Information Risk Management Policy

Inmind Reference:	GDPR02
Category:	General Data Protection Regulation (GDPR) Policy
Version Number:	1.3
Reviewed on:	Jan 2018
Next review date:	Jan 2019
Lead Officer:	GDPR / Director of Contract Performance
Equality Impact Assessment completed:	Yes

Applicable Legislation/Regulations:

NHS Information Security Policy
Health and Social Care Act 2008
Information Commissioners Office (ICO)
General Condition 21 – NHS Standard Contract – Patient Confidentiality, Data Protection, Freedom of Information and Transparency.

Codes of Practice:

NHS Information Risk Management – Digital Information Policy
Please note that this policy has been developed in line with the NHS Digital Best Practice Information Risk Template.
Information technology - Security techniques - Information security management systems - Requirements

Purpose:

The primary objective of this policy is to ensure that Inmind minimizes the dangers of financial and reputational loss caused by untoward events relating to information. This is achieved by ensuring that risks to all data assets are identified, understood and managed appropriately. The objective of the policy is to present a comprehensible, workable framework, understood by all relevant employees, which manages risks to information assets.

Version Control Table

Date Ratified	Version Number	Status
Jan 2018	1.3	Live

Date	Key Revision
Jan 2018	New Information Risk & Risk Matrix to ensure compliance with IG Toolkit – Level 2
Jan 2018	Update on the ISO/IEC 27001:2013 standards
Jan 2018	Addition of consent for disclosure of confidential information

Please check to ensure this is the most current electronic copy of this document as it is updated and published in electronic format only (hard copies may become out of date).

1.0 The Policy

1.1 Inmind has a duty to protect all clinical, personal and commercial information. A key aspect of this process is the identification and assessment of risks associated with information and the development and implementation of processes to address and mitigate these risks. This document sets out the policies and processes which are to be applied across the group.

The primary requirement for robust and effective information risk management processes is that all employees take responsibility for their implementation. To achieve this, wherever possible and practical, all information assets are identified and individuals are assigned ownership of these assets.

‘Ownership’ of an asset is defined as responsibility for its accuracy, timeliness and completeness commensurate with the significance of the asset. This means that in addition to ensuring that the data is kept in a suitable form, there is an assessment of security and analysis of risks run by the asset owner. This policy aims to address the following issues:

- The identification of risk
- The assessment of risk
- Measures to be put in place to identify, address and document information security issues.

Risk management policy and procedures must be understood as part of the overall Information Governance Framework. The relevant ISO standards are ISO/IEC 27001:2013, and this lists the following areas as being of concern in information risk management:

- Security policy
- Organisation of information security
- Asset management
- Human resource security
- Physical and environmental security
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Compliance

1.2 The Scope

For the purposes of this policy, ‘information’ is anything contained in a hard copy or electronic record which relates to service users, their treatment or any other personal details, or which relates to Inmind employees or contractors, or which relates to Inmind and its operations. This policy also covers the transmission of information by speech or any other method.

Risk management and assessment will apply to threats and risks from all sectors including, but not limited to:

- Deliberate or accidental damage to information assets from internal sources (access, modification, deletion, copying of data and operational code and security information).

- Deliberate attempts to access or damage information assets from external sources (including viruses, hacking, etc.).

- Occurrence of events which may impair or prevent access to information assets or otherwise jeopardize information assets. This includes, but is not limited to:

  - IT hardware and network failure
  - Non-IT events which cause denial of access or service such as power failure, building evacuation
  - Loss of computers.

- Incorrect data. Information systems and records management processes should, wherever possible, contain validation routines to reduce the likelihood of incorrect information being recorded. For critical information, periodic audits should be carried out to ensure accuracy. If any employee identifies incorrect or inaccurate information, or the absence of important information within patient, employment or other corporate records, it is their duty to ensure that this situation is rectified whether by correcting it, reporting it to the person responsible or by instigating actions which will lead to the rectification of the data.

Disclosure of confidential information

In general, confidential information should not be disclosed without authority or consent. A detailed description of the requirements of confidentiality is contained in Inmind’s Confidentiality and Data Protection Policies.

1.4 Definitions

Risk – the chance of something happening, which would have an impact upon objectives. It is measured in terms of likelihood and severity.

Consequence – the outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Information Risk – a risk that relates to the loss, damage, or misuse of information or which threatens the confidentiality, integrity or availability of an information asset, especially information which is personal or confidential in nature.

Likelihood – a qualitative description for probability or frequency.

Risk Assessment – the overall process of risk analysis and risk evaluation.

Risk Management – the culture, processes and structures directed towards the effective management of potential opportunities and adverse effects.

Risk Treatment – selection and implementation of appropriate options for dealing with risk which, conceptually, will involve one or a combination of the following strategies:

- Risk avoidance
- Reduction in the likelihood of occurrence
- Reduction in the consequences of occurrence
- Risk transference
- Risk tolerance / acceptance

Risk Management Process – the systematic application of management policies, procedures and practices to the task of establishing the context and identifying, analysing, evaluating, treating, monitoring and communicating risk.

