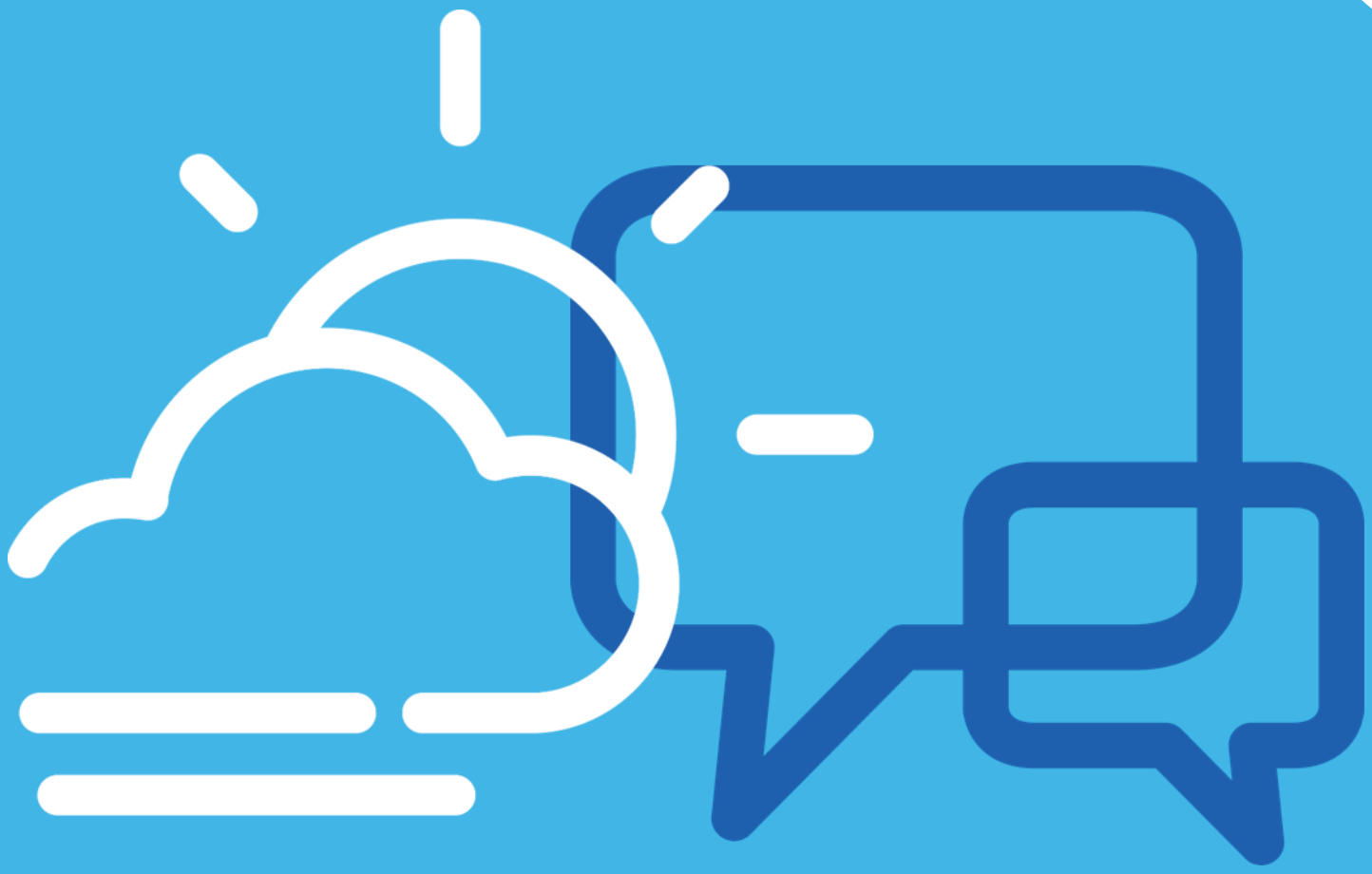
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Information Sharing Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Information Sharing Policy**
Executive Summary:	To ensure the safe sharing of information between organisations for the continuation of seamless care.
Executive Lead:	Director of Finance, Capital and IM&T
Document Author:	Deborah Tonkin (Information Governance Manager) Tel: 0161 358 1573 Email: Deborah.Tonkin@gmmh.nhs.uk
Document Purpose:	Policy
Target Audience:	All Staff
Additional Circulation List:	All staff via SharePoint
Date Ratified:	15/01/19
Ratified by:	Information Governance Steering Group
Consultation:	Representatives from all directorates via membership of the IGSG.
Cross Reference:	Related trust policies and procedures including the Confidentiality Policy and Information Governance Policy
Superseded Docs:	Information Sharing Policy IG09 V1
Date of Equality Impact Assessment:	Pending
Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 11: Consent Regulation 17: Good Governance
Risk Register Reference:	N/A
Contact Details for further information	Deborah Tonkin (Information Governance Manager) Tel: 0161 358 1573 Email: Deborah.Tonkin@gmmh.nhs.uk
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy.

