Greater Manchester Shared Services

Data Protection and Confidentiality Policy

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

Best Care • Best Health • Best Value

Contents

Document Change History

Date	Ver.	Status	Author	Details of Change
November 2016	0.1	Reviewed from Oldham CCG to fit GMSS	IG Team	Amendments to fit with GMSS

Document Tracking History

Date	Ver.	Person Presenting	Area Receiving	Comments
November 2016	0.1	IG Team	GMSS IG Group	Recommend Approval by the IG Group
January 2017	0.2	G Coxon	FPG	Recommend Approval after some amendments
January 2017	0.3	K Rigden	SMT	Amendments needed

1. Introduction and Aims

The purpose of this Policy is to provide guidance to all Greater Manchester Shared Services (henceforth referred to as "GMSS") employees on Data Protection.

GMSS has a statutory duty to safeguard the confidential information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with GMSS shall misuse any information or allow others to do so.

During the course of their day to day work, many individuals working within or for GMSS will often handle or be exposed to information which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company or other organisation to which this policy applies shall not at any time during the period they work for or provide services to GMSS nor at any time after its termination, disclose confidential information that is held or processed by GMSS.

All staff working in GMSS are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the Data Protection Act 1998 and, for health and other professionals, through their own professions' Codes of Conduct.

GMSS understands the need for the strictest confidentiality in respect of data. This applies to manual and computer records and conversations about service users' treatments. Everyone working for GMSS is under a legal and common law duty to keep service users' information, held in whatever form, confidential.

The Information Commissioners Office (ICO) can impose penalties upon GMSS, and/or GMSS employees if non-compliance occurs.

Confidentiality can only be overridden in exceptional circumstances and with the appropriate justification and be fully documented.

GMSS will ensure 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 necessary;
- gain trust in the way GMSS handles information; and
- understand their rights to access information held about them.

It is the policy of GMSS that all processing of personal information by or on behalf of GMSS, whether as a Data Controller or as a Data Processor for others, shall be in accordance with the requirements of:

- The Data Protection Act (DPA) 1998 and any subsequent amendments and statutory instruments;
- the current Data Protection registration of GMSS;
- GMSS's Policies and Procedures in relation to the protection and use of personal information;
- processing personal information for deceased patients;
- The Access to Health Records Act 1990 and any subsequent amendments and statutory instruments.

The aims of this policy are:

- To safeguard all confidential information within GMSS;
- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to confidentiality across GMSS;
- to ensure all staff are aware of their responsibilities with regards to confidential information;
- to provide all individuals working within GMSS access to the documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them. These include:
    - the common law Duty of Confidentiality;
    - Caldicott principles;
    - Data Protection Act 1998;
    - Freedom of Information Act 2000;
    - Human Rights Act 1998;
    - Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures";
    - The Public Interest Disclosure Act 1998;
    - The Computer Misuse Act 1990.

2. Scope

This policy applies to those members of staff that are directly employed by GMSS and for whom GMSS has legal responsibility, including agency and interim staff. For those staff covered by a letter of authority/honorary contract or work experience the organisations 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.

For the purposes of this policy, confidential information shall include any confidential information relating to GMSS and/or its agents, customers, prospective

customers, suppliers or any other third parties connected with GMSS and in particular shall include, without limitation:

- Service user information;
- ideas/programme plans/forecasts/risks/issues;
- trade secrets;
- business methods and business design;
- finance/budget planning/business cases;
- prices and pricing structures;
- sources of supply and costs of equipment and/or software;
- prospective business opportunities in general;
- computer programs and/or software adapted or used;
- policy advice and strategy;
- corporate or personnel information; and
- contractual and confidential supplier information.

This is irrespective of whether the material is marked as confidential or not.

3. Data Protection Act

The Data Protection Act 1998 (DPA) governs how we collect, store, process and share data. The Act dictates that information should only be disclosed on a need to know basis. The DPA is an Act of Parliament which defines UK law on the processing of data on identifiable living people.

The DPA first came into force on March 1st 2000 and covers all personal data held both manually (on paper) and electronically (on a computer).

The DPA is closely linked to the Freedom of Information and Human Rights Acts. Its intention is to focus on promoting the rights of individuals in respect of their privacy and the right to confidentiality of their data.

Although the Act itself does not mention privacy, it was enacted to bring UK law into line with the EU data protection directive of 1995 which required Member States to protect people's fundamental rights and freedoms, and in particular their right to privacy with respect to the processing of personal data. Anyone holding personal data for any purpose is legally obliged to comply with this Act.