Information Assets – in general Information Assets will be administration systems or database used to process PID directly or used in any way that has the potential to affect the confidentiality / integrity / availability / legal processing of PID. The following outlines the main examples of Information Assets:

- Databases and data files
- System information and documentation
- Back-up and archive data
- Operations and support procedures
- Audit data
- Applications and system software
- Data encryption utilities
- Development and maintenance tools
- Paper records (including patient care notes and staff records)
- Environmental services necessary for the safe operational of Information Assets (e.g. power and air conditioning)
- Business continuity plans

Information Governance Compliance Framework – an Information Governance compliance monitoring and management tool.

2.0 The Procedure

2.1 Roles and Responsibilities

Accounting Officer

The Chairman is the Accounting Officer and has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level, where information risks are handled in a similar manner to other major risks such as financial, legal and reputational risks.

Inmind's Board

It is the responsibility of Inmind's Board to create a strong information handling culture, which permeates throughout Inmind and informs everyone's approach to performing daily tasks, regardless of position and seniority.

Senior Information Risk Owner (SIRO)

The SIRO acts as an advocate for information risk on the Board and in internal discussions and provides written advice to the Accountable Officer regarding the "information risk".

The Information Security Manager

Reports to the SIRO and is responsible for ensuring that all risk assessments are completed as required and that appropriate reports are prepared for and reviewed by the Information Governance Steering Group. The Information Security Manager also ensures that Information Asset Owners are appropriately trained and that they maintain Information Asset Registers, Risk Assessment documentation and Information Risk Registers in a timely manner.

Information Asset Owners (IAOs) and **Information Asset Administrators (IAAs)** are senior individuals involved in running the relevant business / service areas, for clarity these individuals will be members of the IG Steering Group (ordinarily the Registered Manager):

- understand and address risks to the information assets they 'own'
- provide assurance to the SIRO on the security and use of these assets
- ensure that policies and procedures are followed
- recognise potential or actual security incidents
- ensure that information asset registers are accurate and maintained and kept up-to-date

Information Governance Steering Group

Subject matter experts used to counsel the SIRO on general and specific information risk issues. Due to the size of the company the IG Steering Group will act as a conduit for discussing all information risk issues.

All staff should be aware of information risk management, how to raise risks and incidents, and have responsibility for ensuring that information is kept secure. Secure practices can help:

- avoid unauthorised disclosure, dissemination or access to information
- support appropriate storage, transportation, transfer and disposal of information

2.2 Risk Management

Risk Management is created to:

- Protect Inmind, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes;
- Encourage pro-active rather than re-active risk management;
- Provide assistance to and improve the quality of decision making throughout Inmind;
- Meet legal or statutory requirements; and
- Assist in safeguarding Inmind's information assets.

2.3 Risk Management Culture

Inmind create a culture of risk management of risk by:

- Implementation of an information asset ownership regime;
- Ensuring that Information Asset owners known and understand their responsibilities;
- Ensure that all employees know and understand their responsibilities with respect to information assets;
- Ensuring that Information Risk Management is regarded throughout Inmind as a strategic issue;
- Ensure that all aspects of Information Risk are identified and assessed and that the policy and risk assessment processes are implemented properly;
- Create and own Risk Assessment framework to be applied to all information assets;
- Ensure periodic testing and review of Information Risk including:

  - Business Continuity Plan development and maintenance
  - Specific Information Asset Risk Assessments and development of the associated action plans.
  - Audit of risk related procedures and review of Events in the Information Risk Register.

Furthermore, Inmind keep the Information Governance Steering Group informed regarding the status of information risk by means of summary reporting from the Information Risk Register and reporting on periodic testing.

2.4 Information Asset Ownership

Inmind will implement its risk management policy by instituting Information Asset Ownership. This will be done by the following means:

- Creation and maintenance of an inventory of Information Assets.
- Allocation of information assets to appropriate owners, responsible for the quality, maintenance, creation and deletion of appropriate procedures associated with the information asset.
- In association with the Information Security Manager, Information Asset Owners will create and maintain a Risk Assessment for the Information Assets

2.5 Information Asset Framework

The Risk Assessment framework sets out for each identified information asset the following:

- **Risk Identification:** This sets out the risks which exist for the information asset. They may include matters such as accidental or deliberate inappropriate exposure of information (for patient data); loss of service (for a system); loss of a laptop containing commercial information; virus infection.

- **Risk analysis:** This involves assessment of what harm would occur if the situation identified occurred. This will involve consideration of a range of factors from patient care to prosecution. Some risks may have minimal consequences.

- **Risk evaluation:** This is an assessment of the combined effect of the consequences of occurrence with the likelihood of occurrence. An overall evaluation will be of the form of an assessment of level of risk (Low, Slight, Moderate, Severe and Catastrophic). See Appendix 1 for typical assessment criteria.