Contents

1. Introduction

1.1 Purpose

The purpose of this policy is to define clear rules, (and associated authorisation governance processes), about:

- what information, (data), may or may not be shared,
- with whom,
- and for what purposes.

There are also explicit requirements around data handling that ensures data is handled in a secure and confidential manner.

1.2 Scope

This document seeks to provide all Greater Manchester Mental Health NHS Foundation Trust (GMMH) personnel who use patient data with guidance to safeguard the confidentiality of the patient when the data is used for purposes other than direct patient healthcare, (legal basis GDPR Article 6 (1)e 9h).

This policy is concerned with the security of patient information when sharing for direct patient care and for purposes other than direct patient care.

This policy is in line with the NHS Operating Framework and the Information Commissioner's statutory Code of Practice.

2. Definitions

DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation 2018
IAA	Information Asset Assistant
IAO	Information Asset Owner
IG	Information Governance
IGM	Information Governance Manager
IGSG	Information Governance Steering Group
ISA	Information Sharing Agreement
PID	personal identifiable data

3. Duties

3.1 Board/Lead Committee

The Information Governance Steering Group (IGSG) will be responsible for the

approval and monitoring of this Policy. The IGSG is accountable to the Digital Strategy Group who has responsibility for ensuring that sufficient resources are provided to support the requirements of this Policy.

3.2 Directors, Heads of Service and Managers

All Directors, Heads of Service and Managers will be responsible for ensuring that this Policy is communicated and implemented within their area of responsibility and that the principles and standards which constitute good information sharing are adopted and are followed on a day to day basis.

3.3 Caldicott Guardian

The Caldicott Guardian is the appointed senior clinician who carries the ultimate responsibility to oversee the use and sharing of patient identifiable and clinical information. This is a key role in ensuring the Trust satisfies the highest practical standards for processing patient identifiable information. Acting as the 'conscience' of the Trust, the Caldicott Guardian actively supports work to facilitate and enable information sharing and advises on options for lawful and ethical processing of information as required.

3.4 Data Protection Officer

A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). The data protection officer is responsible for overseeing data protection and information governance strategy and implementation to ensure compliance with GDPR requirements. The DPO will monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs), and act as a contact point for all data subjects including information sharing.

3.5 Project Owners/ Business Managers/ IAOs

All project owners/business managers/IAOs must ensure that an information sharing agreement is in place before information is shared when starting new contracts. If an information sharing agreement is not in place then it is the responsibility of the project owner to ensure that Information Governance team are made aware of any new projects so the necessary requirements are reviewed and met.

All IAOs will be responsible for ensuring that Information Sharing Agreements are signed off, and reviewed annually in line with the requirements of the General Data Protection Regulation and the Information Commissioner's Office Information Sharing Policy.

All Project Owners will need to complete a Data Protection Impact Assessment before any new requests are started. This will be for the IG team and DPO to review to ensure that there is a legitimate basis to share information.

