be estimated and scored 1-5. It may be possible to do this using reliable historical information but may also involve an educated guess. The scores should take into account the existing measures in place to control the risk (see below);

Likelihood will be estimated using the following guide:

RISK LIKELIHOOD TABLE – Guidance

Descriptor	1	2	3	4	5
	<b>Rare</b>	<b>Unlikely</b>	<b>Possible</b>	<b>Likely</b>	<b>Almost certain</b>
<b>Frequency</b>	Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
<b>Probability</b>	<1% Will only occur in exceptional circumstances	1-5% unlikely to occur	6-20% Reasonable chance of occurring	21-50% Likely to occur	>50% More likely to occur than not

#### 3.3.2 Impact or consequence

Impact will be scored from 1-5 as follows:

Risk impact scoring table

Impact	Insignificant	Minor	Moderate	Major	Catastrophic
Score	1	2	3	4	5

Each score is combined as follows:

		Consequence or Severity of Harm				
		1 None	2 Minor	3 Moderate	4 Major	5 Death, Catastrophe
Frequency or likelihood of recurrence	5: Certain expected to occur	Moderate Yellow 5	Significant Amber 10	High Red 15	High Red 20	High Red 25
	4: Likely will occur in most circumstances	Moderate Yellow 4	Significant Amber 8	Significant Amber 12	High Red 16	High Red 20
	3: Possible should occur at some time	Low Green 3	Moderate Yellow 6	Significant Amber 9	Significant Amber 12	High Red 15
	2: Unlikely might occur at some time	Low Green 2	Moderate Yellow 4	Moderate Yellow 6	Significant Amber 8	Significant Amber 10

	1: Rare will occur only exceptionally	Low Green 1	Low Green 2	Low Green 3	Moderate Yellow 4	Moderate Yellow 5
--	---------------------------------------	-------------	-------------	-------------	-------------------	-------------------

### 3.4 Assessing Risk

The assessment stage involves:

- Assessing the adequacy of existing measures actually in place to control the identified risk. Existing control measures should be considered during the risk scoring process.
- Forming a view on the acceptability of the current position and whether further action is required to control the risk.

### 3.5 Controlling risk

The level to which risks must be reported and the decisions/action taken to control them is determined by the risk score and is set out in the table below:

RISK SCORE			
LOW (Green) 1-3	MODERATE (Yellow) 4-6	SIGNIFICANT (Amber) 8-12	HIGH (Red) 15-25
Normal risks which can be managed by routine procedures	Responsibility for action allocated to a named individual	Urgent senior management attention needed, with action planned within the month	Immediate action required by a Director who must be informed immediately.
Level of Authority for action and reporting route			
Team Leader or equivalent	Team Leader or equivalent	Managing Director	Managing Director

It is acknowledged that some risk will always be inherent and therefore should be appropriately identified and every effort made to ensure that all risks are minimised to an acceptable level. As it is not possible to reduce all risks to zero there needs to be a balance between risk and benefit and the use of available resources.

### 3.6 Risk registers

A risk register is a tabulated list of risks for a level or area (it may be the whole organisation) that typically:

- References a risk
- Describes it (including the consequences)
- Classifies or codes it
- Records where in the organisation it arises, and therefore who "owns" it
- Records the consequence, likelihood and overall scores
- Assesses the adequacy of controls
- Identifies the action to be taken

- Identifies who is responsible
- Sets a date for further review

A generic layout is shown below:

Ref	Description	Scores	Controls	Accountability	Action	Review date
1	xxx...					
2	etc					

The actual layout of risk registers in use at Mayden Health is determined by the Managing Director.

Risk registers are working documents requiring ongoing update.

### 3.7 The recording and reporting of risks

When risks are assessed, they must be formally recorded on Mayden Health Risk Register.

### 3.8 Monitoring and review of Risk

Monitoring and review of risk will take place as part of normal management working. The Risk Register is a useful tool for this and will be supported at the detailed level by the action planning documentation that may support action on any particular risk.

There will be suitable communication throughout the organisation regarding risks so that information is passed up to provide assurance on the effectiveness of processes.

The Risk Register will be updated monthly and discussed at team meetings.

### 3.9 Risk Training

Mayden Health has a systematic approach to Risk Management training to ensure that the training needs of each individual are identified by way of a training needs analysis.

