

GMSS Information Risk Policy

Review Date: October 2019



Greater Manchester Shared Services

Hosted by NHS Oldham CCG
on behalf of the Greater Manchester CCGs

Best Care • Best Health • Best Value

Programme:	Greater Manchester Shared Services
Filename:	I:\GMSS\GDPR\POLICIES
Author:	IG Team
Version:	2.0
Date Released:	December 2017
Purpose of this document:	This document outlines the Information Risk Policy

Document Location

Copies of this document can be obtained from|:

Name:	Corporate Services Office
Address:	Greater Manchester Shared Services Ellen House Waddington Street Oldham OL9 6EE
Telephone:	0161 212 4186

Revision History

Revision date	Revision by	Summary of changes	Version
November 2016	GMSS IG Group	Recommend approval by the IG Group	0.1
January 2017	FPG	Recommend approval after some amendments	0.1
January 2017	SMT	Amendments needed	0.1
August 2017	IG Group	Amendments to accommodate GDPR	1.1

Approvals

Name	Role	Date	Version
K Rigden	SMT	February 2017	1.0
IG Group		December 2017	2.0

Distribution

Name	Role	Date	Version
Saved in Policy Folder		December 2017	2.0
Updated Policy tracker		December 2017	2.0

GMSS Publication Scheme		December 2017	2.0
Shared in Bulletin		January 2018	2.0

DOCUMENT STATUS:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled

Contents

1. Assurance Statement	5
2. Introduction, Scope and Purpose.....	5
3. Communication/Dissemination	5
4. Definitions.....	6
5. Duties and Responsibilities.....	6
6. Policy Detail	7
7. References	9
8. Appendix A – Information Asset	11
9. Appendix B – Risk Assessment Template	Error! Bookmark not defined.

1. Assurance Statement

This policy lays the framework for a formal information risk management programme in Greater Manchester Shared Services (GMSS) by explicitly establishing responsibility for information risk identification and analysis, planning for information risk mitigation, information risk management and its oversight.

GMSS and their management team are required to assure the formal introduction and embedding of information risk management into key controls and approval processes of all major business processes and functions of the organisation.

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of GMSS continuously manage information risk.

It should be noted that this policy complements and works on the same principle outlined in GMSS's Risk Management Frameworks. This policy specifically relates to risk associated with management information, records and data.

2. Introduction, Scope and Purpose

Information risk is a factor that exists in all areas where information of a personal or confidential nature are used and managed

This policy sets out the requirements placed on all staff in the use and management of information and the risks associated with using such information.

The policy takes key areas from the NHS National Patient Safety Agency "Risk Matrix for Risk Managers" and works in conjunction with the Risk Management Framework as well as the Information Governance Policy, Data Protection and Confidentiality Policy and Record Management Policy

Information Risk management is a part of Information Governance (IG) and it is acknowledged that information governance, including the management of information risks become part of the culture of the organisation, ensuring that staff are aware of, and work to, good IG (and therefore information risk) practices.

Purpose - The purpose of this policy is to provide a consistent way of managing information risk in the organisation allowing the information to be managed in a way that highlights when information may be at a significantly high risk, thereby providing a layer of protection for patients, staff and the organisation. The highlighting of risk will then allow risks to be properly addressed and the risk managed in a way that is most suitable.

There are legal and statutory requirements for the protection of information, both personal and confidential, and this policy sets out how the risks to that information will be managed in compliance with those requirements.

Scope - This policy covers all organisational areas including information risk associated with third party provision of services.

3. Communication/Dissemination

This policy will be made available to all staff. The policy will be published, as a minimum, in the following ways:

- Publication in the relevant policy section of the organisation's Internet,
- Publication in the Publication Scheme (Freedom of Information)

4. Definitions

Definitions used in this Policy and risk management include:

- **Risk:** The chance (probability) of something happening which will impact in an adverse way something of value. This may be damage to information or reputation or may involve injury or liability. In this context risk is measured as a product of consequence" x "likelihood" which are given numerical values as will be explained as below
- **Consequence:** The result of a risk becoming a reality. For example injury, financial loss, damage. There may be more than one consequence for each risk occurring.
- **Likelihood:** What is the possibility of the risk actually occurring(becoming an issue)
- **Assessment:** The process of identifying and evaluating risks
- **Management:** In this context, the management of the risk processes within an organisation.
- **Treatment:** Ways of mitigating risk. General risks mitigation involves avoidance, reduction of the risk (consequence, likelihood or both), transfer the risk to someone else, accept the risk.