3.6 Employees

All staff should be aware of their own personal responsibilities for information sharing and compliance with the law. There must be an authorised DPIA, contract and, where appropriate, an ISA in place prior to sharing any data.

3.7 Contractors

Contractors are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these.

3.8 Information Sharing Partners

All information sharing partners must comply with the signed contract and information sharing agreement and any information breaches must be reported back to GMMH.

4. Processes and Procedures

4.1 Information and Data Sharing – Data Protection Impact Assessment

In the early stages of developing a project involving PID, (personal identifiable data), it is a **legal requirement** under GDPR that a Data Protection Impact Assessment, (DPIA), is completed.

The DPIA will ensure that all aspects of data security and protection, including privacy, have been addressed and considered. It will highlight all risks associated with the proposed sharing for escalation to the Information Governance Manager, Data Protection Officer and, where a risk cannot be mitigated to an acceptable level the risk, will be reported to the ICO by the DPO.

Contact the Information Governance team for a copy of the Data Protection Impact Assessment template and to register your DPIA.

When sharing information, it is important to remember that where possible anonymised and/or pseudonymised information should be used.

There must be a legal basis identified for sharing of data. The GDPR legal basis can be found in Appendix 1.

In addition, the Caldicott Principles must also be considered to ensure that the information being used is done so in the best interests of the patients. The Caldicott Principles can be found in Appendix 2.

The following points define the GMMH approach for the sharing of Information and data:

- Information/data use and sharing will meet legal requirements.

- All patient identifiable data flows to the Trust will be recorded on the Trust data flow mapping tool.

- Access to patient identifiable data will be:

    - To use the minimum amount of information required.
    - Data will be anonymised or pseudonymised where possible
    - On a “need to know” basis.
    - Within a secure system/method (technical and organisational).

- All information sharing must have agreed processes for authorising the use of patient identifiable data.

- Person identifiable data will not be shared or otherwise released unless appropriately authorised with a completed DPIA and ISA.

- Where there is no approved process already in place, the Caldicott Guardian holds responsibility for authorizing, (or not), the release of patient identifiable data.

- Any patient level data sharing with other organisations outside the member organisation will be documented and reflected in authorised data sharing agreements and processes.

- Individual consent to sharing information will be sought where appropriate/possible (for example within approved Research Projects).

- Transfer of data will be via approved secure processes (technical and organisational) to prevent loss or unauthorised access.

- Publication rules will be adopted to ensure confidentiality issues, data sources, data quality; audit trails are sufficiently addressed / documented in published information.

- Aggregate data will usually be available to the public unless falling under Freedom of Information Act exemptions.

- Methods of transferring data will be secure and encrypted. Nhs.net to nhs.net using the Secure File Transfer is the preferred GMMH method of transferring data electronically. (If you require an NHS.net account you must contact the IT department via the IM&T Support Central system). Other public bodies email prefixes can be found in the Safe Haven Policy.

- If any changes are made to an Information Sharing Agreement already in place it must be re-signed and dated by all parties or at the very least emails from all signatories approving the changes and all relevant people informed.

4.2 Information Sharing Agreement Template

The ISA template can be found on the IG intranet pages or a copy can be requested by logging a job via Support Central.

4.3 Clinical to Clinical sharing

Data can be shared from clinician to clinician for medical purposes, (including preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services), which is undertaken by a health professional to ensure the continuity of care.

4.4 Sharing data for legal requirements

The Trust will comply with sharing data where current legislation mandates.

This includes:

- when the information is required by statute or court order;
- where there is a serious risk to public health;
- where there is risk of serious harm to other individuals;
- for the prevention, detection or prosecution of serious crime providing the Data Protection Form is signed by a superintendent or above and that the information is for benefit of the wider community;
- the needs of the children as paramount under the Children Act 1989 needs to make reference to Trust Safeguarding Policies to cover children & vulnerable adults and authoritative guidance for professionals;
- knowledge or belief of abuse or neglect;
- circumstances detailed in any Dangerous Offenders policy;
- to protect the vital interest of the subject
- for the purpose of obtaining legal advice, and establishing, exercising or defending legal rights;
- by order of the Secretary of State;
- for the purpose of safeguarding national security.