GMSS has registered with the ICO as a data controller. A data controller must comply with the eight principles of the Data Protection Act (please refer to section 4 of this policy). GMSS Information Governance Lead is the Data Protection Officer. GMSS is committed to compliance with the requirements of the Data Protection Act 1998 and will ensure that all GMSS employees and anyone providing a service on behalf of GMSS (directly employed and contractors) who have access to any personal data held by or

behalf of GMSS or Commissioning Support Unit (GMSS), are fully aware of and abide by their duties and responsibilities of the Act.

GMSS may be required by law to collect and use information about people with whom it works, including patients, public, employees, customers and suppliers. This personal information must be handled and managed appropriately however it is collected, recorded and used and whether it is a manual or electronic record.

The Data Protection Act defines eight data protection principles.

4. Data Protection Principles

Data Protection Principle 1 - Personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

There is a requirement to make the general public aware of why the NHS needs information about them, how it is used and whom it may be disclosed to. GMSS is obliged under the DPA and Caldicott to produce a patient information leaflet. In order to meet the requirements of the first principle a clear policy of consent is also needed to ensure the requirements of the first principle is met.

Data Protection Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Only use personal information obtained by GMSS in connection with the business of GMSS and ensure information is not used for any purposes other than originally intended.

Data Protection Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Only obtain the minimum amount of information and do not obtain information which is not needed.

Data Protection Principle 4 - Personal data shall be accurate and, where necessary kept up to date.

Ensure that all information entered either manually or electronically is accurate, and where recorded elsewhere ensure that there are appropriate procedures in place to continually review and update the different sources, to ensure accuracy and version control. Where possible do not hold duplicate copies as this increases the risk of inaccurate information being held.

Data Protection Principle 5 - Personal data processed for any purpose or purposes shall not be kept longer than necessary for that purpose or those purposes.

All records are affected by this principle regardless of the media within which they are held/stored and comprehensive guidance is available in GMSS's Records Management Policy. When disposing of personal information use only the confidential waste destruction process.

Data Protection Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.

Under this principle of the DPA individuals have the following rights:

- Right of Subject Access;
- right to prevent processing likely to cause harm or distress;
- right to prevent processing for the purposes of direct marketing;
- right in relation to automated decision taking;
- right to take action for compensation if the individual suffers damage;
- right to take action to rectify, block or erase inaccurate data
- right to request an assessment from the Information; Commissioner to establish compliance with the DPA.

Data Protection Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Examples of which are:

- Do not allow unauthorised access;
- do not share passwords and ensure you lock your PC screen before moving away;
- do not leave confidential information on your desk/fax or post trays and ensure all paperwork is tidied away when not in use or at the end of the day.

Data Protection Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Countries outside of the EEA do not have the necessary legalisation in place to adequately protect the data covered by the DPA.

5. Roles, Responsibilities and Accountabilities

Managing Director (MD)

Although it is GMSS that is the data controller, the MD has overall accountability for GMSS's compliance with the Data Protection Act (DPA). The development, implementation of, and compliance with this policy is delegated to the Caldicott Guardian/SIRO and designated Data Protection Officer. The MD shall ensure that

GMSS resubmits an annual data protection notification and fee to the Information Commissioners Office.

Caldicott Guardian

The Caldicott Guardian will act as the conscience of GMSS, and oversee all disclosures of patient information with particular attention being paid to extraordinary disclosures.

Senior Information Risk Owner (SIRO)

The SIRO will oversee compliance with the DPA and the development of appropriate policy and procedure. The SIRO will be advised by the nominated Data Protection Officer and supported by the GMSS Information Governance Team. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk

Information Asset Owners (IAOs)/Administrators (IAAs)

Under the responsibility of the SIRO:

- Information Asset Owners (IAOs) will be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
- will ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
- will be responsible for the Information Asset assigned to them;
- will ensure that all personal data can at all times be obtained promptly from the
- Information Asset when required to process a SAR;
- will ensure that personal data held in the Information Asset is maintained in line with GMSSs Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.

Information Governance Supplier, Greater Manchester Shared Services (GMSS) will:

- manage the Information Governance Team to deliver Information Governance for GMSS;
- maintain an awareness of information governance issues within GMSS;
- review and update the information governance policy in line with local and national requirements providing template documents to GMSS;
- ensure that line managers are aware of the requirements of the Information Governance policy.