Please refer to the Risk Management Framework for more definitions

5. Duties and Responsibilities

Managing Director

The Managing Director has overall responsibility for the organisation's risk management. Operational responsibility may be delegated to a Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

The SIRO will have lead responsibility for information risk and information risk management within the organisation. This position will be an Executive Board Member

Data Protection Officer (DPO)

The DPO's role is to inform and advise GMSS and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Information Governance Group

This group is responsible for the monitoring and assurances concerning information risk management. Operational responsibility is delegated to the Information Governance Team, of which the Deputy SIRO and Caldicott Guardian are informed.

Information Asset Owners

An Information Asset Owner (IAO) is responsible for the information managed within one or more

information assets (system, process, files etc.). Part of the function of the IAO is to be aware of and manage local risks to information and where the risk is sufficiently high (see below) report the risk to their SIRO.

Information Risk Supporting Roles

In addition to the Information Asset Owners (IAO) and Information Asset Administrators (IAA) roles defined above, Information Risk supporting structure for the SIRO will consist of Deputy SIRO, Caldicott Guardian, Information Governance Team and other appropriate Officers - agencies as required

Staff

All staff will be aware of information risk management and understand the need for information risk to be a part of the culture of the organisation.

6. Policy Detail

The information risk management process will take place using the NHS "5x5 Risk Matrix" as detailed in the NPSA's "Risk Matrix for Risk Managers". This document contains guidance on how to interpret the scores that will be attributed to risks and provide the basis for information risk reporting to SMT. Information on the matrix relating to this policy may be found in Appendix A.

Privacy Impact Assessments (PIA) - Risks to personal and confidential information that arise as a consequence of changes to systems (projects) will be identified via the completion of a PIA. This will be a questionnaire completed by the project manager or other suitable project member who will be considered by IG and where necessary a report on information risks and actions to be taken will be produced. This will be managed as part of the overall project with IG oversight at all times.

The PIA processes and proformas are available from the Information Governance Team or on the internet.

Local Information Risks

It is the IAO's responsibility to be aware of, and formally record, information risks to the assets which they manage. Many risks will be managed and resolved locally, but higher risks will need to be managed via IG in order to ensure the organisation is aware of those risks and can be assured that active management of them is in place.

It is necessary to ensure a consistent approach to risk assessment and risk priority ratings so that all risks can be initially prioritised and ultimately agreed by the appropriate governance group. The board will be informed of significant risks.

To ensure this consistency and assurance to each of GMSS's Committees that GMSS are managing their risks adequately and they use the following tools:

- Risk Management process and action plans
- Risk Analysis and recording
- Risk Consequence Table
- Risk Rating Matrix
- Specific Risk Assessment Form
- Risk Register Template

Management of Information Risks

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Please refer to Appendix B for more information on Information Assets

Information assets have recognisable and manageable value, risk, content and lifecycles. All breaches and incidents regarding Information asset should be reported using GMSS online incident reporting system – DATIX.

Information risks will be managed locally, unless the risk score attributed to an individual risk is 15 or greater. The Risk Matrix and scoring is available for reference in the Risk Management Framework (RMF).

The treatment options for information risk are:

- **Avoid:** not proceeding with activity likely to generate the risk
- **Reduce:** reducing or controlling the likelihood of consequences of the occurrence
- **Transfer:** arranging for another party to bear or share some part of the risk, through contracts, partnerships, joint ventures, etc.
- **Accept:** some risks may be minimal and retention acceptable

Risks will be managed via a standard risk log format that will enable risks managed consistently across organisations ensuring a high quality level of support, where it is necessary.

Information risks relating to sensitive personal data and confidential information in hard and soft format will be systematically evaluated throughout the Information Governance team and the Risk Manager and action taken on a risk assessed basis. All significant breaches will be included the IG report which will link in with Datix Process.

All sensitive personal data will be handled as 'confidential information', kept securely in locked cabinets and via appropriate permissions on the network. It will be made available on a need-to-know basis and advice provided to staff as appropriate.

Policies are in place to support information risk management including information security, data protection, confidentiality and Record Management on GMSS's internet.

All internal staff as well as third parties, contractors, agency staff will be required to sign and follow GMSS Confidentiality clauses.

PIA's will be carried out as necessary where new systems have the potential to negatively impact on personal privacy. PIA Proforma will be available on GMSS's internet.

Escalation of Risks

Please refer to GMSS's Risk Management Framework for more information on escalation of Risk. The IAO will be responsible for managing the risks; reporting and ensuring that suitable mitigations are put in place either locally or with support from information governance/risk management.