Employees will be provided with Risk Management training on induction, and will use the employee checklist each month to further reinforce this training and knowledge.

## 4 Implementation and Review

### 4.1 Implementation

This policy and procedure will be distributed to all employees with an accompanying letter setting out any individual responsibilities as required. This policy and procedure will be available on the Mayden Health's intranet and hard copies will be kept at the office in the relevant policy folder.

### 4.2 Review

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

## 5 Risk assessment

A risk assessment is nothing more than a careful examination of the hazards associated with the work activities and premises that could cause harm to people. These hazards are evaluated to decide if adequate precautions have already been taken, or whether more can still be done to prevent harm.

The following factors apply in general terms to all risk assessments:

- An assessment need only be done once, and need not be duplicated to satisfy a similar duty under a different regulation (although the findings of an initial assessment may require a more detailed assessment such as with manual handling).
- Must be undertaken by a competent person. All staff having attended the Risk Management Training are deemed competent.
- Must be reviewed or re-assessed when necessary, such as when there is a significant change in working practice or environment.
- Must take into account changes in technology.
- Needs to be monitored to ensure that risk control needs are measured and effective.
- Requires adequate record keeping (sometimes for a prescribed period).
- Requires consultation with staff and their appointed representatives.
- Must be supported by information and training for staff.

## 6 Carrying out a Risk Assessment

Any risk assessment must consider and take account of the following:

- How likely is it that something that will go wrong?
- Who would be affected?
- If it goes wrong, how serious are the consequences?
- How frequently does the risk arise?
- Are the effects immediate or delayed (acute or chronic)?
- What are the legal requirements to control the hazard?
- What are the commissioner's requirements?

The Health and Safety Executive (HSE) have produced a book about risk assessment entitled "5 steps to risk assessment". The procedure detailed below follows that principle and is endorsed by Prime Diagnostics Limited. The steps are:

- Step 1 – Identify the Hazards
- Step 2 – Identify People at Risk, types of people and quantities
- Step 3 – Evaluate the Risk (consequence versus likelihood)
- Step 4 – Record your Findings/Communicate with stakeholders
- Step 5 – Review and Revise the Assessment as necessary

### ***Step 1 – Identify the Hazard***

The hazard may have already been identified using the hazard reporting procedure or may be part of an initial assessment or review of an assessment.

There may have been an incident or near miss which highlighted a previously unknown hazard. A Health and Safety issue may be noted that has not been previously addressed.

### ***Step 2 – Identify People at Risk***

Consider any group of people who may be at risk. This includes employees, patients, visitors the public and maintenance contractors. Remember there is a greater duty of care toward the young, the sick and the elderly.

Quantities of people at risk should be identified in order to achieve a realistic risk rating for a particular hazard, numbers involved should be recorded on the risk assessment pro-forma as part of the risk assessment process.

### ***Step 3 – Evaluate the Risk***

For each hazard identified it is necessary to identify the significant risks. In doing this consider the worse case scenario and the control measures that are already in use.

The most common method of evaluating risk is to give a numerical value. In order to fully integrate this procedure with the Risk Register the risk quantification maturity matrix attached in appendix 1 must be used to identify the appropriate levels of consequence and the likelihood of the event occurring.

A numerical value between 1 and 5 must be given for both levels of consequence and levels of likelihood, the figures must be recorded on the risk assessment form, by multiplying the figures by each other the risk rating is identified and appropriate action to be taken.

Having calculated the Risk Ranking the action required must be considered. This is based upon what is “reasonably practicable”, weighing the overall risk against time, trouble, cost and degree of difficulty needed to eliminate the risk.

The level of control is based upon a hierarchy as outlined below:

- Eliminate the hazard at source – no residual risk.
- Substitute the hazard for one with a lower risk.
- Enclose the hazard.
- Segregate the hazard to prevent access.
- Develop written procedures to control the risk.
- Provide adequate supervision.
- Provide training to employees.
- Provide information and instructions – signs.
- Use of personal protective clothing (only as a last resort).

The risk assessment pro-forma should be used to record the levels of risk both before and after action has been identified.

#### ***Step 4 – Record and Reporting your Findings***

The assessment must be recorded where there are five or more people employed, or where there is a significant risk. This means writing down the significant hazards, the risk ranking and suggested actions.