Line Managers

All line managers have a responsibility to ensure that their staff are compliant with, and working to, all relevant policy and procedure in relation to Data Protection; where a breach of policy/procedure or near miss occurs, line managers will need to comply with GMSS Incident Management processes.

Line managers will ensure that anyone providing a service on behalf of GMSS (directly employed and contractors) completes a confidentiality statement before commencing employment.

The Data Protection and Confidentiality Policy is part of the induction checklist and should be read in conjunction with the following policies and procedures listed in section 16.

All Staff (refers to all GMSS employees including contractor/temporary staff and work place students):

- Should adhere to this policy and all related Information Assets and processes to ensure compliance with the DPA;
- are subject to Data Protection compliance and accountable via personal liability; have a responsibility to inform the IG team of any new use of personal data immediately;
- must maintain an appropriate level of awareness of the DPA and to attend training as appropriate;
- ensure that all personal information is accurate, relevant, up-to-date and used appropriately, for both electronic and manual Information Asset;
- ensure that personal data is not removed from GMSS premises except where specifically required for the execution of legitimate functions of GMSS and, then, only in accordance with appropriate policies;
- ensure that all copies of personal data output, or obtained from the system whether electronic, recorded on paper, microfilm, or any other form, are securely and confidentiality managed and destroyed/erased when they are no longer required for GMSS purposes;
- ensure that the IG Team is advised as soon as possible of any problems or complaints relating to any SAR or unauthorised disclosures/ breaches of confidentiality;
- failure to adhere to this policy and its associated procedures may result in disciplinary action.

6. Conduct

Individuals shall not be restrained from using or disclosing any confidential information which:

- They are authorised to use or disclose by GMSS and/or;

- has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure of an individual and/or;
- has entered the public domain by an authorised disclosure for an authorised purpose by the individual or anyone else employed or engaged by GMSS and/or;
- they are required to disclose by law; and/or;
- they are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regards to the provisions of that Act.

All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- ensure the physical security of all confidential documents and/or media, including storage of files on PCs. Confidential information must never be unattended and should be secure when not in use;
- use password protection and not disclose passwords to anyone including work colleagues;
- have regards to the provisions of that Act.

All individuals will be required to comply with this policy whilst working within GMSS and therefore for as long as the information remains confidential information. It is only when the information has entered the public domain that the information can no longer be classed as confidential.

If an individual is unclear if information should be classed as confidential, they must discuss the issue with their line manager who will offer advice.

7. The Duty of Confidence

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

Everyone working for or with NHS/CCG records who 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.

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

Service users expect that information given to them by 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. 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 includes those who are not involved in either the clinical care of the service user or the associated administration processes.

No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).

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.

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

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

8. Personal, Confidential and Sensitive Information

Personal data is any data which relates to a living individual who can be identified by that data or from that data in conjunction with other information which the data controller is in, or is likely to come into possession of.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance

number. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary.

Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.

Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.

Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information (as defined by the Data Protection Act 1998 - DPA) regarding race, health, sexuality, etc.

Confidential information may be known, or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

Sensitive/confidential data under the terms of the DPA includes but is not restricted to:

- Demographics, e.g. Name, address, date of birth;
- information about a person's racial or ethnic origin;
- political opinions;
- gender;
- religion and belief;
- membership of a trade union;
- sexual life;
- criminal convictions or charges;
- Any other information which may identify an individual.

9. Subject Access Request

A Subject Access Request, commonly referred to as a SAR, is a request from a data subject to see a copy of, personal information that is held about them as an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by GMSS, both in electronic and paper files, this is known as a Subject Access Request (SAR).

Any individual is entitled to:

- Know what information is held about them and why;
- gain access to it regardless of the media which it is held;
- have their information kept up to date;

- require GMSS to rectify/block, erase or destroy inaccurate information;
- not have processed confidential information about them likely to cause damage or distress;
- not have processed confidential information about them for the purposes of direct marketing.

In most cases GMSS will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent may be needed. It may be a condition of patients, and employment of staff, that they agree to GMSS processing of specific classes of personal information.

GMSS may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety, or comply with the requirements of other legislation.

10. Freedom of Information

The Freedom of Information Act 2000 widens the scope of the Data Protection Act and also makes provision for personal data to be disclosed to third parties providing none of the DPA Principles are breached. Information generally will not be disclosed if to do so would be regarded as a breach of confidentiality or if it would cause distress to the data subject.