The SIRO is responsible for ensuring that policy is followed and to be aware of all risks.

The Risk Register with terms of reference covering the management of risks will be responsible for organisational risk logs, where high risks are to be recorded. This group is also responsible for escalating high risks to the board and ensuring that where relevant they are admitted to the

corporate risk register.

Proactive planning will be undertaken for investigating and identifying risks through different scenarios, regular policy reviews, ICO recommendations and assessment of sources of legal weight and admissibility of evidence for reducing risks.

Information Risk Management Training

NHS Digital – Training Workbooks are used for Additional IG Training as part of your job role. Please see the IG TNA for further details.

The Training Workbooks can be obtained by the IG Training on 0161 2126166 or

All staff must complete all Mandatory and IG TNA role specific IG Training.

Information Asset Register

GMSS will establish a programme to ensure that their Information Assets (IA's) are identified and assigned to an IAO. The SIRO will oversee a review of the organisation's asset register to ensure it is kept up to date, complete and robust.

All critical IA's will be identified and included within the Information Asset Register (IAR), together with details of business criticality, the IAO, the Information Asset Administrator (IAA) and risk reviews to be carried out. In order to improve the usability and maintainability, the Information Asset register may be organised by service, rather than by location. Refer to Appendix B for more information on Information Assets.

Support and Monitoring

Support will be provided to staff in assessing risk and managing their local processes by the IG and Risk teams, locally. Where necessary these teams will seek further advice on behalf of the department making the query.

This policy will be reviewed every two years, and in accordance with the following on an as and when required basis:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- Changes to organisational infrastructure.

7. References

Risk Matrix for Risk Managers" at www.npsa.nhs.uk.
NHS Information Risk Management — HSCIC

Information Commissioner's Officer at www.ico.org.uk

What security measures should I take to protect the personal data I hold? By ICO
Notification of data security breaches to the Information Commissioner's Office by ICO.

8. IG Related Documents

A set of procedural documents will be made available via GMSS Internet.

- Information Governance Framework
- Data Protection & Confidentiality
- Confidentiality Audit Policy
- Information Governance & Cyber Incident Reporting Policy
- Secure Transfer of Information Policy
- Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- Subject Access Procedure
- Registration Authority (Smart Card) Procedure
- Information Governance Staff Handbook

This list is not exhaustive

9. Appendix A – Information Asset

Assessing whether something is an information asset

To assess whether something is an information asset, task the following questions:

- Does the information have a value to GMSS? How useful is it? Will it cost money to reacquire? Would there be legal, reputational or financial repercussions if you couldn't produce it on request? Would it have an effect on operational efficiency if this information could not be accessed easily? Would there be consequences of not having it?
- Is there a risk associated with the information? Is there a risk of losing it? A risk that it is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?
- Does the group of information have a specific content? Is there an understanding of what the information is and what it is for? Does it match the purpose associated with the information?
- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Examples of typical assets include:

Personal Information Content	Software
<ul style="list-style-type: none"> • Databases and data files • Back-up and archive data • Audit data • Paper records (patient case notes and staff records) • Paper reports 	<ul style="list-style-type: none"> • Applications and System Software • Data encryption utilities • Development and Maintenance tools
Other Information Content	Hardware
<ul style="list-style-type: none"> • Databases and data files • Back-up and archive data • Audit data • Paper records and reports 	<ul style="list-style-type: none"> • Computing hardware including PCs, • Laptops, PDA, communications devices e.g. blackberry and removable media. <p>e.g. blackberry and removable media</p>
System/Process Documentation	Miscellaneous
<ul style="list-style-type: none"> • System information and Documentation • Operations and support procedures • Manuals and training materials 	<ul style="list-style-type: none"> • Environmental services e.g. power and air-conditioning • People skills and experience Shared service including Networks and • Printers • Computer rooms and equipment

- Contracts and agreements
- Business continuity plans

- Records libraries



Greater Manchester Shared Services

Information Asset Risk Assessment

Section 1: General Information

Asset Register No.:	<input type="text"/>
Information Asset / System Name:	<input type="text"/>
Description:	<input type="text"/>
Key Asset Status:	<input type="text"/>
Assessment Date:	<input type="text"/>
Undertaken By:	<input type="text"/>
Reviewed By:	<input type="text"/>
IAO:	<input type="text"/>
IAA:	<input type="text"/>
Composite Risk Score:	<input type="text" value="0"/>
Risk Re-Review Period:	<input type="text"/>

Residual Risk Score:

