Greater Manchester Shared Services

GMSS Information Governance Policy

Review Date: October 2018

Programme:	Greater Manchester Shared Services
Filename:	I:GMSS/GDPR/Policies and Procedures
Author:	GMSS IG Team
Version:	1.0
Date Released:	October 2017
Purpose of this document:	This document outlines the IG 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
Sept 2017	GMSS IG Team	Split the IG Strategy & Policy into the IG Policy and IG Framework documents	0.1

Approvals

Name	Role	Date	Version
IG Group		18th October 2017	1.0
SMT		14th November 2017	1.0

Distribution

Name	Role	Date	Version
Saved in policy folder		October 2017	1.0
Updated Policy Tracker		November 2017	1.0

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

1.0 Introduction and Aims

1.1 Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

1.2 Information Governance sits alongside Clinical Governance, Research Governance and Corporate Governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal information. It also provides a consistent way for employees to deal with the many different information handling requirements.

1.3 This document sets out minimum policy standards and common policy directions across Greater Manchester Shared Services (henceforth referred to as "GMSS") for confidentiality, integrity and availability of information (Information Governance). The policy is intended to cover the overlapping areas of:

- Confidentiality (with regard to 'common law');
- Current Data Protection Act and the General Data Protection Regulation (GDPR);
- Information Security;
- FOI Policy (refer to this policy for further information)

1.4 The aims of this document are to ensure that information is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- available as and when required;
- used effectively and ethically;
- shared and disclosed appropriately and lawfully;

The policy provides a guide to Information governance but advice should always be sought from your manager or the GMSS IG Team before disclosing data

2.0 Scope

2.1 This policy applies to those members of staff who are directly employed by GMSS and for whom GMSS has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of GMSS. Further, this policy applies to all third parties and others authorised to undertake work on behalf of GMSS. The collective term 'staff' is used throughout this policy to mean all these groups.

2.2 This policy applies to all forms of information, including but not limited to:

- paper and electronic filing systems;
- communications, including those sent by post, electronic
- mail, text messaging;
- information that is stored in and/or processed by
- information systems including servers, personal computers (PCs), any other mobile device;

- information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internal or externally to a third party

3.0 Principles: Confidentiality & Data Protection

3.0.1 GMSS is committed to the delivery of a first class l service to its customers. This includes ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information where appropriate/necessary;
- gain trust in the way GMSS handles information;
- understand their rights to access information held about them.

3.1 The Duty of Confidence

3.1.1 All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality.

3.1.2 Everyone working for the NHS that handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his/her employer.

3.1.3 The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

3.1.4 Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff.

3.1.5 Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff are likely to include those who are not involved in either the clinical care of the service user or the associated administration processes.

3.1.6 No personal information, given or received in confidence, may be passed unless there is a legal duty to do so. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).

3.1.7 No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information unless there is a legal duty to do so.

3.1.8 Service users are entitled to object to the use of their personal health data for purposes other than their immediate care.

3.1.9 The duty of confidentiality owed to a deceased service user must be viewed as being consistent with the rights of living individuals.

3.2 What is Personal Information?

3.2.1 Personal identifiable information, or personal data is strictly defined in the General Data Protection Regulation to which all organisations processing personal information and all staff within those organisations, must adhere to.

3.2.2 Personal Information is now commonly known as Personal Confidential Data (PCD). Personal confidential data is data in which individuals are clearly identified, or there is a high risk of individuals being identified. This includes patient identifiable data, such as:

- NHS number
- Name
- Address
- Postcode
- Date of Birth
- Date of Death
- Photos
- Web IDs

3.2.3 Personal confidential data also includes sensitive data which may include items such as:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health or data concerning a natural person's sex life or sexual orientation.
- The processing of these characteristics is prohibited unless certain conditions are met

3.2.4 Information that falls into any of the categories above must be regarded as confidential, and must not be used unless absolutely necessary and where there is a legal basis to do so.

3.2.5 If an individual is unclear if information should be classified as PCD, they must discuss the issue with their line manager or the GMSS Information Governance Team, who will offer advice.

3.3 Disclosing Information

3.3.1 A Guide to Confidentiality in Health and Social Care and GMSS IG Handbook provides advice on using and disclosing confidential service user information and has models for confidentiality decisions. All staff must adhere to this guidance.

3.3.2 If a staff member wishes to disclose Personal information then advice should be sought from GMSS IG Team

3.3.3 Consent of the individual is usually required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

3.3.4 Under common law, personal information may be disclosed without consent for example:

- in order to prevent abuse or serious harm to others
- where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

3.3.5 All individuals must:

- exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- ensure the physical security of all confidential documents , including storage of files on PCs.

3.3.6 In most circumstances, police should only be given access to personal records with the patients' consent or a court order. Please speak to the Information Governance Team for guidance on the process. Information should only be released to the police after first consulting your line manager and the Caldicott Guardian/ Deputy Caldicott Guardian

3.3.7 Any individual has the right to request to see the information an organisation holds about them. This is called a Subject Access request. Any individual making such a request must do so in writing. GMSS has a Subject Access Procedure in place which all staff must familiarise themselves with and adhere too.

3.3.8 Staff should never give information to a person claiming to be the friend, relative or representative of a member of staff/patient/service user. Unless appropriate checks have taken place to ensure that person has a legitimate reason for access. Action of this kind may be viewed as a breach of confidentiality and may lead to an investigation; this may result in disciplinary action being taken.