This Act allows public access to information held by Public Authorities. Public authorities include government departments, local authorities, the NHS, state schools and police forces. However, the Act does not necessarily include every organisation that receives public money, e.g. it does not cover some charities that receive grants and certain private sector organisations that perform public functions.

The Act does not give people access to their own personal data (information about themselves) such as health records or credit reference file. If a member of the public wants to see information that a public authority holds about them then they should make a Subject Access Request (SAR).

11. Disclosing Information

GMSS must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances the Police. All staff and individuals providing a service on behalf of GMSS should exercise caution when asked to disclose personal data held on another individual to a third party. Where an individual is unsure as to the legitimacy of disclosing information, the Line Manager or Data Protection Officer should always be consulted.

There may be times when personal data may be legitimately be disclosed, for example where:

- The individual has given their consent for information about them to be disclosed;
- the disclosure is in the legitimate interests of the provision of healthcare (e.g. if members of staff require the information to enable them to perform their jobs adequately or if there are justifiable patient safety concerns);
- GMSS is legally obliged to disclose the data.

The NHS Confidentiality: Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff should adhere to this guidance.

Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.

GMSS will inform service users, staff and any other data subjects why, how and for what purpose personal information is collected, recorded and processed.

Consent of the data subject will be 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.

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

- In order to prevent serious harm;
- 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.

Where information is required by the policeGMSS staff should consult GMSS Information Governance Lead.

12. Human Resources (HR) and Personnel Information

In keeping with good HR 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 the DPA for example in relation to sickness and occupational health records, performance reviews, and equal opportunities monitoring for the prevention of fraud or other illegal activities.

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 is or may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the HR department.

13. Training and Awareness

The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of the DPA and their IG obligations and this will be carried out by regular mandatory Information Governance training sessions. Any new staff members (including temporary, contractors) will be required to complete Information Governance as part of their induction.

Information Governance training is required to be undertaken by all GMSS employees and those providing a service to GMSS. All NHS staff are mandated to undertake annual Information Governance training.

Where staff have specific Information Governance roles within GMSS i.e. Caldicott Guardian, SIRO, etc. Additional Information Governance training will be required. Additional training will be made available to all persons, where it is required. For further guidance refer to the Training Needs and Analysis (TNA) Document.

To maintain high staff awareness GMSS will direct staff to a number of sources:

- Policy/strategy and procedure;
- Manuals;
- line manager;
- specific training courses;
- other communication methods, for example, team meetings; and staff Intranet.

14. Disciplinary

No employee shall knowingly misuse any information or allow others to do so.

Users must not access records/information that they have no legitimate reason to view, this includes records about themselves their family, friends, neighbours, acquaintances. If there is not a legitimate reason to access information users must not browse and should remember all transactions are auditable.

If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and/or to GMSS Information Governance Lead.

Breaches of Data Protection and Confidentiality are a serious matter and a breach of could result in dismissal and/ or prosecution.

15. Monitoring and Review

GMSS will undertake or commission assessments and audits of its framework, policies and procedures to monitor compliance and make improvements where identified.

This policy will be reviewed on a yearly basis, and in accordance with the following on an as and when required basis if the following occurs:

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

Where there are no significant alterations required, this Policy shall remain for a period of no longer than three years of the ratification date.

16. Legislation and Related Documents

Legal Acts:

- Data Protection Act 1998;
- Human Rights Act;
- Freedom of Information Act 2000;
- Thefts Act (1968 and 1978);
- Police and Criminal Evidence Act 1984 (PACE);
- Copyright, Designs and Patents Act (1988);
- Computer Misuse Act (1990);
- Trademarks Act (1994);
- Terrorism Act (2000);
- Proceeds of Crime Act (2002);
- Money Laundering Regulations (2007);
- Criminal Justice and Immigration Act (2008);
- Environmental Information Regulations;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2006 and;
- Human Rights Act 1998.

Supporting Documents

- NHS Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2010;
- NHS Information Risk Management;

- Records Management Code of Practice for Health and Social Care 2016
- The Information Governance Toolkit.
- Caldicott 2

17. Relevant Policies and Procedures

The following policies and procedures should be read in conjunction with this policy:

- Information Governance Policy;
- Records Management Policy;
- Information Risk Policy;
- Freedom of Information Policy;
- Acceptable Use Policy;
- Confidentiality Code of Conduct for Staff;
- Secure Transfers of Information Procedure
- Subject Access Procedure