Risk treatment (Action Planning): Each risk will be allocated an appropriate treatment. An Action Plan is then required for each item. This should be created, monitored and reviewed on a regular basis. Where appropriate rehearsals or ‘dry runs’ should be carried out on a regular basis and the results investigated and improvements put into place. The options available are:

- Accept and monitor the risk
- Avoid the risk
- Reduce the likelihood of the risk occurring – e.g. through contractual agreement, audit and compliance, preventative actions, supervision, training.

  - Reduce the consequences of the risk occurring – e.g. through contingency planning, minimizing exposure to the risk, public relations, relocation of activity
  - Transfer of risk – through contractual arrangements or 'insurance'.

- **Risk review**: Information risks should be reviewed periodically on a regular basis or as needed. Any risk should be reviewed at least annually. Any new risks should be added to the framework and notified to the SIRO.

2.6 Risk Register and Log

- Any incident which has or could lead to a breach of information security or normal business processing should be recorded using the Incident Report and an entry made in the Incident Log.

- The Log should be reviewed on regular basis by the Information Security Manager to determine whether any changes to Information Governance framework are required.

- The Information Security Manager and Information Asset Owner should ensure that any events are logged and closed in a proper manner.

See Appendix 2 for information on the Risk Assessment Matrix.

2.7 Risk Mitigation

Information risk mitigation must:

- Be commensurate with the level of risk – it does need to remove the risk entirely
- Be kept simple so that it is manageable and can be communicated to staff
- Include monitoring and reporting on the ongoing level of information governance / confidentiality / information security breaches, so that the effectiveness of the protection being achieved can be assessed
- Risk must be assessed in terms of the general level of harm that could be reasonably caused if data were to become compromised or unavailable
- Take the form of a wide range of controls directed at reducing the likelihood of an information (confidentiality, integrity or availability) failure and reduce the amount of harm a failure could cause
- Control and reduce the likelihood and amount of harm of a failure and enhance overall mitigation
- Apply 'good practice' controls, which are easy for staff to understand and apply
- Be supplemented with customised controls for specific high risk circumstances

Appendix 1

Risk Scoring Categories

Category	Impact on Employee / User / Patient / Visitor	Cost to Inmind	Reputation / Publicity	Litigation / Enforcement Action	Quality / Performance
Low	Minor inconvenience	< £3,000	Within Inmind	None / Minor civil action	Minor non-compliance
Slight	Significant system disruption	£3,000 – 20,000	Local press	Civil action	Failure to meet internal standard Failure of test of Business Continuity
Moderate	Major system disruption Loss of laptop – No clinical data or encrypted data	£20,000 – 100,000	National media < 3days coverage Internal enquiry	Minor Criminal prosecution – low level employee	Repeated failure to meet internal standard
Severe	Permanent loss of clinical data Loss of laptop – Clinical data unencrypted	£100,000 - £1,000,000	National media > 3 days coverage MP concern External enquiry	Criminal prosecution – Senior employee	Failure under Data Protection Act Failure under Caldicott guidelines
Catastrophic	Major fraud	£1,000,000	Public enquiry Loss of operational licences BIS or similar investigation	Criminal prosecution - Board	Major failure under Data Protection Act Major failure under Caldicott guidelines

Appendix 2

RISK ASSESSMENT MATRIX

Risk Priority
Key: Red – High Risk Amber – Medium Risk Green – Low Risk

RISK MATRIX					
5 - Very High	A	A/R	R	R	R
4 – High	A	A	A/R	R	R
3 – Medium	A/G	A	A	A/R	A/R
2 – Low	G	A/G	A/G	A	A
1 – Very Low	G	G	G	G	G
Impact	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost Certain
	Likelihood				

Risk Matrix – Likelihood

Likelihood rating	Description
5 Almost Certain	this type of event will happen frequently
4 Likely	this type of event will happen, but it's not a persistent concern
3 Possible	this type of event may well happen (e.g. 50/50 chance)
2 Unlikely	unlikely that this type of event will happen
1 Rare	cannot believe that an event of this type will occur in the foreseeable future

Appendix 3

Equality Impact Assessment for this policy

Protected Characteristic (domain)	Area of conflict	Resolution
Age	Nil	N/A
Disability	Nil	N/A
Gender Reassignment	Nil	N/A
Pregnancy & Maternity	Nil	N/A
Race	Nil	N/A
Religion or Belief	Nil	N/A
Sex	Nil	N/A
Sexual Orientation	Nil	N/A
Marriage and Civil Partnership	Nil	N/A

All relevant persons are required to comply with this policy and must demonstrate sensitivity and competence in relation to diversity in race, faith, age, gender, disability and sexual orientation. If you feel you are disadvantaged by this policy, please contact the Registered Manager and the service will actively respond to the enquiry.