3.4 Personnel Information

3.4.1 In keeping with good Human Resources practice, GMSS retains and processes personal data on its employees. In addition, GMSS may from time to time, retain and process "sensitive personal data" as defined by GDPR for example, in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring, for the prevention of fraud or other illegal activities.

3.4.2 GMSS may process such data and such data may be legitimately disclosed to appropriate employees and GMSS professional advisors, in accordance with the principles of the current Data Protection Act and GDPR.

3.4.3 GMSS takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with GMSS HR Lead.

4.0 Principles: Information Security

4.0.1 The information held and managed by GMSS is an asset that all staff have a duty and responsibility to protect. The availability of complete and accurate information is essential to GMSS functioning in an efficient manner.

4.1 Information Security – Requirements

4.1.1 GMSS will implement technical and operational standards, policies and processes that align with prevailing standards such as ISO27001 (Information Security Management).

4.1.2 The requirements of policy, processes and procedures will be incorporated into GMSS operational procedures and contractual agreements.

4.1.3 Information stored and processed by GMSS will be appropriate to business requirements and no information will be stored or processed unnecessarily.

4.1.4 GMSS will develop, implement, maintain and test where required, local business continuity plans. Such plans will be a contractual obligation of any relevant supplier.

4.1.5 GMSS will ensure that appropriate controls are applied to all types of communication, internal and external, to ensure the communication is secure, appropriate and reaches the intended recipient.

4.1.6 GMSS will undertake risk assessments to identify, quantify and prioritise information security risks in accordance with GMSS Information Risk Policy. Controls will be selected and implemented to mitigate the risks identified.

4.1.7 All breaches of information security, actual or suspected will be reported and suitably investigated in line with information incident management procedures which will provide guidance on what constitutes an information incident.

4.2 Asset Management

4.2.1 GMSS information (electronic and hardcopy), software, computer and communication equipment, will be accounted for and have an owner.

4.2.2 GMSS will implement controls that will ensure its assets are appropriately protected.

4.2.3 Owners of such assets owners will be responsible for the maintenance and protection of assets they are assigned.

4.3 Information Systems Acquisition, Development and Maintenance

4.3.1 Information security requirements will be defined and communicated during the development of business requirements for new systems or changes to existing systems.

4.3.2 Controls to mitigate risks identified during design, procurement, development, testing and deployment will be implemented.

5.0 Accountability, Responsibilities and Training

5.1 The Managing Director has overall responsibility for Information Governance within GMSS. As Accountable Officer, they are responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

5.2 GMSS has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements

5.3 Overall responsibility for the Information Governance Policy lies with the Head of Integrated Governance who has delegated responsibility for managing the development and implementation Information Governance within GMSS.

5.4 Further responsibilities will be delegated to:

5.5 Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of the patient and service user information and enabling appropriate information sharing.. The Deputy Caldicott Guardian supports this work

5.6 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for identifying and managing the information risks to GMSS. This includes oversight of the organisation's information security / governance incident reporting and response arrangements and the Registration Authority business process. The Deputy SIRO supports the work of the SIRO

5.7 The Data Protection Officer (DPO)

The DPO is required as part of the changes to the Data Protection Act which will now be the General Data Protection Regulation. 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).

5.8 Information Asset Owners (IAO)

IAO's are required to know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset. An IAO must be aware of access to an asset, checking that its compliant and understand and address any risks.

5.9 Information Governance Team

GMSS Information Governance Team are responsible for supporting the organisation and staff to ensure information is processed legally, securely, efficiently and effectively.

5.10 Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their group or directorate, including any temporary or contract staff.

5.11 It is the responsibility of all staff (including any temporary or contract staff) covered by the scope of this policy, to adhere to and keep up to date with any changes to this policy.

5.12 Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods, for example, team meetings; and staff Intranet.

5.13 All staff (including any temporary or contract staff) must ensure that they read and follow the user requirements within GMSS Information Governance user handbook which supports GMSS Information Governance policies.

5.14 All staff (including any temporary or contract staff) are mandated to undertake IG Training as per the Training Needs Analysis.

5.15 Where relevant further training and education will be required of staff, the staff will be informed via the Information Governance Training Needs Analysis.

5.16 GMSS will monitor and co-ordinate the implementation and ongoing management of the Information Governance framework and IG Toolkit requirements via the IG Group, GMSS Caldicott Guardian and the SIRO.

5.17 The IG Group will report to the GMSS Senior Management Team. This will be the route of escalation for issues.

5.18 Failure to comply with any part of this policy could result in disciplinary and/or legal action.

6.0 Monitoring and Review

6.1 This policy will be monitored through staff awareness and supporting evidence to the NHS Information Governance Toolkit.

6.2 This Policy will be reviewed on an annual basis, 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.

7.0 Legislation & Acts

Data Protection Act
General Data Protection Regulation
The Common Law Duty of Confidentiality
Confidentiality: NHS Code of Practice (Department of Health)
Caldicott Report 1997
The Public Interest Disclosure Act 1998
Human Rights Act 2000
Regulation of Investigatory Powers Act 2000
Computer Misuse Act 1990
Public Records Act 1958
Caldicott 2 Report
Caldicott 3 Review

8.0 IG Related Documents

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

- 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

8.2 Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via GMSS staff intranet.