Advice on when any of the above conditions may apply in relation to the sharing of information can be obtained from the Caldicott Guardian or the Information Governance Manager.

5. Training Requirements

Training is not required for this document. Advice on completing an Information Sharing Agreement can be obtained from the Information Governance Team.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
All new Information Sharing Agreements to be reviewed	Before final sign off	Reviewed by the IG team	ISA Matrix	IG Team	IGSG
Contracts and ISA's already in place need to be checked to make sure they are still in date and cover current legislation and data protection.	Annually	Reviewed by Directorate IAO	Contract and ISA Matrix	Individual Departments	IGSG

7. Resource/Implementation Issues

The Information Sharing Policy has been reviewed and no additional resource issues have been identified.

8. Risk Issues

Directorates are not always aware of contracts and ISAs in place. All Directorates have to list contracts and ISAs in place as evidence for the Data Security and Protection Toolkit.

9. Requirements, Supporting Documents and References

9.1 Requirements

Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 11: Consent Regulation 17: Good Governance
Other requirements	NHS Digital Data Protection & Security Toolkit (formerly known as information governance toolkit) Legislation including GDPR & Data Protection Act

9.2 Supporting Documents

- Information Governance Policy

- E-mail and Internet Policy
- Information Security Policy

9.3 References

There are several acts and national guidance by which Information Governance abides. These include but are not limited to:

- General Data Protection Regulation available from www.opsi.gov.uk
- Access to Health Records Act 1990 available from www.**opsi**.gov.uk
- Human Rights Act 1998 available from www.**opsi**.gov.uk
- Freedom of Information available from www.**opsi**.gov.uk
- Record Management available from: http://www.nationalarchives.gov.uk/recordsmanagement
- Records Management NHS Code of Practice http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf
- Common Law of Confidentiality www.**opsi**.gov.uk
- NHS Confidentiality- code of Practice available from: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPo_licyAndGuidance/DH4069253
- Caldicott Report available from: https://www.gov.uk/government/uploads/system/uploads/attachment data/file/ 192572/2900774InfoGovernanceaccv2.pdf
- The Abortion Regulations Act 1991 available from: http://www.opsi.gov.uk/SI/si1991/Uksi19910499en1.htm
- The Computer Misuse Act 1990 available from: http://www.opsi.gov.uk/acts/acts1990/Ukpga 19900018 en 1.htm
- The Census (Confidentiality) Act 1991: http://www.opsi.gov.uk/ACTS/acts1991/Ukpga19910006en1.htm
- The Civil Evidence Act 1995: http://www.opsi.gov.uk/ACTS/acts1995/Ukpga 19950038 en 1.htm
- The Electronic Communications Act 2000: http://www.opsi.gov.uk/acts/acts2000/20000007.htm
- The Public Interest Disclosure Act 1998: http://www.opsi.gov.uk/ACTS/acts1998/19980023.htm
- Crime and Disorder Act 1998: http://www.opsi.gov.uk/ACTS/acts1998/19980023.htm

10. Subject Expert and Feedback

Deborah Tonkin, Information Governance Manager

Chris Daly, Caldicott Guardian

11. Review

Trust policy for review is every five years, however this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.

Appendix 1 – GDPR Legal basis for sharing

Mental health data is classified as special category data as such it must meet at least one basis in Article 6 **and** one form Article 9

Article 6 (1)

a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;

d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 9

a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

b) processing is necessary for the purposes of carrying out the obligations and exercising specific **rights of the controller or of the data subject in the field of employment and social security** and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made **public by the data subject**;

f) processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity;

g) processing **is necessary for reasons of substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of **preventive or occupational medicine**, for the **assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of **public interest** in the area of **public health, such as protecting against serious cross-border** threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for **archiving purposes** in the **public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2 – Caldicott Principles

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.