All assessments must be reported to all staff affected at least annually or when the process changes and the assessment reviewed. All assessments must be routed to the line manager and appropriate assessments in accordance with the risk matrix must be routed to the Risk Lead to include within the Risk Register. On an annual basis, the Risk Register will be reviewed at Board level.

#### ***Step 5 – Review and Revise the Assessments as Necessary***

Risk assessment is a continuous and on going process. Any significant changes in either working practice or environment could introduce new or unfamiliar hazards and affect the risk assessment. Accidents and incidents may also identify hazards that are not adequately controlled. All reviews of a particular hazard must be communicated to staff.

## **7 Training**

In order to ensure that hazard identification and risk assessment are undertaken, it is essential that staff receive suitable and sufficient training in the techniques that are required.

Under current health and safety legislation employers are required to provide all such training that is necessary to ensure the competency of its employees, and that such training is undertaken during work hours at no charge to the employee.

## **8 Applicable Legislation**

- Health And Safety At Work etc Act 1974
- Management of Health and Safety at Work Regulations 1999
- Manual Handling Operations Regulations 1999
- Lifting Operations and Lifting Equipment Regulations 1999
- Control of Substances Hazardous to Health Regulations 2002
- Provision and Use of Work Equipment Regulations 1998
- Personal Protective Equipment Regulations 1996
- Display Screen Equipment Regulations 1992

## **9 Equality and Diversity statement**

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

**Appendix 1**

<b>Impact</b>	<b>Insignificant</b>	<b>Minor</b>	<b>Moderate</b>	<b>Major</b>	<b>Catastrophic</b>
<b>Score</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Service/ Business interruptions</b>	Interruption in a service, which does not impact on the ability to continue to provide service. Immediate on-site containment.	Short-term disruption to service with minimal impact. Locally contained situation.	Some disruption in service with unacceptable impact. Non-permanent loss of ability to provide service. On-site containment with outside assistance.	Sustained loss of service, which has serious impact on delivery resulting in major contingency plans being invoked.	Permanent loss of core services or facility.
<b>Patient/ Staff feedback/ Litigation</b>	Unlikely to cause complaint. Litigation risk is remote.	Complaint possible. Legislation unlikely	Litigation possible but not certain. High potential for complaint.	Litigation expected/ certain.	Litigation expected/ certain.
<b>Adverse Publicity/ Reputation</b>	Unlikely to warrant coverage in media, little effect on client confidence/staff morale.	Local Media – short-term. Minor effect on staff morale/ client attitudes.	Local Media – Long-term impact on staff morale and overall perception of organisation.	National Media <3 days. Public confidence in organisations undermined. Usage of services affected.	National Media >3 days.
<b>Quality of the Client/ Staff Experience/ Outcome</b>	Unlikely to impact on quality of client or staff experience.	May impact on client/ staff experience – readily resolvable	Mismanagement of client or staff experience, short-term effects (less than a week)	Mismanagement of client or staff experience, Long-term effects (more than a week)	Totally unsatisfactory client/ staff outcome or experience.
<b>Performance targets</b>	No impact on targets.	Insignificant impact on targets.	Adverse effect on targets.	Failure to meet targets.	Failure to meet statutory obligations.
<b>Injury/ Harm</b>	No injuries or adverse outcome.	Short-term injury/illness <3days sickness	Adverse event, which impacts on small number of people. RIDDOR reportable. Long term sickness. Semi-permanent injury/illness	Permanent injury. Long-term adverse effect.	Incident leading to unexpected death or major permanent injury to one or more person.
<b>Information Security</b>	Damage to an individual's reputation.	Damage to a team's reputation. Some local media interest that may not go public.	Damage to an organisation's reputation. Local media coverage.	Damage to an organisation's reputation. Local media coverage	Damage to reputation. National media coverage.

<b>Information Security</b>	Potentially serious breach. Less than 5 people affected or risk assessment as low, e.g. files were encrypted	Serious potential breach & risk assessed high, e.g. unencrypted clinical records lost. Up to 20	Serious breach of confidentiality, e.g. up to 1000 people affected.	Serious breach with either particular sensitivity, e.g. sexual health details or up to 1000 people affected.	Serious breach with potential for ID theft or over 1000 people affected
-----------------------------	--	---	---	--	---